A Policy Landscape

In this chapter we present our recommendations for how the policy landscape in the US and other liberal democracies should respond to the opportunities and challenges brought on by quantum information science. These recommendations are informed by the four scenarios of quantum futures we presented in Chapter 8, combined with the understanding of technology capabilities we discussed in Part I.

The most important social and political changes resulting from quantum technologies will not be felt uniformly: there will be winners and losers. But this is not a zero-sum game: with good policy choices, there can be *dramatically more* winners than losers, and we can use other mechanisms to mitigate the negative impacts.

Policymakers have already decided to make large, but not historically unprecedented, investments in quantum technologies. Such investments are known as *industrial policy*, because they are intended to stoke a nation's prowess in science and technology. As these political *bets* reach maturity and begin to pay off, some quantum technologies will diffuse into society. How can we manage the policy challenges raised by those technologies?

We begin this chapter by putting our cards on the table and presenting our policy goals. We then explore how to achieve these goals using traditional policy levers: direct investments, education, and law. We conclude with a discussion of national security issues.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

9.1 Quantum Technology's Policy Impact

To ground our policy discussion, we start by articulating our high-level policy goals that we hope will be shared by most readers:

1. Quantum technologies have the potential to profoundly benefit human society, particularly if non-military, non-intelligence uses predominate. To take just one example, there are clear paths to improved detection, diagnosis, and treatment of disease from quantum sensing and quantum simulation. A public/private sector approach that enables commercialization of quantum sensing and computing is likely to produce a market for medical and other pro-social uses of quantum technologies.

2. We think there is an important contextual difference between intelligence and military technology uses on one hand, and law enforcement uses on the other. While we understand the need to use quantum sensing for the first, these technologies would allow unprecedented surveillance and intrusion into private spheres. Therefore we seek to avoid having quantum sensing devolve to law enforcement and proliferate to private actors in advance of significant public discussion and approval, lest we become inured to the privacy invasions that these technologies would likely enable.

3. The capabilities brought about by quantum sensing and quantum computing could result in devastating destabilization of civilian infrastructures and undermining societal trust and integrity mechanisms, public and private law, and even the historical record. As such, civic society needs to embark now on a fact-based, science-based discussion of these capabilities and appropriate mechanisms for controlling them, similar to the discussions in the 1950s and 1960s regarding the control of nuclear weapons and nuclear energy.

Next, we surface two of our assumptions regarding quantum technology, the first regarding technological determinism, the second regarding technological novelty of quantum information science:

Moderate technological determinism We view QIS technologies as political artifacts, in the tradition identified by Langdon Winner (see Section 8.1, p. 305). We do not view this technology as

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

policy-neutral. Quantum technologies are powerful and will tend to push policy discussions in a specific direction, absent political will to redirect. We may be in the driver's seat, but the car is in motion and it is proceeding down a highway with limited offramps and forks in the road.

The invention and growth of the Internet provides a good example of the power and limits of technological determinism. It also shows how *predictions* of where the car will travel depend strongly on each forecaster's beliefs, principles, and hopes. In the initial adoption of the computer networks, visionaries like Ithiel de Sola Pool and John Perry Barlow predicted that the technology would promote democratization, individual empowerment, and exclusion of government power and action.[1] They may have been excellent forecasters, or they may have been merely expressing their hopes as prediction: both were self-described libertarians.

History has shown the Internet's impact is more complex, but also dependent on *implementation specifics*, the social contexts in which the technology was deployed. In liberal democracies cyberspace largely erased restrictions on speech, commerce, and intellectual property. In nations such as China, the government spent significant effort to transform the Internet from a technology of freedom into a technology of control – and it was largely successful. The effect is that the Internet has strengthened China's political institutions.

We embrace the idea that quantum technologies are inherently political, while rejecting the notion that our future is determined by them. We can anticipate the effects of quantum technologies and work so their deployment supports liberal values, but the longer we wait, the harder it will be to do so.

Novelty that's limited but nevertheless game-changing In some cases, quantum technologies offer fundamentally new capabilities, but in other cases they offer merely enhancements for capabilities that we have long had at our disposal. In part this is because many quantum technologies, particularly those of quantum sensing, date back to the 1950s.

We believe that casting quantum technologies as entirely novel is itself a political act, because the claim of novelty is frequently noth-

[1] Sola Pool, *Technologies of Freedom* (1983); Barlow, "A Declaration of The Independence of Cyberspace" (1996).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

ing more than an ideological appeal against government regulation of the marketplace.

That is, while some might argue that quantum technologies are "novel" and that regulating them now might kill the goose before it lays its first golden egg, we argue that making this argument is itself a wolfish, anti-regulatory political argument against regulation, wrapped in the sheep's clothing of technological exceptionalism that only partially applies. It is an argument designed to limit the ability of policymakers to make sense of what are in reality predictable futures.

* * *

In this chapter, we emphasize strategically and legally relevant differences between classical and quantum technologies. Because the landscape of implications is so large, leading to complex, contingent policy conflicts, and because this quantum age as we conceive of it is so new, we strive to remain at the options level rather than solve specific policy issues.

9.1.1 Game-Changers: Code-Breaking and Possibly Machine Learning

Based on our analysis in the preceding chapters, we believe that the two key areas where quantum's impact will be the greatest are code-breaking and machine learning. We discuss code-breaking extensively in Chapter 5, but we mention machine learning only in passing. This is because far more is known about quantum computing's impact on the first than the second.

We *know* that a sufficiently large quantum computer will be able to crack nearly all of today's encrypted messages, because we have mathematical proofs that show a sufficiently large quantum computer will be able to factor large numbers and compute discrete logarithms in polynomial time. If we can build a large enough machine, today's encryption algorithms are toast.

Quantum-assisted machine learning is at a much earlier point in its development. There is no scientific consensus on whether or not quantum-assisted machine learning will offer fundamental speedups in training machine learning algorithms. For example, many algorithms require that training data itself be stored in some kind of quantum memory – something we don't know how to build. Even if quan-

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

tum computing dramatically reduces the time and power requirements for training machine learning algorithms, there is no mathematical proof that perfectly training statistical classifiers will offer breakthrough capabilities not enjoyed by today's systems. Therefore, for the remainder of this chapter, we explore the policy implications of instantaneous, perfect, and all-powerful realized machine learning applications, without addressing the question of whether or not quantum computing will ever get us there.

We believe that the most likely near-term quantum technologies to be realized, the quantum-simulators, are unlikely to have game-changing, breakthrough policy implications. However, as we argued in Chapter 5, the process of creating teams to realize quantum simulators, and access to the simulators themselves, will make it more likely for an organization to realize the other game-changing benefits of quantum computing that we mentioned above.

9.1.2 Quantum Technology Dominance

Accepting that there is a role for policymaking in promoting the goals we articulate above, an important question to answer is, *What is the appropriate governmental level to engage in that policymaking?* Should there be QIS treaties among governments, similar to the way that the Treaty on the Non-Proliferation of Nuclear Weapons was designed to promote the peaceful use of nuclear power while preventing the spread of nuclear weapons? Is quantum education something that should be promoted at the community level, with school boards advocating for the establishment of science-based courses in "quantum thinking" for children in secondary school aged 12 through 14, and quantum physics being taught alongside mechanics for students destined for college?

To put it in the language of defense doctrine, is it possible for a nation to achieve *quantum dominance*? By "dominance" we mean, is it possible for a nation to take unilateral actions on matters of quantum technology research, development and deployment, while simultaneously denying state-of-the-art quantum technology to others?

Achieving and maintaining quantum dominance would require a unification of industrial policy, education policy, significant support for research, and strong export controls. We discuss these options in this chapter.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

At the same time, the race to build working quantum systems lays bare the fiction of other national attempts to achieve and maintain various forms of technological sovereignty. At the end of World War II, Operation Paperclip successfully scooped up Germany's rocket scientists, giving the US a brief head start in the space race, but the Soviet Union quickly pulled ahead in both rocketry and space exploration. Likewise, the Soviet Union was able to eliminate US nuclear dominance through a combination of espionage and scientific ingenuity.

9.2 Industrial Policy

Whether governments should invest in quantum technologies is a settled policy issue: they are doing so, generously, but not at levels that are historically unprecedented, such as the Manhattan Project ($28 billion in adjusted dollars) or the Apollo Space Program ($190 billion). The pursuit of quantum technologies is now a significant *industrial policy* priority in the US and abroad. Industrial policy is "a strategy that includes a range of implicit or explicit policy instruments selectively focused on specific industrial sectors for the purpose of shaping structural change in line with a broader national vision and strategy."[2] Industrial policy can be general, in the sense that tax breaks or incentives for investment are shaped to broadly advantage domestic business interests. Industrial policy can also be specific, in that the government can organize policies to aid a particular vertical industry, such as price supports for corn farming, tax-subsidized grazing fees for cattle ranchers, and requirements to add ethanol to gasoline.

9.2.1 National Quantum Investments outside The US

The embrace of quantum technologies by national governments clearly flows from lessons learned by observing the US technology miracle. The US has enjoyed a decades-long period of technological superiority, culminating with the internet boom and the vast production and concentration of wealth, thanks to strategic investments in computing, microelectronics, packet networking, and aerospace between 1940 and 1980.

Quantum technologies provide an opportunity for a reordering of technical might that should concern US policymakers whose goal is to maintain the nation's technological superiority. The EU and

[2] Oqubay, "Climbing without Ladders: Industrial Policy and Development" (2015).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

China are desperately seeking opportunities to overcome the asymmetric advantages that the US has enjoyed from incubating Silicon Valley. For example, the Internet, as a global communications system, is still largely seen by other nations as America's playing field. Political scientists now recognize how American power is exercised through control of others' access to and use of networked systems like the US-dominated Internet.[3] Many nations have acknowledged the continuing disadvantage of having their domestic communications structured by the Internet and often delivered by US dominant companies. This is another lens for understanding the ongoing antagonism between US policymakers and Chinese communications firms such as Huawei.

Both the EU and China have established significant quantum information science efforts that include basic research funding. This funding often goes beyond the development of specific quantum technologies, and supports basic, theoretical research, workforce preparation, educational outreach, and even funds inquiry into the philosophy of quantum mechanics.

In 2018 the EU funded a €1B ($1.2B) quantum initiative, supporting both multiple corporate and academic research groups and funding specific projects. Europe's investment also builds upon a number of domestic competitors in quantum computing, communications, and precursor technologies, such as high-end cooling devices and precision-machined equipment.

China appears to have invested about $3B in quantum technology, according to a report warning of the country's muscularity and devotion to surpassing American innovation in the space.[4] But there are many popular reports claiming many billions more are invested in China's quantum technology, and in infrastructure for massive technology integration centers. For instance, it is reported that China invested $10B in support for quantum internet science based at the University of Science and Technology of China in Hefei. As detailed in Part I, China has implemented the longest publicly known fiber quantum network, distributed quantum keys by satellite intercontinentally, created the most powerful (albeit single-purpose) quantum computer, and appears to be developing game-changing quantum

[3] Farrell and Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion" (2019).

[4] Kania and John Costello, *Quantum Hegemony? China's Ambitions and The Challenge to US Innovation Leadership* (2018).

sonar technology that could one day be deployed to hotbeds of conflict, such as the South China Sea. Many of these accomplishments are not heralded by state media, but rather by peer-reviewed articles in *Science* and *Nature*.

Press accounts of national quantum policies frequently focus on pan-EU projects and overlook individual national initiatives. As early as 2014, the UK embarked on an academic/industry program investing £270M ($375M) to establish hubs focusing on sensing, communications, and quantum technology development. These UK national quantum technologies (UKNQT) hubs involve many universities and scores of private partners. A related initiative is pouring over £167M into graduate training in QIS – Brexit is giving the UK additional incentives to compete technologically with Europe. Germany announced an additional €650M in funding in early 2020, but after the COVID pandemic's effects were realized, Germany introduced a €50 *billion* ($60B) stimulus package in "future technologies," which explicitly earmarks €2B ($2.4B) for quantum technologies, as well as €300M ($360M) for development of a Munich Quantum Valley.[5] France has committed over €1B to QIS as well.

Nations in Europe with their own quantum industrial policies are engaged in a two-sided strategy. These nations want to be part of the EU funding compact, which is characterized by regional sovereignty and technology superiority goals. Such sovereignty carries with it the East/West bloc downsides we discuss in Chapter 8. But by investing in their own national quantum portfolios, EU nations straddle the divide between closed sovereign strategies and the open collaboration typical of scientific inquiry. The two-sided approach enables nations to attain more independence from the EU and have more opportunities to engage the US and foreign companies that might end up developing breakthrough insights.

Russia appears to be late to the competition and is absent from state-of-the-science developments in quantum technology. Not until December 2019 did the country announce a major initiative to fund quantum research, and when it did, the amount specified – $790M over five years – was underwhelming given the country's population, ambition, and early contributions to the field.[6]

[5] Bundesministerium für Bildung und Forschung, "Die Zweite Quantenrevolution Maßgeblich Mitgestalten" (2020).

[6] Schiermeier, "Russia Joins Race to Make Quantum Dreams a Reality" (2019).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

India too has recently announced a major initiative in QIS research, with a $1B commitment made in its 2020 budget.[7] India's investment should be seen in context with the nation's outer space program, which it funds in the billions, and that has launched vehicles to the Moon and Mars.

9.2.2 US Quantum Technology Industrial Policy

The US government quickly changed its posture in response to EU and Chinese investment. Previously, the US had spent hundreds of millions pursuing various QIS projects, many of which were funded through the Department of Defense, making them difficult to track. Responding to the foreign interest and investment, Congress quickly introduced and enacted the National Quantum Initiative Act.[8] Signed by President Trump in December 2018, the NQIA authorized $1.2 billion in research and education, to be coordinated by the White House's Office of Science and Technology. The NQIA's National Quantum Initiative (NQI), led by NIST, NSF, and the Department of Energy, in turn coordinated government/industry/academic relations to promote the development of QIS and quantum technologies.[9] NQIA also formally established the Subcommittee on Quantum Information Science (SCQIS) of the National Science and Technology Council. Congress specified that this new body will be chaired jointly by the Director of the National Institute of Standards and Technology (NIST), the Director of the National Science Foundation (NSF), and the Secretary of Energy, and has participation by the Office of Science and Technology Policy (OSTP), Office of the Director of National Intelligence (ODNI), Department of Defense (DOD), Department of Energy (DOE), National Institutes of Health (NIH), and the National Aeronautics and Space Administration (NASA).

In 2020, the Trump administration named appointees to the National Quantum Initiative Advisory Committee (NQIAC), which was established by the NQIA to advise the new subcommittee. Advisory committees are typically constituted of experts from outside government; initial appointees are prominent academics and participants from startup, defense industrial base, and established technology

[7] Padma, "India Bets Big on Quantum Technology" (2020).

[8] US Congress, *National Quantum Initiative Act* (2018).

[9] Christopher Monroe, Raymer, and J. Taylor, "The US National Quantum Initiative: From Act to Action" (2019).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

firms in the space.[10] The body is charged with regularly making reports to the President and Congress, and to give advice on progress made in implementing the quantum initiative, management and implementation issues, American leadership strategy in QIS, potential for international cooperation in QIS, and whether "national security, societal, economic, legal, and workforce concerns are adequately addressed by the Program." The first meeting took place on October 27, 2020.

Following the NQIA, President Trump proposed doubling research funding for QIS by fiscal year 2022. In August 2020, the administration announced the creation of five quantum information science centers coordinated by Department of Energy Labs (the Argonne, Brookhaven, Fermi, Lawrence Berkeley, and Oak Ridge National Laboratories). In addition to a $625 million commitment of federal government funds, the project is complemented with over

[10] The body was chaired by Dr. Charles Tahan, OSTP Assistant Director for Quantum Information Science and Director of the National Quantum Coordination Office, and by Dr. Kathryn Ann Moler, Dean of Research at Stanford University. The initial appointees were: Professor Timothy A. Akers, Assistant Vice President for Research Innovation and Advocacy, Morgan State University; Professor Frederic T. Chong, Seymour Goodman Professor, University of Chicago; Dr. James S. Clarke, Director, Quantum Hardware, Intel Corporation; Professor Kai-Mei C. Fu, Associate Professor of Physics and Electrical and Computer Engineering, University of Washington; Dr. Marissa Giustina, Senior Research Scientist, Google, LLC; Gilbert V. Herrera, Laboratory Fellow, Sandia National Laboratories; Professor Evelyn L. Hu, Tarr-Coyne Professor of Electrical Engineering and Applied Science, Harvard University; Professor Jungsang Kim, Co-Founder, IonQ and Professor of ECE, Physics and Computer Science, Duke University; Dr. Joseph (Joe) Lykken, Deputy Director for Research, Fermi National Accelerator Lab; Luke Mauritsen, Founder/CEO, Montana Instruments; Professor Christopher R. Monroe, University of Maryland; Professor William D. Oliver, Associate Professor EECE, Professor of Practice Physics, and MIT-Lincoln Laboratory Fellow, Massachusetts Institute of Technology and MIT-Lincoln Laboratory; Stephen S. Pawlowski, Vice President of Advanced Computing Solutions, Micron; Professor John P. Preskill, Director of the Institute for Quantum and Matter, California Institute of Technology; Dr. Kristen L. Pudenz, Lead for Quantum Information Science, Lockheed Martin; Dr. Chad T. Rigetti, Founder and CEO, Rigetti Computing; Dr. Mark B. Ritter, Chair, Physical Sciences Council, IBM T.J. Watson Research Center; Professor Robert J. Schoelkopf, Sterling Professor of Applied Physics and Physics, Yale University; Dr. Krysta M. Svore, General Manager of Quantum Systems, Microsoft Research; Professor Jinliu Wang, Senior Vice Chancellor for Research and Economic Development, The State University of New York; Dr. Jun Ye, JILA Fellow, Professor of Physics, National Institute of Standards and Technology.

$300 million in commitments from academic institutions and companies.

It is important to recognize that research funding has many paths in the US. In addition to NQIA funds, quantum technology projects receive support directly from the Department of Defense, under its Research, Development, Test, and Evaluation (RDT&E) budget. This budget now exceeds $100 billion annually; the DOD 2021 budget estimates for RDT&E mention the word "quantum" on 27 pages of the 1094-page document.[11] As this manuscript goes to publication, President Biden and other policymakers proposed an extra $250 billion in funding for general high-technology research. With this level of money flowing into the field, the question becomes one of talent: are there enough people with the rarefied, specialized forms of training that quantum technologies require? Below, Section 9.3 (p. 401) focuses on the challenge of workforce training.

9.2.3 Industrial Policy: Options and Risks

With billions being spent by many nations, quantum technologies are clearly part of many nations' industrial policy. We note, however, that the spending is not at the levels of previous big technology feats, such as when Russia and Europe each found the need to replicate the US GPS constellations (see Figure 9.1).

Quantum technologies make a good case for vertical industrial policy interventions under a framework applied by Vinod Aggarwal and Andrew W. Reddie. Writing in the cybersecurity context, one that shares strategic characteristics common with quantum technologies, the authors explain that governments pursue industrial policy to create markets (market creation), to facilitate markets, to modify markets, to substitute for market failures (market substitution), and to set rules to control technologies created by markets (market proscription).[12]

In this section, we consider the risk of market substitution for quantum key distribution, quantum networking, and quantum computing in general. In all three categories of quantum technologies, market substitution appears to be necessary to support continued

[11] Office of the Secretary of Defense, "Department of Defense Fiscal Year (FY) 2021 Budget Estimates" (2020).

[12] Aggarwal and Reddie, "Comparative Industrial Policy and Cybersecurity: a Framework for Analysis" (2018).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Market Substitution

In the literature of industrial policy, the phrase *market substitution* occurs where "instruments of political authority are used to allocate or distribute resources or control conduct of individuals or organizations..."[a] Aggarwal and Reddie point to several examples in the cybersecurity context. For instance, In-Q-Tel is a privately-held not-for-profit venture capital firm that is funded by the US Intelligence Community and other federal agencies to help the government stay atop cutting edge technology developments. Governments also substitute for cybersecurity market failures by promoting educational and workforce training efforts.[b] Such moves can "prime the pump" by supporting a new market until there is sufficient demand. Market substitution is a more controlling approach than market *facilitation*, where incentives are shaped to spur the private sector into useful action – for example, by eliminating the liability shield for cybersecurity vulnerabilities that many software and service providers currently enjoy. The control inherent in substitution means that choosing properly, and choosing in the public interest – instead of the interest of the choosers – is a challenge in industrial policy.

[a] R. G. Harris and Carman, "Public Regulation of Marketing Activity: Part II: Regulatory Responses to Market Failures" (1984).

[b] Aggarwal and Reddie, "Comparative Industrial Policy and Cybersecurity: a Framework for Analysis" (2018).

development of these technologies for an indeterminate amount of time.

QKD Market Substitution

While there are obvious commercial uses for quantum metrology and sensing among the most sophisticated and well-resourced companies (such as oil services firms, mining firms, and medical imaging), the National Academies report estimated that there are only limited short- to medium-term commercial uses for quantum communications such as QKD.[13] One of those limited uses of quantum communications is to secure point-to-point links used by banks and trading houses – organizations that have both the resources to procure

[13] Grumbling and Horowitz, *Quantum Computing: Progress and Prospects* (2019).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

private fiber connections, and the risk of loss necessary to justify investments in QKD.

Otherwise, despite the excitement surrounding QKD, commercial justifications for it are thin. To date, most public deployments of QKD are better regarded as technology demonstrations, rather than the first step in creating significant new markets. For example, in 2007 the Swiss government allowed a domestic company to use quantum encryption to transmit election information to a central government repository, with the justification provided by Geneva state chancellor Robert Hensler, that QKD would "verify that data has not been corrupted in transit between entry and storage."[14] The irony here is that QKD does not provide data integrity, it provides secrecy against some future attacker with a code-breaking quantum computer *who also captured and made a permanent recording of the encrypted transmission*. But the use of QKD by the Geneva government did result in having *New Scientist* note that "three companies [are] pioneering the field – BBN Technologies of Boston, US; MagiQ of New York, US; and ID Quantique of Geneva, Switzerland."

Today's commercial QKD systems send their flying qubits down a single strand of fiber-optic cable that's typically 10 km to 100 km in length. This is ideal for exchanging encryption keys between a data center in lower Manhattan and a data center in Hoboken, NJ. A near-future satellite-based QKD system might send pairs of entangled photons simultaneously to an embassy in Moscow and a government office in London, assuring that no future Russian government might be able to crack RSA encryption keys that are used today (although another way to address this threat would be to use a human courier to deliver a year's worth of AES-256 keys in a secured briefcase). However, it is inconceivable that businesses or consumers would opt for QKD technology to encrypt the packets that they send over today's Internet: there is no way that the pairs of photons could be routed to the correct destination to be used for decryption. Quantum encryption for the masses will need to wait for a quantum internet, and that might be a very long wait.

Where QKD might play a role in the commercial Internet would be ISPs using it to encrypt specific internal, high-risk long-haul links. The distance from Moscow, Russia, to Kyiv, Ukraine, is 865 km; in a few years this might be within the service range of a QKD system.

[14] Marks, "Quantum Cryptography to Protect Swiss Election" (2007).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Western businesses with offices in Moscow might be willing to pay a premium for an internet connection from the Ukraine that is encrypted using QKD. However, if they do, it is our opinion that they will be wasting their money unless they also have 24-hour guards to protect against having their laptops stolen, perform detailed background investigations of all their employees, and undertake similar measures to protect themselves from a wide range of electronic surveillance.

Another possible customer of QKD is backbone providers and others that have private ("dark fiber") networks. Such providers typically have more control over elements of the network and their protocols, and are interested in protecting point-to-point connections. Some of these network owners may also have particular concerns about nation-state spying, either by adversaries digging up their private fiber and tapping it, or by bribing or extorting company engineers to provide access. For instance, as discussed in Chapter 7, in 2017 South Korea's SK Telecom claimed that it had secured its network backhaul with a QKD system, offering additional protection to a wireless network serving over 350 000 mobile users in Sejong City. Given that the cost of QKD network encryption devices is similar to the cost of a few full-page advertisements in a leading newspaper, this may be money well-spent, even if it is just for bragging rights.[15] That's because QKD protects today's encryption tomorrow: any possible fallout that would be protected by a QKD-based system won't take place for years, or even decades.

We thus believe that the commercial prospects for QKD are poor, because of a lack of incentives, coordination problems, and primarily the sufficiency of classical encryption alternatives. Furthermore, although the QKD protocols are information-theoretic secure, the actual QKD *devices* can still be hacked.[16] Market substitution will be required to create a viable QKD industry.

Quantum Networking Market Substitution

The near-term case for quantum internet is even poorer than the case for QKD for one simple reason: although commercial QKD systems can be purchased and used today, working quantum network-

[15] Kwak, "The Coming Quantum Revolution: Security and Policy Implications, Hudson Institute" (2017).

[16] Anqi et al., "Implementation Vulnerabilities in General Quantum Cryptography" (2018).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

ing systems appear to be even further in the future than large-scale quantum computers.

Consistent with the market substitution approach, in 2020, the Department of Energy and University of Chicago announced plans to build a national quantum internet framework.[17] Such a fully quantum internet would use entangled photons for communication, thus giving communicants security against quantum computing attacks, the ability to detect interception or blockage of the signal, and the ability to connect quantum computers over distances. Nevertheless, quantum internet is still an experimental concept. Most designs call for a fiber optic network passing entangled photons between quantum computing elements to maintain and communicate quantum states. Many fundamental engineering problems need to be addressed. And even if some kind of quantum network is created, such a network would be a para-internet, for specific use cases, and not a general communications infrastructure.

The power of the Internet that we have today is that it is a general network. Although the Internet started as a slow-speed network capable of sending email and allowing users to log on to remote computers, by the 2000s the Internet was being used to transmit all manner of broadcast and interactive content. Slowly legacy networks such as telephone systems were reworked so that they traveled over the Internet. But this was not a surprise: even in the 1970s, it was clear that the Internet would one day encapsulate all other communications networks. (Xerox's Palo Alto Research Center demonstrated the first packet network voice system, called the "Etherpone," in 1982, before the Internet adopted TCP/IP.) No such technology roadmap is envisioned for quantum networks.

No similar claim can be made for a quantum internet. Although some authors claim that quantum networks will be able to transmit vast amounts of data faster than the speed of light, such claims are inconsistent with both our vision of quantum networks and the laws of physics as we currently understand them (see the sidebar "Alas, Faster-than-light Communication Is Not Possible" on page 301). Instead, it appears that the advantage of quantum networks is they would allow quantum computers to engage in quantum communications algorithms that would decrease the number of required steps

[17] Dam, *From Long-Distance Entanglement to Building a Nationwide Quantum Internet: Report of The DOE Quantum Internet Blueprint Workshop* (2020).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

for certain operations. Such a network would also allow for a quantum computer to connect to a remote quantum database (if one existed) to search that database using Grover's algorithm, without the database operator learning what had been searched and what had been retrieved (blind quantum computing). But such fantastic applications seem decades in the future, if they are even physically possible.

For these reasons, as governments promote development of the quantum internet, the best-case scenario is a para-internet for certain applications, and of course, the learning-by-doing inherent in research and development. After all, quantum communications devices are merely small quantum computers that compute with flying qubits. Governments investing in quantum communications are also preparing their scientific and technical workforce for the eventual emergence of large-scale quantum computers, although there may be more efficient ways to do so.

Quantum Computing Market Substitution

Turning to the industrial policy case for computing, some companies are beginning to experiment with quantum computing, but there is no broader market for quantum computing services. Classical computers still outperform quantum ones in all practical applications. Although there is a growing commercial market for quantum computing, this use is limited to experimentation and training. That is, at the present time, researchers are focused on researching quantum computing, rather than on using quantum computers to do research. Simply put, there is no market to facilitate with ordinary incentives. Thus, market substitution, in the US case, through massive funding of research, is in order for the time being.

Consider that a wide range of companies are testing a variety of applications for quantum optimization using cloud-based quantum computers and annealers. One promotional video by a quantum computing company summarized projects at:

- BMW (robotic manufacturing)
- Booz Allen Hamilton (satellite placement)
- British Telecom (placement of antennae)
- Denso (ride sharing)

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

- DLR (aircraft gate assignment at an airport)
- Los Alamos National Laboratory (face recognition, social networks of terrorist groups, and attack prediction)
- NASA/Ames (cybersecurity of aircraft traffic management systems)
- Ocado (robot product picking in a warehouse)
- QBranch (election modeling)
- Recruit Communications (real-time bidding in online advertising)
- Volkswagen (vehicular traffic analysis),
- ... and a former academic researcher focused on prediction of health outcomes even where relevant data are missing.

This same promotional video explained that four institutions had installed its systems, perhaps for secrecy reasons, and these systems were mostly focusing on aspects of optimization:

- Google/NASA Ames/USRA,
- Lockheed Martin Corporation/USC ISI,
- Los Alamos National Laboratory, and
- Oak Ridge National Laboratory[18]

But to date, the aspects of these projects that have been shared publicly are aimed entirely at simply getting model problems to work, rather than developing cost-effective solutions to problems that the companies are currently facing.

For companies outside quantum technologies – that is, most companies – buying quantum computing services is still not worth the investment. The National Academies lamented in 2019 that broadly appealing commercial uses of quantum computers have not been developed, and that investment in applications is necessary to kick-start a "virtuous cycle" of innovation in quantum computing. One of

[18] D-Wave Systems Inc., "Quantum Experiences: Applications and User Projects on D-Wave" (2019).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

the group's main findings was that "There is no publicly known application of commercial interest based upon quantum algorithms that could be run on a near-term analog or digital NISQ computer that would provide an advantage over classical approaches."[19] By *commercial*, the Academies essentially means quantum-enhanced computation or service that would give a company a competitive advantage sufficient to justify its cost.

9.2.4 Innovation and The Taxpayer

Until commercial and consumer applications take root, quantum technologies will need some kind of research sponsor to substitute for a market. In the US, the government, major technology firms, and private foundations have been patrons for QIS. These efforts are matched by the EU and China's government-patronage approach. The EU and China seem to be trying to replicate the US success with the Internet in their funding of QIS.

Indeed, there is compelling proof that sustained federal investment over decades in an industry or region can yield ample rewards. Consider California. Prior to the commercialization of the Internet as a tool for connecting consumer and business devices, "the military-industrial complex was the West's biggest business in the cold war years," writes Gerald D. Nash in his economic history of the West. "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."[20] Margaret O'Mara observes that Lockheed, which minted billions creating cutting-edge military hardware, including the P-80, the Polaris missile, the U-2, the SR71, GPS satellites, and the stealth attack aircraft (see Figure 2.12), was the largest high-technology employer in Silicon Valley until the Internet boom.[21] Joan Didion elucidates nineteenth-century forms of federal largess, such as waterworks, dams, irrigation subsidies, railroads and other infrastructure that set the stage for development of the region, again complicating the California narrative of self-reliance and self-made fortunes.[22]

[19] Grumbling and Horowitz, *Quantum Computing: Progress and Prospects* (2019).

[20] Nash, *The Federal Landscape: an Economic History of The Twentieth-Century West* (1999).

[21] O'Mara, *The Code: Silicon Valley and The Remaking of America* (2019); O'Mara, *Cities of Knowledge: Cold War Science and The Search for The Next Silicon Valley* (2015).

[22] Didion, *Where I Was From* (2003).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Today's internet companies emerged from a region where an educated middle class with a focus on engineering was groomed over generations, thanks to the largess of the federal government and the American taxpayer. Companies like Apple built revolutionary products and services but in context these products can be seen as remixes and masterful re-implementations of technologies developed for the military at taxpayer expense.[23] Other Silicon Valley darlings might flounder if they lacked the ability to freely depend on taxpayer-provided infrastructure such as GPS or even the nation's highway system.

Consider the story of Konrad Zuse (Chapter 4). Zuse built a cutting-edge, switch-based computing device in 1936, four years before the British Bombe and eight before a similar project at Harvard University. However, the German government did not embrace computing in the ways the British and the US did. After World War II, the British failed to capitalize on their lead, in the interest of preserving the secrecy of Bletchley Park. (Tommy Flowers, who designed and built the code-breaking Colossus computer, was blocked from re-implementing or commercializing the technology and spent the rest of his professional career working on telephone switching systems.)

The absence of credible competition from overseas allowed the US to dominate the nascent field of electronic computing. In the US, the military, scientific, and defense communities aggressively adopted computing, giving the US a lead that it held for decades. Visionary scientists such as J. C. R. Licklider anticipated the importance of computers and invested in them long before their uses were fully apparent. Licklider convinced legendary defense industrial base company Bolt Beranek Newman Inc. (BBN)[24] to buy not one but two early computers, the most expensive laboratory devices that BBN had ever purchased, before the firm even had uses for them. Of course, such uses quickly became clear. The need for ever-intensive machine analysis during the Cold War funded computer and com-

[23] Mazzucato, *The Entrepreneurial State: Debunking Public Vs. Private Sector Myths* (2015).

[24] Discussed earlier in Section 4.4.1 (p. 146). BBN Inc. eventually became BBN Technologies, and was acquired by Raytheon in 2009. In 2012, President Barack Obama awarded Raytheon BBN Technologies the National Medal of Technology and Innovation, the highest award given by the nation to technologists, recognizing "those who have made lasting contributions to America's competitiveness and quality of life and helped strengthen the Nation's technological workforce."

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

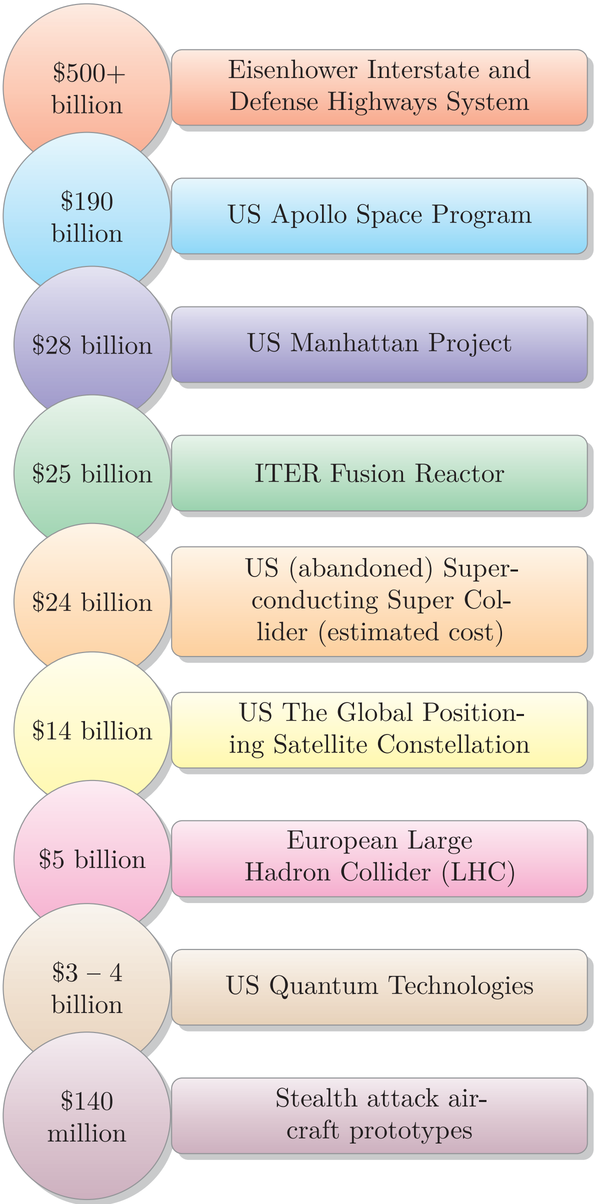
$500+ billion
Eisenhower Interstate and Defense Highways System
$190 billion
US Apollo Space Program
$28 billion
US Manhattan Project
$25 billion
ITER Fusion Reactor
$24 billion
US (abandoned) Superconducting Super Collider (estimated cost)
$14 billion
US The Global Positioning Satellite Constellation
$5 billion
European Large Hadron Collider (LHC)
$3 – 4 billion
US Quantum Technologies
$140 million
Stealth attack aircraft prototypes

Figure 9.1. Major science, technology, and military projects (2021 inflation-adjusted dollars, not to scale). Precise figures for quantum technology investment are elusive because funding flows through both specific authorizations and separately through the Department of Defense.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

ponent manufacturers and drove employment of untold number of programmers. With the advent of the personal computer, computing was democratized, resulting in a cycle where computers became both less expensive and faster. And the US was at the center of that virtuous cycle.

At the dawn of internet commerce, it was not clear at all that the web would even succeed as a medium. Other similar systems had failed: France's "Minitel" was widely used, but it had not spurred an economic revolution. Likewise, the US online service Compuserve had 1.5 million subscribers in 1993, but it was not a vibrant marketplace. Today's most profitable companies, such as Amazon.com, spent years trying to perfect a web platform for commerce. In the process, the company developed its web services platform, which today is responsible for the bulk of the company's operating profits.

Despite these facts on the ground, it is European thinkers and policymakers who primarily promote the belief that governments can be effective market creators in technology,[25] and that these new fields need government incubation to eventually become successful. But Europe suffers because it lacks both Silicon Valley's affluent and gamblesome venture market, and the Valley's highly efficient labor market – the highly educated high-tech workers who, because of state law, can leave an employer when a better deal or more promising technology comes along and go work for a startup or even a competitor.[26]

Turning to the development of quantum technologies, US government funding and technical achievements abound. Scientists at NIST developed the first quantum circuit. That agency's scientists have been in the vanguard of quantum technologies, with three Nobel Prize recipients in this field alone. This book recounts many examples of scientific achievements realized by Department of Defense research institutions, the Department of Energy National Laboratories, and the federal government's medical research gem, the National Institutes of Health. US government agencies were critical for both convening events to develop the theory of quantum computing, and for developing a vision and strategy for funding investment in the field. The state of the science in quantum technologies has advanced

[25] Mazzucato, *The Entrepreneurial State: Debunking Public Vs. Private Sector Myths* (2015).

[26] Saxenian, *Regional Advantage: Culture and Competition in Silicon Valley and Route 128* (1996).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

because of US taxpayers' dollars supporting a strong science and technology industrial policy.

In the larger political conversation, there is rhetoric rising to the level of reaction formation against government involvement in new technology in Silicon Valley. Many technology advocates parrot libertarian ideas from John Perry Barlow's ahistorical statement on internet freedom:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather ...You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions.[27]

Barlow's essay and others like it argue that governments lacked the competence to understand and to act on the Internet. We find such arguments disingenuous, given the US government's widely known and dramatic investments in science and technology that occurred during his lifetime. More broadly, we argue that this brand of libertarianism is bad policy, dangerous, and smacks of hypocrisy. It's bad policy because if the US taxpayer had not supported basic science research, the twentieth century might have been defined by innovation in Japan or Europe. It's dangerous because libertarianism animates extremist anti-government actors, such as Oklahoma City bomber Timothy McVeigh,[28] and because the ideology shares overlapping space with nationalist movements. And it's hypocritical because many of the greatest advocates of libertarianism have themselves been the beneficiaries of significant public largess: we note that between 1971 and 1988, when he ran his family's cattle ranch with his mother,[29] Barlow's business was heavily subsidized by the US government and favored by US tax policy.

[27] Barlow, "A Declaration of The Independence of Cyberspace" (1996).

[28] Ayn Rand's hero, Howard Roark, blows up a public housing complex in response to slights from government bureaucrats.

[29] Schofield, "John Perry Barlow Obituary" (2018).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Many of today's US policy debates flow from a libertarian frame, and the idea that government impedes innovation is widely shared. Perhaps this is why Aggarwal and Reddie observe that 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."[30] Such patronage is an explicit goal in Europe and China's quantum initiatives. Other nations seem to be learning from what the US has done, rather than what various influential opinion leaders have said about industrial policy.

9.2.5 The Risk of Choosing Poorly

One risk of industrial policy is that of choosing poorly: choosing the wrong technology, or investing just enough money to crowd out private investments without sufficient funds to kick-start an industry, or investing more money than can be spent by the available talent, leading to waste and making it more difficult for valuable contributions to stand out.

Governments around the world are trying to position their industrial centers for the future, and quantum technologies are but one possible focus. Governments are also focusing on the promise of automation and machine learning; big bets are being placed on battery and photovoltaic technology development.[31] Innovation is also shaped by other policy concerns, such as environmental impact, that have intersections with quantum optimization. For instance, the European Union is seeking to arrange the economy "circularly," so that technologies used in the future are serviceable and repairable, resulting in less waste.[32]

Consider what happens if governments excessively fund quantum technologies for a decade and the technologies do not create self-sustaining markets: at that point, governments might significantly curtail funding, leaving companies, faculty, and graduate programs fighting amongst themselves for the few remaining scraps. Many people who had spent years mastering difficult quantum technologies would suddenly find themselves without jobs: some would success-

[30] Aggarwal and Reddie, "Comparative Industrial Policy and Cybersecurity: a Framework for Analysis" (2018).

[31] The German government is in the midst of an ambitious plan called *Industrie 4.0*, designed to leapfrog ahead with a focus on the Internet of Things and automation.

[32] European Commission, "A New Circular Economy Action Plan" (2020).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

fully transition elsewhere, others not.[33] It might take quantum information science 10 or 20 years to be taken seriously again, and when it came back, it might be in a very different form. This is the *quantum winter* scenario, based on the "AI winters" of the mid-1970s and the late 1980s.

We think that this is a real risk. Quantum sensing is already paying off, so there are clear reasons to believe that some investments in quantum technologies are a good bet. But while quantum sensors have similar physics requirements to quantum computers in terms of controlling noise and managing materials, quantum sensors do not run algorithms the way quantum computers do. Some skills from quantum computing are transferable, others not.

There are also strategies governments can pursue to lessen the consequences of a bad technology choice:

1. Governments can invest in basic quantum research, rather than applied research, development, or marketization. This is because the basic challenges in quantum technologies are so great and we are so early into their development. In classical computing, the transistor is the basic technology used to create bits, and that technology scaled dramatically from the 1960s, with transistors getting smaller, chips getting larger, and the number of transistors per chip increasing geometrically (not exponentially!) over time. But the basic idea of silicon-based transistors has not changed. Contrast that with quantum computing, where no consensus has emerged for the fundamental qubit technology, in part because scaling is so much more difficult when scale requires control over quantum-level phenomena. Basic research to find the transistor-like invention for quantum states does not bet on any single technology, and if successful, will revolutionize the field.

2. Governments can pursue diverse research and development efforts. Because the fundamentals of quantum computing are so uncertain, government money is better spent funding smaller,

[33] Consider the Japanese Fifth-Generation computing project, one that started in 1989 to develop artificial intelligence and that sought to make breakthrough gains in natural language processing. The Japanese project is considered a failure; even mid-project stream reviews of the project were disappointing. The one main benefit of the project seems to be the training of Japanese people in computer programming, a field that the nation was considered to be behind in at the time.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

more innovative projects that are high-risk, high-reward, and ultimately less likely to produce workable systems. Placing many bets on different breakthrough approaches might result in winning the quantum computing technology lottery. If the lottery is lost, it still provides training opportunities for multidisciplinary researchers who could bring diverse insights to the winning technology.

Market-leading companies such as Google, IBM, and Microsoft have immense amounts of cash on hand, and incentives to develop quantum technologies as quickly as they become financially viable. These companies can decide to spend their treasure to pursue quantum computing, and they can pull back if they believe that the market is premature. (Nathan Rochester, an IBM research scientist, was one of the organizers of the 1956 conference on artificial intelligence.[34] But after IBM received negative publicity for its research into AI, Rochester was directed to other tasks.)

We believe that it is too early to bet on a specific physical medium for quantum computing. At present, the risk of locking in to a specific quantum technology seems low, and none of the current technologies may be the one that ultimately carries the day. Indeed, as the National Academies report states, no technological approach currently demonstrated can scale to a fault-tolerant quantum computer.[35]

3. Governments are better positioned to evaluate the implications of international collaboration for their national security and overall global stability than are multinational corporations. Government regulators and policymakers have access to information obtained from many non-public sources, are able to plan using longer timescales, and have a wide range of tools available to realize their policy goals.

Current industrial policy is tilting towards the East/West bloc scenario we present in Section 8.4 (p. 361), where nations choose sides and pursue research efforts independent of each other. This stands in opposition to other grand-scale science projects, such as the

[34] McCarthy et al., “A Proposal for The Dartmouth Summer Research Project on Artificial Intelligence” (1955).

[35] Grumbling and Horowitz, *Quantum Computing: Progress and Prospects* (2019).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Large Hadron Collider (LHC) built by the European Organization for Nuclear Research (CERN), or the ongoing attempt to create a workable fusion reactor at ITER, the International Thermonuclear Experimental Reactor (a collaboration that includes China, India, Japan, Russia, South Korea, and the US).

One compelling reason to continue an individual nation approach is that unlike the LHC and ITER, quantum technologies do not require massive engineering efforts, the retraining of significant numbers of workers, or thousands of workers with hard hats. Both the LHC and ITER are projects that only rich nations can afford. In quantum computing, startup companies relying only on private funding are able to assemble NISQs.[36]

Another compelling reason is that, unlike the LHC and ITER, a successfully realized quantum computer would immediately have implications for national security and intelligence gathering efforts.

Perhaps the deeper industrial policy concern surrounds betting on QIS at all, instead of putting more money into artificial intelligence powered by classical computers or some kind of new approach for organizing electronic computation, such as the Fujitsu "quantum-inspired" digital annealer.[37] Much like the first 60 years of nuclear fusion research, quantum computing is a field where its advocates predict that fundamental advances are at hand, yet these advances remain, like the Chimera, on the horizon but out of reach.

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. Satellite networks also enable quantum communications, and a number of competitors are attempting to make worldwide broadband systems through low-earth-orbit mini-

[36] The startup company Rigetti required less than $100 million in funding to develop its 19-qubit superconducting "Acorn" system in 2017. By 2020, Rigetti offered "Aspen-8," a 31-qubit superconducting system, connected through Amazon's cloud. As of this writing, Rigetti accomplished all of this with only $174 million in funding, just $8 million of which came from a US government source (DARPA).

[37] Aramon et al., "Physics-Inspired Optimization for Quadratic Unconstrained Problems Using a Digital Annealer" (2019).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

satellites. The choice of physical infrastructures for communications will lead to long-term policy consequences surrounding access to and control over communications.[38]

9.3 Education Policy

Public policy can be shaped to realize quantum goals, but no matter the goal, human capital is necessary.

National governments can increase the availability of human capital through education policy, training programs, tax credits, and even immigration policy. Of these, education is among the slowest but potentially the most effective in the long term.

9.3.1 Graduate Training in QIS

Most academic research in Western nations is performed by graduate students pursuing doctorates under the guidance of a faculty advisor. Thus, the number of graduate students pursuing doctorates in QIS is as critical as the availability of funding: without the supply of students who can work at all hours of the day and night, explore new ideas, and immerse themselves in new possibilities, money spent on basic research is frequently money wasted. One of the best ways to measure productivity of graduate students as a group is to count the number of dissertations and theses published each year.

We searched ProQuest Dissertation and Theses Global seeking QIS-related graduate research output[39] and found 10 242 results in March 2021.[40]

In examining graduate output over time, there is clearly a steadily increasing number of students training in QIS-related areas (Figure 9.2).

[38] Musiani et al., *The Turn to Infrastructure in Internet Governance* (2016).

[39] The search expression used was: `(noft(quantum) AND (noft(compu*) OR noft(communic*) OR noft(sensor OR sensing) OR noft(entangle*) OR noft(superposition) OR noft(``cloning theorem'') OR noft(wave AND particle)))`. That is, the search was limited to the term quantum plus a technology or quantum effect, such as superposition appearing in the title, abstract, or keywords (full text was excluded).

[40] "ProQuest Dissertation and Theses Global is the world's most comprehensive curated collection of dissertations and theses from around the world, offering 5 million citations and 2.5 million full-text works from thousands of universities all over the world." ProQuest claims, "PQDT Global includes content from more than 3000 institutions all over the world." See "ProQuest Dissertations and Theses Global" (n.d.).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

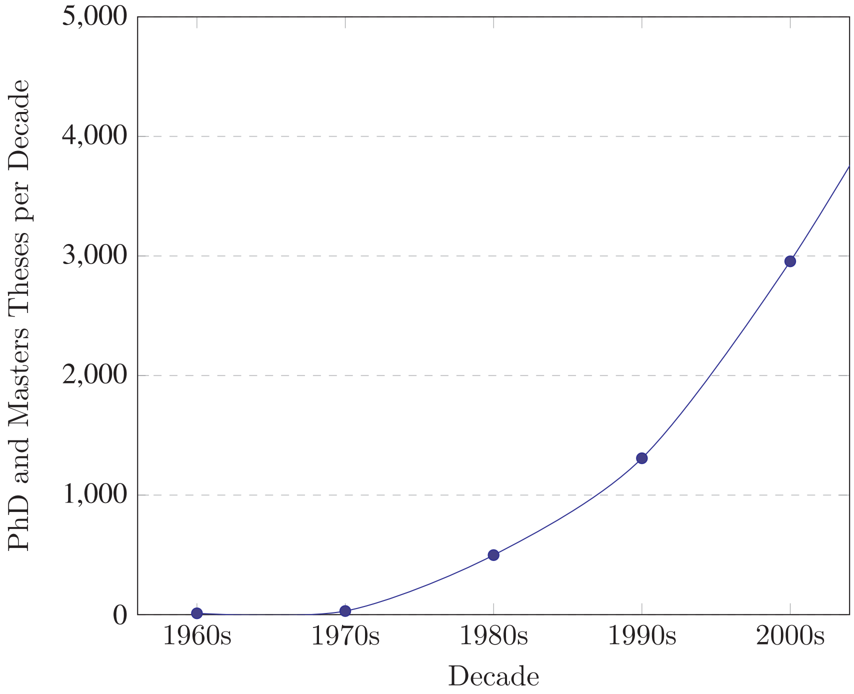

Figure 9.2. Graduate research output in QIS

ProQuest also produces subjects related to the graduate work. Here are the subjects associated with the corpus of quantum-related graduate output, as shown in Table 9.1. The disciplines represented also signal how difficult it would be to form a credible quantum information science academic department. Such a department would have to unify and ensure rigor amongst chemists, computer scientists, electrical engineers, and physicists just to cover the most popular disciplines in QIS represented with more than 150 works. Below that threshold, many other disciplines emerge, from astrophysics to information theory to music theory.

The ProQuest data also help us understand where graduate students are training. As suggested by Table 9.2, US institutions have a strong lead in QIS. Even work being performed outside the US is largely being written in English (Table 9.3). And while academic institutions broadly collaborate, they also compete fiercely; Table 9.4 indicates who is currently on top in the race for academic quantum superiority.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Table 9.1. Subjects associated with QIS graduate theses and dissertations (limited to subjects with more than 100 works)

Subject	Number of Works
Electrical Engineering	1591
Optics	1214
Quantum Physics	940
Physics	894
Condensed Matter Physics	836
Theoretical Physics	742
Atoms and Atomic Particles	720
Computer Science	682
Condensation	662
Chemistry	652
Materials Science	632
Particle Physics	568
Mathematics	463
Physical Chemistry	441
Nanotechnology	294
Inorganic Chemistry	202
Nanoscience	179
Molecules	176
Organic Chemistry	175
Analytical Chemistry	160
Nuclear Physics	152
Chemical Engineering	148
Biochemistry	137
Mechanical Engineering	137
Computer Engineering	136
Biophysics	132
Astronomy	128
Electromagnetics	124
Applied Mathematics	114
Astrophysics	111
Engineering	108
Total	13 650

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Table 9.2. Nations and number of QIS theses and dissertations

Nation	Number of Works
United States	6494
England	1249
People's Republic of China	1053
Canada	536
Scotland	201
Sweden	88
Hong Kong	66
Northern Ireland	55
Germany	47
Finland	34
Wales	34
Ireland	29
Netherlands	26
Republic of Singapore	24
Switzerland	23
Total	9959

Table 9.3. Nations and number of QIS theses and dissertations

Language	Number of Works
English	8963
Chinese	1039
French	29
German	14
Spanish	4
Dutch	3
Polish	3
Afrikaans	1
Catalan	1
Finnish	1
Total	10 058

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Table 9.4. Institutions with more than 100 dissertations and theses published on QIS

Institution Name	Number of Works
Massachusetts Institute of Technology	253
University of California, Berkeley	225
University of Oxford	198
University of Illinois at Urbana-Champaign	176
Purdue University	165
University of California, Santa Barbara	159
Princeton University	156
University of Maryland, College Park	156
Harvard University	148
University of Cambridge	144
University of Toronto	138
Stanford University	121
Northwestern University	118
University of Michigan	117
Cornell University	111
California Institute of Technology	110
Tsinghua University	110
Imperial College London	109
The University of Texas at Austin	108
University of Rochester	105
University of Colorado at Boulder	103
The University of Wisconsin - Madison	101
Total	3131

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

We can derive several observations from these tables. First, research in quantum technologies is attracting attention in many nations and regions. Second, despite the strategic advantages made possible by quantum technologies, a healthy amount of research is being openly published. Indeed, nations and individual scientists are competing for prestige with their quantum research portfolios. Finally, while quantum publications are emerging from many nations, most graduate training in the field is in US institutions. All three of these observations should inform the policy discussion on industrial policy, immigration, and secrecy.

Education policy interacts with immigration policy. Many US graduate students in science and engineering fields hold temporary "student" visas. These students do not automatically qualify for permanent residence upon graduation under current US policy. Instead, the graduating students must return to their home country unless they can find an employer to sponsor the graduate for one of the limited number of H-1B visas. Such a policy might make sense for disciplines in which there is a surplus of graduates, such as PhDs in English or Art History, but seems short-sighted in science and technology – unless the purpose of the policy is to train students in the US and then send them home to seed high-tech hubs in China and India.

According to the National Center for Science and Engineering Statistics at the National Science Foundation, between 1999 and 2019 the number of doctorates granted in science and engineering fields rose from 25 997 in 1999 to 41 519 in 2019. At the same time, the number granted to temporary visa holders rose from 7500 (28.8 percent) to 15 801 (38.1 percent).[41]

In Computer Science, Computer Engineering, and Information Technology the numbers are even more lopsided. According to the 2019 Taulbee survey, 60.4 percent of the PhDs awarded in 2019 went to "nonresident alien students."[42] (For comparison, the survey found that only 13.2 percent of bachelor degrees were awarded to nonresident aliens.) Sadly, the Taulbee survey does not separately recognize quantum computing as a computer science specialization.

The Taulbee surveys tell us how many of these newly minted nonresident PhDs manage to stay in the US, or return to the US at some

[41] National Center for Science and Engineering Statistics, *Doctorate Recipients From US Universities* (2019).

[42] Zweben and Bizot, *2019 Taulbee Survey* (2019), p. 10.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

later point, but it does give us an upper bound. The Taulbee survey asks the fields, economic sectors, and geographical areas where graduates get their first job, but only has data for 1362 of the 1860 graduates. Of those, 7.5 percent find their first job "outside North America." But given that employment type and location is unknown for 26.8 percent of the cohort, it is likely that many of these graduates couldn't be reached because they had already left the country. So as many as 34.3 percent may find their first job after graduating with a US doctorate in the service of the country's economic competitors.

9.3.2 The Human Capital Challenge

In 2015, the European Commission estimated that only 7000 people were working on QIS *worldwide.*[43] Presumably, if a quantum technology virtuous cycle takes hold, many more people will be needed to invent, research, design, program, test, market, and deploy quantum technologies.

The US can stay ahead on quantum technologies 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 technologies for team USA. That is, solving the human capital challenge requires integration between education policy, export controls, and immigration policy.

Immigration is an important part of the human capital equation because the skills are in short supply, the time to create a quantum PhD, postdoc or assistant professor is long, and these people are highly sought after. Absent restrictive emigration policies, some human capital will flow between nations – both for research fellowships lasting a few years, and permanently.

One need only look at the biographies of those working on quantum projects to see that quantum information science is staffed with experts from around the world. The esoteric, multidisciplinary skillset and focus on difficult-to-grasp quantum mechanics concepts is a rare fit for job applicants.

In the US, uncharitable immigration laws combined with government policies that are increasingly hostile to aliens and immigrants have the potential to create a "brain drain"[44] that might push quantum scientists and engineers to countries such as Canada, Germany,

[43] Omar, "Workshop on Quantum Technologies and Industry" (2015).

[44] Moller, "How Anti-Immigrant Policies Thwart Scientific Discovery" (2019).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

or the Netherlands. These countries heavily support quantum technology research and offer high-quality of living.

When we interviewed him about IBM's quantum computing research within the US, Dr. Robert Sutor, who was then the vice president for Q Strategy and Ecosystem at IBM Research, made it clear to us that there is no US strategy: there is a single IBM strategy, and it is international. "All we can really say there is that we have teams working on Quantum. If you look at the papers, you can follow the addresses. It's primarily in the US, in New York, in California at our Alamaden Lab, in Japan, in Switzerland, in Zurich. We do have a couple of people here and there, but everybody in the countries that I mentioned are working together," Sutor said.

Indeed, even within the US, he said, IBM's team is an international one. "More than half the people at IBM, at last count, are from outside the US We get people from all other countries."

One might think that China has the raw population numbers to find domestic talent that checks all the boxes. But even scientists in China rely on international collaborators. China's "father of quantum," Jian-Wei Pan, wrote to us that "Over the past decade, my laboratory in China has received more than 20 international students and visiting scholars from the United States, Canada, the United Kingdom, Germany and other countries…As a physicist who has been devoted to quantum information research for 20 years, I would like to emphasize that quantum information technology has a long way to go before it can be widely used. Active international cooperation and open exchanges are imperative."

We believe that nations that wish to succeed in quantum technology will be pushed to adopting liberal immigration policies that ease administrative burdens when it comes to short-term visits for conferences and other scientific and technical exchanges, medium-term visits lasting up to two years for extended bouts of collaboration, and easily obtainable residency for an indefinite period – what the US calls a "green card." The human capital market will select against countries with more restrictive policies.

9.3.3 Faculty Research Incentives

The intricate engineering and resource intensity of building a quantum device is significant. Some scientists we spoke with signaled that their full ambitions were difficult to realize because the need to

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

spend time building a device competed with teaching, service, and even publication expectations.

In fact, part of the requirements for building quantum devices seems to be the creation of intermediate steps that provide publication opportunities. In the National Science Foundation's 2019 workshop on quantum simulation, for instance, a consensus statement valorized the approach of creating experimental simulators that in themselves were worthy of study.[45] The timeline suggested would keep faculty publications coming as expected.

Universities are in competition with private companies and research labs to make discoveries in QIS. In fact, universities are in competition with their own faculty, in a way, because so many faculty form private companies to supplement their basic science work free from institutional red tape, to spend money while avoiding rules and competitive bidding requirements, to hire and keep their brightest students, and of course to make more money. Universities might benefit from creating more research professorships to give faculty time to develop quantum devices free from other responsibilities. Universities should also have policies that discourage or prohibit faculty from hiring students prior to the student's graduation, as such business relations between faculty and their students present many opportunities for conflicts of interest. (For example, MIT's Policies and Procedures generally prohibit faculty from hiring their students at the faculty's startup, for example.[46])

A separate question concerns whether educational institutions should create quantum information science departments. Table 9.5 demonstrates why department creation is a challenge: quantum technologies draw from so many different, well-established disciplines that unifying them in a single department presents quality and rigor-control challenges. Theoretical physicists, for instance, might not feel prepared to evaluate colleagues from materials sciences or applied science fields and vice versa. This disciplinary diversity explains why so many institutions have pursued academic "center" models that leave faculty in their home departments while providing support for collaboration across relevant fields.

[45] Altman et al., "Quantum Simulators: Architectures and Opportunities" (2019).

[46] MIT, "Outside Professional Activities" (2018).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Table 9.5. Fields associated with quantum technology

Field	Number of Papers
Optics	3780
Physics Multidisciplinary	3737
Physics Applied	2297
Physics Atomic Molecular Chemical	2182
Engineering Electrical Electronic	1873
Computer Science Theory Methods	1527
Physics Mathematical	1314
Quantum Science Technology	1261
Materials Science Multidisciplinary	1202
Physics Condensed Matter	1168
Multidisciplinary Sciences	1079
Computer Science Information Systems	597
Nanoscience Nanotechnology	585
Telecommunications	476
Physics Particles Fields	446
Chemistry Physical	429
Computer Science Artificial Intelligence	412
Chemistry Multidisciplinary	377
Computer Science Hardware Architecture	360
Computer Science Interdisciplinary Applications	269
Computer Science Software Engineering	244
Mathematics Applied	242
Automation Control Systems	158
Mathematics	135
Engineering Multidisciplinary	100
Total	26 250

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Education Pipelines

Over the longer term, the US and other nations would be wise to build in quantum physics to grade-school curricula. Such an approach could both grow the number of students exposed to quantum physics and help diversify potential candidate pools for the workforce. In 2020, the National Science Foundation and the White House Office of Science and Technology Policy created a partnership anchored at University of Illinois Urbana-Champaign and University of Chicago to promote K–12 education (see the sidebar "Key QIS Concepts for K–12 Students" on page 412). Called Q2Work, the group will develop online educational material and modules for in-person learning, presumably so that these will diffuse to school systems. The partnership includes participation from big players in quantum computing, including Google, IBM, Microsoft; DIB companies Boeing and Lockheed Martin; and startups Rigetti and Zapata.

Q2Work builds upon a NSF workshop that defined key quantum information science concepts to be taught in schools. The workshop output, a high-level, five-page summary, "Key Concepts for Future Quantum Information Science Learners," reflected input from leading QIS researchers, and teachers and officials from public and private schools. We note in Appendix A that without training, people may be familiar with how everyday objects behave, but will have little intuition about how angstrom-sized objects behave. Education in the K–12 years could start developing that intuition. Yet, basic questions about QIS education in schools are still unanswered. For instance, what learning goals are appropriate for grade and secondary school students? What do we expect the average student to be able to do with the knowledge? What advantages and risks come from reforming education so that it is QIS-first, for instance, by teaching quantum mechanics before classical mechanics?

9.4 National Security and Quantum Technologies

Quantum technologies can give nations strategic advantages. This section focuses on how nations might consider the advantages and disadvantages of export control and other tools to hinder adversaries' development of quantum technology. The section then turns to other limits and dynamics implicated by quantum technologies: the effect on nation-state competition in space and in cyberspace.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Key QIS Concepts for K–12 Students

A March 2020 NSTC/NSF workshop produced the following high-level concepts for teaching QIS in K–12 schools.[a]

1. Quantum information science (QIS) exploits quantum principles to transform how information is acquired, encoded, manipulated, and applied.

2. A quantum state is a mathematical representation of a physical system, such as an atom, and provides the basis for processing quantum information.

3. Quantum applications are designed to carefully manipulate fragile quantum systems without observation to increase the probability that the final measurement will provide the intended result.

4. The quantum bit, or qubit, is the fundamental unit of quantum information.

5. Entanglement, an inseparable relationship between multiple qubits, is a key property of quantum systems necessary for obtaining a quantum advantage in most QIS applications.

6. For quantum information applications to be successfully completed, fragile quantum states must be preserved, or kept coherent.

7. Quantum computers, which use qubits and quantum operations, will solve certain complex computational problems more efficiently than classical computers.

8. Quantum communication uses entanglement or a transmission channel. to transfer quantum information between different locations.

9. Quantum sensing uses quantum states to detect and measure physical properties with the highest precision allowed by quantum mechanics.

[a] Alpert, Edwards, and Freericks, *Key Concepts for Future QIS Learners* (2020).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

9.4.1 Export Controls

According to the US International Trade Administration, “The United States imposes export controls to protect national security interests and promote foreign policy objectives. The US also participates in various multilateral export control regimes to prevent the proliferation of weapons of mass destruction and prevent destabilizing accumulations of conventional weapons and related material.”[47] US export controls are administered by the Bureau of Industry and Security (BIS) within the US Department of Commerce.

Export controls and other approaches for preventing the spread of advanced technology can be effective in the short term, but in the long term they can inadvertently create independent foreign tech ecosystems that are resistant to any controls. Three illustrative cases are the US Global Positioning System (GPS), the US attempts to regulate the export of cryptographic technology, and the proliferation of nuclear weapons.

GPS

Originally developed by the US military, for military purposes, at an inflation-adjusted cost of $14 billion, the Global Positioning System (GPS) is now available to the public freely.[48] Over the course of two decades, the US launched the GPS constellation, with Europe following with the Galileo network, Russia with GLONASS, the Japanese with the Quasi-Zenith Satellite System, which enhances the resolution of the US system, and India with the Indian Regional Navigation Satellite System (IRNSS).

Reflecting US concern that a high-precision location service might be used by its enemies, the original GPS system had two tiers of service. The US military received an encrypted, highly accurate service. The unencrypted service had noise intentionally added, a practice that the US called “selective availability.” Industry found ways around selective availability, and the lower quality helped spur interest in the Russian and European alternatives. In response, President Clinton ended selective availability in 1990, meaning that civilians can reliably obtain a signal accurate within 4 m, with the military and other users obtaining greater accuracy through capturing more signals or by augmenting the GPS data. Unencumbered civilian use

[47] International Trade Administration, “US Export Controls” (2021).

[48] Posen, “Command of The Commons: The Military Foundation of US Hegemony” (2003).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

of GPS 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.[49] American companies dominate the Internet in important sectors, even overseas, where usage rates of Google Search exceed those of domestic competitors created to fend off the American company. The situation is different in China, where direct blocks on American internet services combined with more significant language differences allowed the country to develop its own domestic internet ecosystem.

Quantum Technologies and Export Control

Should quantum technologies, to the extent it is possible, be open for similar public use and extension? This question relates to the above-discussed industrial policy issues. Industrial policy often seeks to benefit domestic companies, in an attempt to reach technological sovereignty. If quantum technologies are sufficiently open, no one country is likely to dominate the field.

In the US, several quantum technologies, particularly quantum sensors, and their precursors are already subject to export controls.[50] Under the Trump administration, the US retained a market proscription posture, and funding models that make it easier for the government to restrict openness of research outputs. 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 Export Control Reform Act of 2018.[51] This initial regulatory exploration suggested that quantum sensing,

[49] Clark, *Designing an Internet* (2019).

[50] The US has traditionally followed a policy making applied research subject to more restrictions than basic research. "It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted." "'Fundamental research' means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons." National Security Decision Directive 189 (1985).

[51] Department of Commerce, Bureau of Industry and Security, "Review of Controls for Certain Emerging Technologies" (2018).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

computing and encryption are "foundational technologies," indicating that they are "emerging technologies that are essential to US 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 Department of Commerce sought how to define and thus bound the definition of quantum technologies so that identifiable products could be included on an export control list. Initial reporting suggested a narrow set of restrictions, yet one technology identified as possibly controlled is the "quantum diluted refrigerator," a device used to supercool some quantum devices with helium (see the sidebar "The Helium Challenge" on page 251).[52] For this reason, national competitors may be dependent on foreign makers of low-temperature devices. Companies such as Cryomech (New York based), Sumitomo (Japan), Oxford Instruments (UK), and Bluefors Oy (Finland) all offer helium coolers, while some competitors offer low-kelvin devices that do not use a cryogen (a cooling agent such as liquid helium or liquid nitrogen). Presumably export control of dilution refrigerator devices will hinder China and Russia in their efforts. Yet, competitor nations can build their own domestic cryogenic industries, or rely on devices already circulating in the market. As early as 2012, the Cryogenic Society of America claimed on its website that "Dilution refrigerators are a common technique for reaching temperatures below 1 K … reliable dilution refrigerators are in fact a commercial product and can be purchased as turnkey systems from vendors." IBM is creating its own custom supercooling device in anticipation of building a large superconducting machine. If a single private company can build a cooler, it would seem not to be much of a challenge for other nations.

European governments generally approach quantum technologies as something that should be relatively open. The €1 billion European initiative to promote quantum technologies explicitly embraces openness, calling for "end-user-inspired applications" in quantum networks and inclusion of quantum random-number-generation-based encryption in even "cheap devices."[53] The European posture sug-

[52] Alper, "US Finalizing Rules to Limit Sensitive Tech Exports to China, Others" (2019).

[53] European Commission, High Level Steering Committee, DG Connect, "Quantum Technologies Flagship Final Report" (2017a).

gests support for an end-to-end quantum internet for the average person to use. This anti-surveillance interest also aligns with a series of high court opinions in Europe that object to intelligence gathering on European citizens by American agencies.

It is unclear what posture China will take toward openness of quantum technologies. Chinese scientists are publishing their work in top journals and are genuinely interested in engagement. However, national competition between the US and China has led both companies to discuss and implement economic *decoupling* policies, that is, deliberate strategies to separate technology supply chains from other nations. For instance, US policymakers have made a priority of removing China-made Huawei equipment from domestic and even foreign telecommunications networks. At the same time, China is creating domestic industries, such as helium capture plants, to address gaps left from decoupling.

At the moment, it would seem that both the US and China would lose in a decoupling scenario. US domestic manufacturers of quantum components and optics sell their wares to a large foreign market. For instance, examining Jian-Wei Pan's Jiuzhang device reveals it to have an astonishing number of components from US-based Thor-Labs and from Israel-based Raicol Crystals (see Section 6.7, p. 250)). America will lose out on those high-precision manufacturing sales as China in-sources technology manufacturing. Conversely, as decoupling intensifies, we should expect more explicit export control to prevent Chinese-developed and -manufactured technologies from diffusing into the US and Europe.

This discussion makes it clear that rather than asking whether governments should export-control innovations in quantum technologies, one should begin by considering whether it is even possible. Imposing export controls will have different implications for our categories of quantum technologies. In metrology, interferometry is already widely dispersed, indeed many of its applications were demonstrated by European investigators. Jian-Wei Pan's Jiuzhang quantum computer is a masterful implementation of interferometry (see Section 6.6, p. 243). Some sensing technologies can be miniaturized in part because they lack supercooling requirements, thus making controls practically more difficult. Quantum computing 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 in the near future.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Adding to the market proscription complexity is that private companies play lead roles in quantum communication and computing development. Yet, there are ways to bring private companies into the fold and make it difficult for them to diffuse discoveries to potential adversaries. The Trump administration strategy was to encourage private sector participation, including financial outlays from the private sector, with government research money vested in Department of Energy Labs. In August 2020, the Trump administration allocated over $600 million in funding to five national labs, with over $300 million in commitments from academic and industry companies. These private-sector partners include many of the recognized leaders, including IBM, Microsoft, Intel, Lockheed Martin, and Rigetti. Notably absent is Google, and its absence is not for a lack of merit. Google and other companies may be avoiding government entanglement so as to keep its inventions in the public sphere.

The Energy–labs centered approach signaled that the Trump administration was taking a market prescription strategy, by funding companies lavishly and aligning incentives to keep the technology restricted to domestic actors. This has elements of the longtime domestic defense firm practice of "paternalistic socialism."[54] Interestingly however, this strategy is limited in efficacy. Despite efforts to keep domestic aerospace firms well sated, these same firms often pay large fines for export violations.

The capture of industry through the military embrace approach is becoming more complex with the rise of the power of the private sector. Most quantum technology companies are located in liberal, Western democracies, and many already have military funding in the form of leased computer time or purchases of devices, or they are angling for it (for instance, by having former high-level military officials on their boards).[55] Many technology companies are depen-

[54] Paternalistic socialism is where the government spreads money around several competitors to ensure that America has multiple options for companies to hire for projects. Rich and Janos, *Skunk Works: a Personal Memoir of My Years at Lockheed* (1994). Particularly in aerospace, the need for government patronage of the private sector is explicit: "the development in the United States of a dynamic and innovative private-sector space industry will be indispensable to future US space leadership." Independent Working Group on Missile Defense, *Missile Defense, The Space Relationship, and The Twenty-First Century: 2009 Report* (2009).

[55] Rigetti Computing's board features three PhDs, the obligatory representative from a venture capital funder, and a former chair of the Joint Chiefs. ColdQuanta

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

dent on military investment; some seem to abhor this investment. For instance, in 2018, Google employees objected to "Project Maven," an effort to improve the object recognition capabilities of the Department of Defense.[56] Google is widely agreed to be among the leading companies in the quantum computer research space. Will its employees forgo military markets for quantum technologies, many of which have no other obvious buyer than governments? Google's closest rivals in the quantum technology space, IBM and Microsoft,[57] both have extensive government consulting practices and are unlikely to turn away from military and intelligence services.

Theft is an additional complexifier. Nations that follow others in technical might can develop their own quantum programs, but it is probably easier to copy the leader. Cybersecurity vulnerabilities are among the newest ways that competing nations have lifted secrets from American companies, and in some instances, companies have lost huge portions of their intellectual property portfolios to attackers. There is no reason to believe this will not continue. In academia as well, thefts of secrets occur, but also bribery which is masked as scholarly accolades. The Chinese government in particular has bought access to American scientists through its Thousand Talents programs, where faculty members receive what appear to be prestigious honors (often accompanied by money) for collaboration with Chinese institutions. In recent years, faculty members have been targets of criminal prosecutions for pursuing these relationships while not disclosing "honoraria" to their own institutions and the US government.

Tools for Controlling Quantum Technology Proliferation

The US and other nations have several tools to block diffusion of technology. For inventors seeking a patent, the government has a broad power to impose secrecy on the invention, even if the inventor

has a strategic board with former officials from several intelligence agencies.

[56] Unnamed Google Employees, n.d. Project Maven had clear implications for the unmanned air vehicle 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 commercially focused 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 is easily deployed for ISR or offensive purposes.

[57] B. Smith, "Technology and The US Military" (2018).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

is a private person. Outside the patent system, government can use export controls to bar sales and services.

Patent secrecy may be an attractive option to prevent diffusion of quantum technologies, Under the Invention Secrecy Act, the federal government has broad powers to force secrecy of an invention if its publication is "detrimental to the national security."[58] The Federation of American Scientists tracks secrecy orders under the law, and finds that almost 6000 patents are subject to secrecy orders. Most of these pertain to government-funded inventions, but in any given year, a few dozen "John Doe" secrecy orders are imposed on private citizens or companies that independently sought patent rights in a sensitive technology. The Act provides for criminal and civil penalties, and those who disclose the secret patent "abandon" it under the statute, thereby losing any economic benefits of the invention.

One might think that patent secrecy orders primarily deal with nuclear bomb-making plans and the like,[59] but the scope of inventions that could be detrimental to national security is seen as much broader. The Federation of American Scientists' Steven Aftergood has obtained summary statistics and identifiers of formerly secret patents. Conventional weapons building and targeting systems appear in many formerly secret patents. Patent secrecy orders concern stealth aircraft countermeasures, radar resilience, anti-radar technologies, and encryption. Quantum technologies will likely contribute to these same fields, making quantum technologies likely targets of secrecy orders.[60]

But what about sensitive, non-nuclear technologies that are sold directly as goods or as services? The government has three primary controls for such technologies. These controls can be focused on technologies, individual firms, and nation states.

The Department of Commerce's Bureau of Industry and Security owns the Export Administration Regulations (EAR), which focus on

[58] Secrecy of certain inventions and withholding of patent, 35 USC § 181. Consulted agencies include the Department of Defense, Department of Justice, NASA, Department of Energy, and the Department of Homeland Security.

[59] A separate provision of the US Code creates criminal penalties for disclosure of atomic weapons design-and-manufacture information if the person has "reason to believe such data will be utilized to injure the United States." This is the "born secret" provision of US law, 42 USC § 2274.

[60] If a secrecy order is rescinded, a patent does not explicitly state that it was subject to an order. However, secret patents sometimes have a filing date that precedes an issuing date by decades, hinting that it was subject to suppression.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

control over export of dual-use technologies. Dual-use technologies are those that have both commercial and military uses, and these are broadly defined to include commodities but also software. Thus, allowing a download of software, even in the US, to a foreign person could be an “export.” The Department of Commerce’s Commerce Control List (CCL) identifies a lengthy list of controlled technologies; those listed cannot be transferred to or through certain countries without a license.

Several quantum technologies are explicitly identified in the CCL, including superconducting quantum interference devices (SQUIDs) of a certain resolution, gravimeters, quantum wells, quantum cryptography, and post-quantum cryptography. The CCL also identifies precursors to quantum computing, encryption, and sensing technologies to stop their spread to designated nations.

The Department of State oversees the International Traffic in Arms Regulations (ITAR), which blocks the transfer of military-related technologies, and information about their design, to non-US persons. The transfer carries civil and criminal penalties, on a strict liability basis (many violations of the regime do not require ill intent). Almost all the dominant US defense firms have paid fines or settlements for ITAR violations, and these are large, often in the eight-figure range.

Keying a violation on transfer to non-US persons means that sharing technical data, even inside the country, can be a violation if the recipient is a foreigner. This means that foreign (defined as people lacking permanent residence) graduate students and employees have to be excluded from ITAR-regulated projects (absent special permission). ITAR does not apply to public domain information, which includes research performed at universities that is intended for publication. This would seem to be a large loophole that gives researchers significant freedom. However, as explained above, only a small amount of research in quantum technologies is funded by private foundations. Most flows through the NSF, Department of Energy Laboratories, and a panoply of Department of Defense agencies that can condition work on these sponsored projects to be in compliance with ITAR.

A wide set of technologies related to quantum sensing and communication fit under ITAR’s “United States Munitions List,” an enumeration of technologies that is now over 33 000 words in length. Many quantum technologies fall under the current munitions enu-

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

meration because the broad categories include sonar and radar technologies, quantum clocks, gravimeters, communications systems that are difficult to intercept, cryptographic and cryptanalytic systems, and computer systems for modeling weapons.

Companies need to carefully monitor ITAR restrictions to understand the rules for technologies that really can only be made in America. Policymakers too need to monitor the commercial landscape because if foreign firms can create quantum technologies and are willing to sell them to designated nations, ITAR restrictions make the US less competitive. The most recent example of this phenomenon came in satellite technologies, where ITAR restrictions on US firms enabled foreign companies to capture a significant share of the space market.[61]

Finally, under federal law, the President has a sweeping power to declare emergencies in peacetime that, in turn, enable declaration of sanctions and other interventions to shape economic activity.[62] Over two dozen such emergencies are currently declared, with some identifying broadly scoped, potentially worldwide emergencies, such as weapons proliferation, transnational criminal activity, and the scourge of cyber-related intrusions and influence. The Department of the Treasury's Office of Foreign Assets Control (OFAC) oversees the primary mechanism used to block economic transactions under the declared emergency. This agency is charged with enforcing trade sanctions and other international relations policy positions through economic deterrence.

OFAC does so through the Specially Designated Nationals and Blocked Persons List (SDN). US persons, companies, and, perhaps most importantly, banks, are prohibited from engaging in transactions with any entity in the database. Because of the network effects and surveillance power in international banking,[63] being designated effectively locks sanctioned entities out of mainstream value transfer mechanisms and other businesses.[64] The SDN database is now

[61] Zelnio, "The Effects of Export Control on The Space Industry" (2006).

[62] 50 USC. §§ 1701 et seq.

[63] Farrell and Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion" (2019).

[64] Some wily actors find ways of buying goods despite being designated. For a fantastic case study of SDN evasion focusing on North Korea and Kim Jong-un's acquisition of an armored Mercedes-Maybach S600 Guard, see Kuo and Arterburn, *Lux and Loaded: Exposing North Korea's Strategic Procurement Networks* (2009).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

sprawling. It is used to enforce over 60 trade sanction or policy regimes, including to punish Russians involved in hacking the US elections. The SDN is over 1400 pages long and contains the name Muhammad over 3800 times. Suffice it to say that as a general matter, no quantum technology can be sold to any entity on the list. But more broadly, if quantum technologies are associated with weapons proliferation, for instance the use of quantum computing to simulate more effective biological and chemical agents, the SDN is another tool the government can use to block relevant entities, nations, and people from transactions.

9.4.2 Quantum Technology and Space Law

The seminal Outer Space Treaty of 1967 declares that the use of space will be "for the benefit and in the interests of all countries..." and "exclusively for peaceful purposes." The Treaty further prohibits stationing any weapon of mass destruction in space. But despite that proscription and affirmative obligation for peaceful purposes, nation states have many options for using force in space.

The US military sees the U.N. Charter's inherent right to self-defense language as limiting the exclusively peaceful purposes language. And once the door to self-defense is opened, many "defensive" preparations resemble offensive ones.[65]

There are other loopholes allowing weaponization as well. As Jeremy Rabkin and John Yoo explain in their book analyzing next-generation weaponry and conflict, the treaty does not prohibit ICBMs, as they are not installed in space but rather pass through it.[66] Nor does the treaty explicitly ban intelligence and surveillance activities,[67] even those that support or enhance force in conflict. The treaty

[65] A fascinating 2002 study by RAND signals the US government's interest in and options for space weapons. Celestial weapons are attractive in part because they give nations the ability to attack anywhere on Earth without pesky complications of weather and troop deployment and supply chain concerns. See RAND, *Space Weapons: Earth Wars* (2002).

[66] Rabkin and John Yoo, *Striking Power: How Cyber, Robots, and Space Weapons Change The Rules for War* (2017).

[67] United Nations, *Principles Relating to Remote Sensing of The Earth From Outer Space* (1986). The affirmative command of "peaceful purposes" 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. Consider that a launch-monitoring satellite is key to waging war, but at the same time provides monitoring essential for nuclear peace.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

has not stopped the advance of anti-satellite weapons, including by China[68] and India.[69]

Quantum technologies' utility in outer space is evident. Companies angling for government contracts have often appointed board members and advisors with former leadership roles in Department of Defense agencies with a space focus, such as the National Geospatial-Intelligence Agency (NGA) and the National Reconnaissance Office (NRO). As MASINT becomes more important, NGA and NRO will be key agencies for deployment of quantum technologies.

Quantum technologies also appear to have even more leeway than other military-related activities in space. Even when used in a force-enhancing role, quantum technologies in no way trigger the traditional concerns of weapons regulation, which are indiscriminate or superfluous injury, or of widespread, permanent environmental damage.[70] In fact, these technologies might be de-escalatory, in that they help nations understand adversaries through better intelligence, and in conflict, they may enable more discriminate applications of force.

Quantum technologies may be lawful in space, but they still could change adversaries' strategies. Nations may find it compelling, even necessary, to make first strikes at space-based vessels to silence or blind the handful of superpowers that have both a space program and quantum technology. If *jus ad bellum* requirements (the rules for initiating armed conflict) or rules for engaging in self-defense, are met, it would seem that *jus in bello* considerations (the rules for the actual waging of war) might mitigate in favor of striking at space-faring platforms. This is because targeting satellites could be justified as a discriminate attack on military infrastructure and that does not directly harm people, thus minimizing human suffering, in the sense of injury and death.

Nevertheless, the psychological harm from a satellite attack could be substantial. People, particularly in developed nations so dependent on communications, may panic as uncertainty deepens with normally chatty devices going mute. Another side effect, analogous to the long-term, serious destruction of habitat, may be discounted: attacking space vessels can create clouds of space junk that remain in orbit for years, endangering all space programs.[71]

[68] Kan, *China's Anti-Satellite Weapon Test* (2007).

[69] Brumfiel, "India Claims Successful Test Of Anti-Satellite Weapon" (2019).

[70] Boothby, "Space Weapons and The Law" (2017).

[71] Zissis, "China's Anti-Satellite Test" (2007).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Quantum sensing could be so powerful that a national policy of parallel contingent restraint is appropriate. That is, nations may find it expedient to voluntarily limit where and when quantum sensing is deployed so long as others do so as well. In some cases, 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 terrestrial forbearance, the Antarctic Treaty System prohibits militarization (both offensive and defensive uses) in Antarctica, making it more strictly regulated than outer space.

Generally speaking, intelligence systems are seen by policymakers as providing more context and information to adversaries, and thus, traditionally, espionage has been a tolerated activity of statecraft.[72] As uncomfortable as intelligence systems may make us feel, we have to contemplate that they can make us safer.

9.4.3 Quantum Technology and Cybersecurity

In his discussion of designing a next-generation internet, David Clark recounted how early internet designers relied upon contacts within the intelligence community to model security threats. According to Clark, two salient principles emerged: that endpoints should be the focus of security (because it was hopeless to provide security for the voluminous infrastructure between endpoints), and that endpoint security had to resist nation-state-level determination and ingenuity. The result of these emphases is that there is little trust for confidentiality and integrity "in the network."[73] As a result of this architecture, one does not know whether internet intermediaries are trustworthy, whether they relay information faithfully, or whether they copy or alter data for their own purposes. We use encryption to reduce the risks of intermediary opportunism. Yet, intermediaries

[72] German Chancellor Angela Merkel provides an example of this ambivalence. After documents were released purporting that the US NSA had intercepted her wireless phone conversations, Merkel allowed herself to be photographed holding her phone aloft, in a kind of protest. Less well known is that behind the scenes, Germany has been clamoring to join the US "Five Eyes" partnership with Australia, Canada, New Zealand, and the UK. See Spiegel, "Angela Merkel Eyes Place for Germany in US Intelligence Club" (2013). A follow-up investigation found no evidence that the NSA had targeted her phone.

[73] Clark, *Designing an Internet* (2019).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

can still infer the meaning of messages from monitoring metadata. One might address these problems by routing information differently, but the classical internet makes this difficult. Could quantum networks change the game theory of surveillance?[74] Recall that quantum technologies change communications in two ways: first, quantum key distribution makes it possible to enjoy communications confidentiality and integrity that is invulnerable even to a quantum computing attack. But that is not so different than the situation today, with proper AES or post-quantum encryption. Content is protected, while metadata can be observed.

The second quantum communications change is more consequential: a quantum-entangled communication network would enjoy full end-to-end quantum encryption, meaning that interception (whether by spies or by natural events that interfere with the transmission) will be apparent. In essence, a quantum internet gives its users no need to rely on fraught network trust. How might governments react to that?

One could imagine that governments will double-down on interception, perhaps in the form of creating noisome interference that blocks photonic communication. Having an eavesdropper present could deny communicants the ability to establish a secure session because "listening" would interfere with the quantum states. Eavesdropping might also have a signaling function that has utility in a "defend forward" security posture, one characterized by penetration into third party networks.[75] Currently, such eavesdropping on networks is easy because internet traffic is both copied multiple times and is routed circuitously, sometimes leaving national boundaries, which has legal consequences for its protection.[76] Unless the current infrastructure of the Internet changes, nation states will have many opportunities to physically access fiber optic cables and "listen," even if they cannot understand what is being sent.

On the other hand, QIS could also make the very design of the Internet change, such that the network is more resilient against interception. One could imagine an investment in quantum entangled networks coming with careful planning surrounding the routing of the fiber, and security measures for it. Rather than implement the

[74] Tambe, *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned* (2012).

[75] Springer, *Cyber Warfare: A Documentary and Reference Guide* (2020).

[76] Kerr, "The Fourth Amendment and The Global Internet" (2015).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

system in existing fiber used by others, one could foresee a factionalization of networks, with nation-state controlled, central trunks, much like China's Beijing to Shanghai fiber network.[77] For regions such as the EU and countries like Russia and China, the promise of an interception-resistant channel might make it worthwhile to reroute the physical layer so that it is more controlled and so that one might choose the paths that important data take to avoid likely interception points. Still, if these routes are not defended, nation states might dig up fiber lines and place devices that interfere with quantum states.

Another, likely approach to the hardening of network privacy is to erode endpoint security.[78] That is, to discover ways to degrade the security of end users' devices. As discussed in Chapter 8, 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 through faked software upgrades or other exploits will be able to see all data stored on them. Another network-hardened scenario is that the future of cyberattacks becomes physical, in the sense that spies or crooks simply steal devices from targets at gunpoint. They will ask you to unlock your phone before leaving.

9.5 Quantum Technology and Privacy

Privacy rules, which take the form of constitutional rights, statutory limitations (from the many different sections of the US Code from the criminal law to evidence rules), administrative regulations, to social and business norms, might blunt the kinds of transparency that quantum technologies will provide. This section discusses how we might arrange privacy rules to prevent a quantum technology privacy meltdown.

Military and intelligence technologies tend to devolve to law enforcement and proliferate to nongovernmental actors.[79] Law and custom provide few limits on the kinds of technologies that even local law enforcement can obtain. Recent examples include "eye in the sky" monitoring that can provide moment-by-moment surveillance

[77] Liao et al., "Satellite-Relayed Intercontinental Quantum Network" (2018).

[78] Kadrich, *Endpoint Security* (2007).

[79] Consider the scenario of the "GEOINT Singularity," conceived as "the convergence, and interrelated use, of capabilities in artificial intelligence, satellite-based imagery, and global connectivity, where the general population would have real-time access to ubiquitous intelligence analysis." Koller, *The Future of Ubiquitous, Realtime Intelligence: A GEOINT Singularity* (2019).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

of entire cities, cell-phone-hijacking "Stingray" devices, encryption-circumventing device forensics platforms, and malware that collects secret information from users.

Over time, invasive monitoring equipment finds its way into the private sector as well. A 2017 Rand Corporation market analysis of surveillance systems relying only on unclassified sources found "examples of SIGINT capabilities outside of government that are available to anyone [with applications in] maritime domain awareness; radio frequency (RF) spectrum mapping; eavesdropping, jamming, and hijacking of satellite communications; and cyber surveillance."[80] Such technologies are used by private investigators, stalkers, and employers that tend to see themselves as having a kind of dominion over workers similar to that of parents over children.

We should be prepared for a similar devolution of quantum technology. Military and intelligence agencies are likely to lead the deployment of these technologies. But with time, the same technicians that build, operate, and provide service for military and intelligence actors will naturally cross over to federal law enforcement agencies. Joint federal–local activities will further diffuse quantum technologies. Incentives to grow the marketplace will naturally cause quantum technology companies to find commercial and employment-related uses. Before long, we will have to ask what is to stop the average person from looking into the home of their neighbor. In most people's minds, technical might makes actions right. How can we create norms now to prevent a new era of forced transparency?

9.5.1 Secrets and Their Time Value

All individuals and institutions have secrets. Most of these secrets are only valuable for a limited time. For instance, business strategies might be relevant for a few years, the secret sauce of an invention may only be valuable until competitors figure out how to copy it, and the encryption on entertainment media might only need to be strong enough to protect the movie or music as long as people are willing to pay to enjoy it. Immutable personal facts, such as one's Social Security Number, might need protection for a lifetime.

Turning to secrets of the United States, policy dictates periods of protection for government materials. The Obama administration set

[80] Weinbaum et al., *SIGINT for Anyone: The Growing Availability of Signals Intelligence in The Public Domain* (2017).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

a policy of automatic declassification of agency documents.[81] Many records will be declassified after 25 years, but the policy also envisions longer periods of protection for certain sensitive documents, keyed at classification lengths of more than 50 and more than 75 years. Outside the intelligence field, other secrets are time-limited. Most notably, the US Census keeps individually-identifying information secret for 72 years, meaning that in 2022 the 1950 Census records will be released.[82]

These dates give us some guidance for how we might think about the protections for encrypted data and when the things we write or keep today will lose their sensitivity. Again, if a large quantum computer is built, economics dictates that most owners of the device will make more money synthesizing chemicals and materials than cracking old messages. But cryptanalysis is a real risk among governments, which will carefully task the highest-value keys in their attacks. Owners of sensitive information must consider the time value of data, along with the proposition that the first quantum computers will be large machines owned by large companies and governments, but over time, the technology will shrink, become less expensive, and be democratized. These risks are unlikely to be realized in the next decade, but 20 to 50 years from now, quantum cryptanalysis could be a much larger risk.

9.5.2 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 technologies. To start with, practically speaking, because quantum computers are so expensive to build and maintain, the technology will not be democratically distributed for some time. 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 decryption efforts. There are economic constraints too. Companies will want to capture profits from the devices, and there will be

[81] President Barack Obama, "Classified National Security Information, E.O. 13526" (CFR2010).

[82] In the meantime, to maintain its confidentiality duties, the US Census releases datasets processed in some way to prevent reidentification of individuals in the enumeration. Similarly, many governments release datasets under the assumption that the data cannot be tied to particular individuals.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

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 computing users will have to be policed in other ways – through constitutional tort and political oversight.

Protections for Encryption

Avoiding a new era of eroding lines between personal and public space requires revisiting the capabilities of quantum technologies. Two broad areas of concern are present: attacks on widely used encryption and the different ways quantum sensing will give institutions powers to perceive phenomena in new ways.

In the encryption threat scenario, recall that quantum computing will degrade (but not render useless) the most widely used encryption for stored files – AES, the Advanced Encryption Standard. Confidentiality of stored information is critical because so many of our communications and other interactions in the world are now recorded and retained somewhere. Even if one has "nothing to hide"[83] – but we all do – these stored files might contain commercial secrets, passwords, financial information that might be exploited by swindlers, information about third parties, such as clients or children, who have not agreed to publicity, and so on.

Recall from Chapter 8 that passwords are essential to security but that their crypographic hashes could be reversed more quickly with quantum computers. We think this an unlikely use of quantum computers. Classical computing techniques, and simple trickery such as phishing, offer inexpensive, and too frequently, effective ways of getting into accounts.

Policymakers should focus on situations where, over time, information aggregates about people, creating particularly valuable attacks. One example is email. With the advent of limitless-storage email services, it is now easier to keep all emails than to segregate out material that should be deleted. The result is that if one can guess an email password, years of embarrassing, or simply valuable, data (think about yet-to-be-used gift card numbers and the like) are easily exfiltrated, mined, and sometimes made public. Increasingly multi-factor authentication is available for high-value accounts (and

[83] For a comprehensive critique of the "nothing to hide" argument, see Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy" (2007).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

patient users), but the reality remains that once access is obtained, all this data can be quickly exfiltrated.

Recall that protections for stored data, notably AES, are resilient to quantum cryptanalysis. It would seem sensible to start storing email archives with such encryption. Such archiving is what Professors John Koh and Steven Bellovin have proposed in Easy Email Encryption (E3), an approach that focuses on encrypting the stored emails that many people use as a kind of backup method for information.[84] Currently this information is protected while it is sent by the user, and by login authentication. But once an email password is guessed, all bets are off. The E3 approach downloads email, encrypts it, and throws away the original message. Breaches of such a system only expose the most-recently received messages. An attacker who used a quantum computer to break the password would then have to break an AES-protected archive.

Several classical computing techniques could frustrate mass decryption by a hypothetical quantum computer.[85] A simple way of countering Grover algorithm attacks (typically against stored data), which in effect cuts symmetric key sizes in half, is to lengthen key sizes, thus re-imposing fantastic levels of computational costs.[86] With respect to asymmetric encryption systems widely used for payments and communications, "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.[87] 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,[88] 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.[89] Certain problems are uniquely tractable by a quantum computer; post-

[84] Koh, Bellovin, and Nieh, "Why Joanie Can Encrypt: Easy Email Encryption with Easy Key Management" (2019).

[85] Bernstein and Lange, "Post-Quantum Cryptography" (2017).

[86] Grumbling and Horowitz, *Quantum Computing: Progress and Prospects* (2019).

[87] Goldberg, D. Wagner, and Brewer, "Privacy-Enhancing Technologies for The Internet" (1997).

[88] National Security Agency and Central Security Service, "Commercial National Security Algorithm Suite and Quantum Computing FAQ" (2016).

[89] Bernstein, "Introduction to Post-Quantum Cryptography" (2009).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

quantum researchers test measures that are intractable for quantum computers. For instance, company PQ Solutions developed a technique that involves injecting random noise into each message. In 2016, the Open Quantum Safe Project was formed to create open source versions of quantum-resilient encryption. Already other 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 keep information forever. But now even Google, the standard-bearer for information hoarding, has started efforts to randomize identifiers associated with searches and to delete them. 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. To do otherwise risks the creation of what Paul Ohm has called the "database of ruin," aggregations of even pedestrian facts that could haunt us.[90] One can imagine that behavior considered perfectly acceptable at one time could mar one's reputation in the future. But even documentation of perfectly legal behavior has been weaponized to degrade individuals' reputation, resulting in a drip-drip-drip of revelations about public officials, exposing what appear to be inconsistencies between their public and private lives. UK political theorist William Davies speculates that such banal revelations are triggering a crisis for liberal governance.[91]

Establishing ceilings for how long data is kept, even if those data are pseudonymous,[92] 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 de-

[90] Ohm, "Broken Promises of Privacy: Responding to The Surprising Failure of Anonymization" (2009a).

[91] Davies, *This Is Not Normal: The Collapse of Liberal Britain* (2020). The idea is that large-scale transgressions now matter less than minor revelations that impugn the authenticity of a political actor. When authenticity becomes the coin of leadership, the result is the rise of uncompromising, yet authentic, political personalities on both the left and right.

[92] Because of the advent of machine learning-enabled reidentification techniques.

stroy the data logically rather than physically.[93] 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 – anything less than AES-128 – used for deletion purposes will fail in the presence of quantum computing.

Several quantum computing innovators have created cloud-based devices for the public to use.[94] This is an ingenious strategy because it allows the company to study how users manipulate the device and to identify the most talented programmers. It also allows the quantum computer owner to keep its engineering secrets private, locked away in some secure cloud facility that makes reverse engineering impossible.

The cloud strategy is likely to be a winning one because few companies will be able to afford their own quantum computers. Providers thus become a chokepoint that can monitor their cloud for signs of decryption, just as one can look for signs of child pornography trading or spam transmission today. Importantly, a cloud monitoring 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 (see Section 7.5, p. 293).

Finally, regulating decryption may seem futile, but US law already regulates many forms of information manipulation that are technologically easy to perform. These are attempts to set norms, and they are sometimes effective. US copyright law prohibits the circumvention of digital rights management technologies (often a form of encryption) that protect copyrighted works.[95] The Fourth Amendment and the wiretapping laws prohibit warrantless interception of communications content,[96] even though such activity is technologically simple for private investigators, law enforcement, and the intelligence community. Just as it is creepy to wiretap others, and dishonest to watch movies without paying, we might be able to create

[93] Reardon, *Secure Data Deletion* (2016).

[94] M. Harris, "D-Wave Launches Free Quantum Cloud Service" (2018).

[95] 17 USC § 1201.

[96] 18 USC § 2511.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

norms that prevent most people from using quantum technologies to spy on each other.

9.5.3 Challenges of Government Power

Constitutional law precedent will likely apply to some kinds of privacy invasions brought about by quantum technologies. Chapter 8 describes capabilities that law enforcement agencies would pursue, such as UAV-mounted quantum sensors that search for firearms, explosives, and contraband drugs. One could imagine a city (but do not discount the privacy invasions of well-resourced advocacy groups) scanning entire neighborhoods for the presence of guns in the homes of people who are disqualified to own them: for instance, convicted domestic abusers or those on supervised release (probation, parole, or house arrest).

Investigatory Power

Yet, as private spaces and conduct become more vulnerable to sensing at a distance, courts have adapted and expanded Fourth Amendment protections for the home. For instance, in *Kyllo*, the Court interpreted the use of infrared cameras to detect heat emanating from homes as a Fourth Amendment search.[97] *Kyllo* would be strong precedent for the proposition that home-directed quantum sensing is exceptional and requires a warrant.

In recent years, the Fourth Amendment has had a kind of renaissance, embraced by both liberal and conservative justices. For instance, the Supreme Court has expanded privacy protections concerning information outside the home. As wireless phones have proliferated and made it possible to track individuals continuously, the Court has increasingly brought such devices and even the data they generate held by third parties under the ambit of Fourth Amendment protection.[98] As the Court contemplates how modern privacy protection requires government restraints on data held by the private sector, there could increasingly be warrant preference and other limits on data held by third parties.

As exciting as the Fourth Amendment renaissance is, the Court's actions merely establish a warrant requirement or "preference." The warrant preference, upon inspection, is a limited protection. Many

[97] *Kyllo v. US*, 533 US 27 (2001).

[98] *Carpenter v. United States*, 585 US ____ (2018); *Riley v. California*, 573 US 373 (2014).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

people simply waive their right to privacy when the government asks to do a search, so no warrant is needed. And where the government does obtain a warrant, the exercise is more paperwork-intensive than substantive. That is, a lot of paperwork and procedure is involved, but as a substantive matter, all the government must show is "probable cause" that the place to be searched has evidence of a crime. The word "probable" leads many to think the government has to have more than 50 percent proof – that it is more likely than not that the suspect's private space has evidence of a crime. But that is not the standard. Courts interpret "probable" to mean a "fair" probability, something less than a 50 percent chance that evidence is present.

Thus, the question that civil libertarians should be considering is: is a warrant a sufficient safeguard against quantum-enhanced remote sensing? Traditional searches of homes occur a single time and are performed by people who may overlook contraband or forbear from an exhaustive search. But a quantum sensor, perhaps with millimeter resolution, would not just see more finely but also enable continuous searches. Just as we use quantum sensors at the borders to detect radioactive material (see Section 2.1, p. 36), we could foresee a day where searches are comprehensive and easy. Daily quantum searches might be in store for certain populations, for instance those with reduced expectations of privacy because they are on supervised release.

The wiretapping "superwarrant" standard may be apt for quantum sensing searches. In wiretapping, an activity that now includes the monitoring of many kinds of communications, even with wireless phones, the government has to comply with extra safeguards. These "superwarrant" limitations include the requirement that wiretapping only be used to police serious crimes, that irrelevant conversations be purged, and that surveillance occur only for a time-limited period. Importantly, the government must also explain why wiretapping is necessary, that is, why the investigation cannot proceed using other investigatory methods. These substantive and procedural safeguards could be adapted to quantum sensing searches to make such searches exceptional, time-limited and to exclude them from routine police procedure.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Sensemaking Power

The above discussion primarily deals with situations where the government is seeking to collect information. Indeed, civil libertarians have long sought to limit government power by keeping the government in the dark and stopping it from collecting data. That strategy's efficacy erodes as the government is involved in more aspects of our lives, giving it opportunities to collect data, and as the government gains greater power to make sense of the data it possesses than other actors have.

A further conceptual step is necessary to impose limits when the government lawfully obtains information and subjects it to some quantum-enhanced scrutiny. As Orin Kerr observes, Fourth Amendment analysis focuses on the government's acquisition of data, not on the depth and cleverness of the subsequent analysis of such data.[99] Thus the government is free to attempt to make sense of ciphertext, in the same way it is free to decode puzzling mysteries associated with a crime.

A series of parallel developments in machine learning may cause us to rethink whether the government's power of analysis requires additional regulation to protect existing civil liberties.

Today we have so much data about the world that many academics and policymakers think that the world is comprehensible to the average person. However, data have no meaning until they are given context. Increasingly it is clear that access to data is not enough: the process of sensemaking, the ability to evaluate data and convert it to information and knowledge, is critical. Yet, there is a dramatic sensemaking gulf between the ordinary person and governments and companies.

Already, sophisticated actors can examine evidence more deeply, and for a longer period of time, than can individuals or small organizations. This ability to interrogate data may itself become an independent basis for concern and rationale for limiting future government activity. For instance, sophisticated computer vision algorithms combined with a massive archive of imagery allowed an agent at the Department of Homeland Security to identify a child sex offender living in Las Vegas because their face appeared in two different photos. One was a grainy, oblique photo of his face that appeared in

[99] Kerr, "The Fourth Amendment in Cyberspace: Can Encryption Create a Reasonable Expectation of Privacy?" (2001).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

a Syrian Yahoo user's account showing a young girl being sexually abused; the other was a thumbnail-sized image of him standing in the background of a family vacation photo.[100]

In 2009, a student project at MIT called "Gaydar" discovered that it was possible to reliably infer the sexual orientation of many MIT students by analyzing their online social networks.[101] Thus, some scientists claim that merely viewing a photograph that a person chooses to display on their social media profile can reveal that person's sexual orientation.[102] Since then, scientists have shown that it is possible to infer a person's sexual orientation using "minimal cues"[103] – and if such cues can be inferred by humans, then surely they can be inferred by machines as well (although rigorously controlled scientific experiments to answer this question have yet to be conducted). Another study showed that the photos that a person posted to their Instagram feed could be analyzed for depression, and that the results were just as accurate as diagnostic tests currently in use.[104]

An entire industry now sees emotion as fair game for manipulation by computer, with applications ranging from voting to buying to workplace conduct.[105] Presumably, higher-dimensional analyses only possible with quantum computers will accelerate these trends, making it difficult in practice to avoid revealing facts that, for whatever reason, we would rather not reveal.

Sensemaking is powerful, and the power to make sense is becoming concentrated. As quantum computing and sensing enhance machine learning, there will be even more troubling advances in com-

[100] The match was made possible by Clearview AI, a company that later came under attack for the way in which it has quietly downloaded over a billion such photos from social network websites and made the tool available to law enforcement and others. See Hill, "Your Face Is Not Your Own" (2021).

[101] Jernigan and Mistree, "Gaydar: Facebook Friendships Expose Sexual Orientation" (2009).

[102] Y. Wang and Kosinski, "Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation From Facial Images" (2018). For a critique of Wang and Kosinski, see Katyal, "Why You Should Be Suspicious of That Study Claiming A.I. Can Detect a Person's Sexual Orientation" (2017).

[103] Rule, "Perceptions of Sexual Orientation From Minimal Cues" (2017).

[104] Reece and Danforth, "Instagram Photos Reveal Predictive Markers of Depression" (2017).

[105] Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at The New Frontier of Power* (2019).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

puter vision and sensemaking that contribute to government investigatory power in public spaces. Consider these scenarios:

- Quantum illumination might make darkness no longer a barrier to observation with cameras. Private actors or the government might use low-light cameras to film people in darkened areas.
- Perhaps through quantum sensing, dense objects such as firearms will be remotely detectable through clothing.
- Single-quanta sensors and machine learning might contribute to a technique known as blind signal separation, tying individual voices to specific speakers even in a chaotic, loud environment. Such a world would change from the "masquerade ball" conception of identity in public[106] spaces to one with perfect identity and speaker attribution.
- Finally, these sensing techniques could be augmented with a range of machine-learning-based analytics claiming to predict personality, predisposition to crime, and so on. Quantum computing could enhance such analyses through optimizing machine learning, or at least add a patina of credibility to underlying pseudoscience.

Police departments might find such applications attractive because they would effectively allow officers to conduct a "Terry Stop" or "Stop and Frisk" of everyone on a public street. In court, the defenders of the practice would say that analysis of lawfully acquired data observed in public is fundamentally no different than observing a bulge in a person's pocket from a handgun.

9.5.4 The European Approach to Privacy Rights

European human rights and rules provide one attractive approach that is technology-neutral in order to prevent new techniques from evading legal controls. Article 8 of the European Convention on Human Rights (ECHR) establishes privacy as a human right, and specifies that the right to privacy shall not be interfered with unless the interference "is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the

[106] Bailey, *The Open Society Paradox: Why The 21st Century Calls for More Openness – Not Less* (2004).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." This framework requires states to put people on notice of special investigative measures with specific, enabling legislation. A broad range of police conduct is considered an "interference" including the mere collection of data about individuals in police files, but also special investigative techniques, such as the use of phone-number collecting pen registers, and even the recording of suspects while in a jail cell.

Interferences with privacy must be lawful, necessary, and proportionate. Lawfulness is satisfied by enacting a domestic law authorizing the special measure in question; the law must be specific enough to put the individual on notice of the consequences of the investigative measure. That is, the law must impart guidance to the individual, so that the individual can foresee what the government technique might lead to.

Necessity and proportionality are judgement calls relating to the power of the state, and the kinds of interests that the state seeks to satisfy. European courts are more likely to authorize special measures in response to specific security threats, but to reject them when applied to general criminal deterrence. As part of the analysis, European courts consider whether the technique is effective in addressing articulated state interests, and whether there are alternative techniques that are less invasive of privacy. In this respect, the European approach is different from the Fourth Amendment to the US Constitution. Courts have interpreted the Fourth Amendment to be *transsubstantive*, that is, privacy protections apply with equal weight regardless of the crime suspected. US persons' privacy is the same whether the substance of the crime is murder or mere vandalism. There are many advantages to transsubstantive approaches, but one serious downside from a civil liberties perspective is the ability to scale up police powers to address serious crimes while disallowing high-power approaches from being unleashed in investigation for petty crimes.

Under the European framework, many investigative techniques are indeed lawful, because of the need to provide national security or security against crimes. But in some cases, particularly when government interests pursue general deterrence, even in anti-terrorism matters, courts have curtailed government power. As this book goes to press, a United Kingdom appellate court ruled that a face recog-

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

nition system used *in public* – a widespread practice in the US – violated ECHR's Article 8. Despite having implementing legislation, the court found the law too vague in that it failed to specify who might be targeted by the system or where it would be physically implemented. On separate grounds, the court found the government violated an anti-discrimination law for failing to test whether the facial recognition system produced biased results based on race and gender.[107] In a separate case, the European Court of Justice held that broad mandates for data retention among communications providers are illegal for general crime fighting and even national security purposes. Only specific, serious national security threats justify mandates that providers keep data about users, and only for a "strictly necessary" time.[108] Meanwhile in the US, police are free to deploy face recognition even to deter petty crime, and police need not consider bias; they are also free to order providers to retain users' data for almost any crime and without having to ask a judge.

In addition to substantive checks on government power, the procedural aspects of the ECHR framework have real value. The requirement of enacting a law forces a public debate about government power. In regard to quantum technologies, this debate, and the law flowing from it, would have to be sufficiently specific to warn the public about the kinds of powers the technology enables. This is a much-needed reform in America. Recall that much of the controversy surrounding NSA surveillance in the US relates to the Department of Justice developing ingenious, strained, and often secret interpretations of laws that greenlighted bulk collection of personal data in ways that surprised even skeptical civil libertarians. But under an ECHR-like framework, experts' surprise itself would be evidence that the law was arbitrary; that the law failed to tell the public what the government can and cannot do with the technology.

The ECHR framework is just one piece of Europe's criminal procedure. Other instruments regulate police investigative practices at the state level, nation states do have oversight mechanisms for intelligence, and in 2016, community law was passed comprehensively regulating how law enforcement agencies, from investigation to prosecution, collect and use personal data. Taken together, this belies the narrative that Europeans "trust the government" and that Eu-

[107] *R (Bridges) v. CC South Wales & ors*, Case No: C1/2019/2670.

[108] *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs et al.*, Case No: C-623/17.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

ropeans allow police to run roughshod over civil liberties. Americans have few criminal procedure protections as substantively strong as the Europeans, and nothing as comprehensive.

As the military acquires new surveillance techniques that inevitably find their way into the hands of federal and then local law enforcement, the European model would force useful transparency and place limits on power and consequently preserve civil liberties. Short of the European model, the US could create safeguards that require substantive and procedural review before these technologies leave federal government agencies and end up in the local sheriff's office.

The human rights approach has another, more subtle advantage: it can be framed as a positive agenda, as in we are *for human rights*. Technology policy today emphasizes a *negative* approach, one focused on denying China the ability to press its political will on the world through technology. Advancing the cause of human rights, demanding that these rights be respected, gives policymakers a positive frame and a way to reject technologies based on their effects rather than their source.

9.6 Quantum Prediction

Companies developing quantum technologies have identified a number of commercial goals for the technology. Some companies are seeking short-term goals, but Google is aiming for the moonshot of achieving artificial intelligence using quantum computers.[109] Quantum computing is thought to both speed existing machine learning processes but also create the infrastructure for entirely new techniques.[110]

Machine learning may receive a significant advance with quantum computing 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 datasets makes computing faster or, in some cases, simply possible. For instance, in natural language

[109] Google, "Quantum – Google AI" (n.d.).

[110] Sandia National Laboratories and National Nuclear Security Administration, *ASCR Workshop on Quantum Computing for Science* (2015).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

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").[111] Similarly, to reduce the problem space, data scientists use stemming and lemmas to collapse words with similar roots into a single concept. Presumably a quantum machine learning approach would have no need for throwing out so much data.

It is not clear if cognition of human experts operates in the same manner as modern machine learning systems, largely because we still have very little understanding of how human cognition works – especially among human experts. It's clear that expert-level human performance requires a combination of innate skill, learning, and thousands of hours of practice. What's not clear is how much of that expert-level performance is based on some kind of memorization and knowledge integration, and how much is based on establishing new neural pathways that can rapidly analyze new patterns.

9.6.1 Product development

Among the most intriguing proposals is the possibility of combining machine learning with quantum simulation of physical objects. The implications of these proposals are profound for product development in materials sciences, pharmaceuticals, and chemicals. Given any goal, such as for a drug that is more targeted and thus has fewer side effects, the combination of quantum sensing and computing could identify treatments that fit the bill. With the quantum sensing approach, scientists will see deeper into molecules. The understanding gained could create a revolution in using structure to target and to choose attributes of a chemical or material that are desired. Once structures are understood, quantum computing, using Grover's algorithm, presumably could search for the optimal candidate structures.[112]

[111] Berry et al., *Survey of Text Mining II: Clustering, Classification, and Retrieval* (2008).

[112] Aspuru-Guzik et al. put it nicely: "Imagine that you want to find a 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

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

One can imagine the fantastic outcomes and their knock-on effects from simulation. If one can simulate the chemical basis for energy storage, perhaps a super-efficient battery could be built. Energy then becomes cheaper (because we can store it easily) and the knock-on effects could be that we have more energy capacity and that solar generation and storage become economical for more households. Similar research could be applied to energy transmission efficiency and to countless energy-intensive processes, from creating fertilizer to metals.

What do these capabilities mean for safety regulation? One approach is to trace the requirements for pharmaceutical and chemical safety to current processes, and explore how computer simulation might add, change, or even eliminate requirements. At the highest level, pharmaceuticals go through four levels of review: pre-clinical testing, clinical research, review by the FDA, and finally, surveillance after the drug is in the marketplace. Consider that in the earliest phases of drug development, before humans are involved, developers must answer basic questions surrounding absorption, dosage, and risks surrounding toxicity.

This earliest screening of drugs requires time and labor-intensive explorations, because people are not all alike, and treatments may have different effects on people based on their sex, race, age, body weight, and presence of existing conditions. The Food and Drug Administration specifies procedural rules to ensure good design and to prevent guile.[113] And this is where quantum simulation may offer the best speedups. In addition to basic discovery of promising treatments, the effects of those treatments could be simulated with models of drug absorption and interaction. Once the complex interactions can be modeled and specified on a quantum computer, presumably these models could be run as standalone programs on classical computers. In fact, entire businesses could arise that specialize in creating these models for others to use. A market would exist for creating models based on many different human characteristics going beyond sex and age. One could foresee models for pregnant people, for people with genetic or environmental conditions that may create complications,

in search of one that the trained model believes will have therapeutic properties." See Sandia National Laboratories and National Nuclear Security Administration, *ASCR Workshop on Quantum Computing for Science* (2015).

[113] See e.g. FDA, Protocol for and Conduct of a Nonclinical Laboratory Study, 21 CFR 58 (2020).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

or even models for single individuals afflicted with cancer or other diseases that have idiosyncratic characteristics.

Later phases of drug development require human experimentation, with all of its complexities and contingencies. The FDA process specifies three rounds of clinical trials with increasing numbers of human subjects. Each phase can take years, and the final phase can involve thousands or even tens of thousands of subjects. It is unclear how quantum simulation might affect these requirements. Perhaps developers could more precisely identify how many people must be tested and whether over-, or under-sampling is called for based on genetic or environmental factors.

Clinical trials elicit side effects from participants, and any patient is now familiar with the lengthy, sometimes conflicting lists of complications that any drug might create. A straightforward counting of adverse event disclosure found that the most popularly prescribed 200 drugs on average have 106 such warnings. One popular drug had 459.[114] How much of this disclosure is noise or risk management instead of useful knowledge about risk? One could imagine quantum machine learning being used to tease out all the conflicting and confusing signals surrounding side effects of medicines. Perhaps there are indeed hundreds of risks from any given drug; finding ways to prioritize these risks could contribute to physicians' risk/reward considerations.

Finally, in the post-market phase, FDA monitors the marketplace for bad outcomes, lack of advertising compliance, and enduring safety and quality risks from manufacturing. Here too one could see quantum simulation providing more efficient oversight. For instance, in the post-market phase, companies making generics may copycat existing treatments, under a different regulatory standard that seeks to ensure that the generic treatment is equivalent in mechanism and effect. One could imagine simulation finding or verifying equivalent treatments. Whether these applications emerge, and whether they could possibly relieve regulatory burden on pharmaceutical makers is a question for another day.

9.6.2 Fairness

Artificial intelligence and machine learning (AI/ML) have raised deep concerns about how data inputs, algorithms, and commercial

[114] Duke, Friedlin, and Ryan, "A Quantitative Analysis of Adverse Events and 'Overwarning' in Drug Labeling" (2011).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

practices might result in machines that engage in unlawful discrimination or other kinds of unfairness.[115] 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.[116] A key problem in this space is that there appears to be an inverse relationship between learning power and explainability in modern ML approaches. That is, the most powerful learning systems, because of their complexity, find subtle and unpredictable relationships.[117] Yet this power comes with a price – users may not be able to explain why these relationships occur, these relationships may be specious, and they may correlate with race or other factors that could be perverse.

Of course such transparency does not guarantee fairness, but policymakers will see transparency as an important factor in evaluating machine decision making.

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 a person to play chess or Go against a supercomputer. But what if we are called to play consumer or investor against adversaries using quantum computing-powered optimization?

In the consumer context, the immense volume of internet traffic and tracking that is collected simply cannot be computed on classical machines. The disconnect between data volume and the ability to process it causes marketers to 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 computing marketing machine,

[115] Calo, "Artificial Intelligence Policy: A Primer and Roadmap" (2018).

[116] See ACM Conference on Fairness, Accountability, and Transparency (ACM FAccT), a computer science conference with a cross-disciplinary focus that brings together researchers and practitioners interested in fairness, accountability, and transparency in socio-technical systems.

[117] Gunning and Aha, "DARPA's Explainable Artificial Intelligence Program" (2019).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

individual consumers could come into fuller 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. Lawyers see advertising as a rational information exchange but marketers understand it as a tool that communicates on several levels, including on raw emotion. In a marketplace optimized by quantum computers, sellers might understand our willingness to pay, our strongest preferences, our subjective emotional valences, and the kinds of evidence that cause us to change our minds. Imagine the face-recognizing camera system described above optimized to understand how desperate the consumer is for a product, how the consumer has responded to other offers, how emotion can be invoked to appeal to a certain individual, and whether the consumer is innumerate or otherwise unable to understand common strategic selling techniques such as bundling. Might we see such a marketing machine in the same light as advanced selling techniques targeted at children? Would the standard regulatory approach of labeling (perhaps "quantum ad") be enough to prepare consumers for the kinds of persuasion we may face?[118]

Recall that quantum computing is most likely to be achieved by nation states or dominant technology companies, such as Google. Google reportedly refrained from using user search terms to predict stock movements,[119] apparently because it realized that searches may include material non-public information (which is illegal to use under US law). Google may similarly conclude that quantum trading approaches using search data 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, from gaining a foothold in telecommunications

[118] A core function of advertising law is to help consumers recognize strategic communication so that they can use their own self defenses against deception or other manipulation. Self defense is necessary because there is so much false advertising that regulators could never police it. See Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (2016).

[119] Fortt, "Top 5 Moments From Eric Schmidt's Talk in Abu Dhabi" (2010).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

markets. The intelligence community has already found offensive cyber to be a useful, asymmetric, secret tool to undermine adversaries. Won't quantum technology 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.

9.7 Measuring Quantum's Research Output

We conclude the chapter with an attempt to evaluate the impact of policy efforts to date: where is the quantum action?

9.7.1 Academic Publications

To better understand state sponsorship of quantum technologies, this section presents data from the Web of Science to elucidate high-level trends in quantum technology research outputs. The data source is the Web of Science Core Collection, "a curated collection of over 21 000 peer-reviewed, high-quality scholarly journals published worldwide (including Open Access journals) in over 250 science, social sciences, and humanities disciplines."[120]

Quantum Technology's Research Output

We examined statistical data about scientific literature and patents to identify funding and other trends regarding quantum information science.[121] In examining funding sources for 15 130 papers we identified as relevant, Web of Science reports that the National Natural Science Foundation of China (2692) is the dominant funding organization for published research in quantum technologies, followed far behind by the US National Science Foundation (1275). But such a categorization ignores how nations have multifarious routes to funding research. For instance, in addition to the NSF, other major US government supporters of quantum technology research include the

[120] Clarivate, "What Is Web of Science Core Collection?" (2021).

[121] A simple text search for "quantum" in titles, abstracts, and keywords returns over 400 000 papers published since 2009. We used two approaches to narrow these results. First, we used a search for publications mentioning the three categories of quantum technologies focused on this book; that returned 15 696 papers ("quantum sen*", n = 629; "quantum commun*", n = 3852; "quantum compu*", n = 11 215). There were 566 duplicate publications appearing in two or more of these searches, resulting in n = 15 130 unique publications. Almost all of the literature appears in English.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Department of Defense,[122] the Department of Energy, the National Aeronautics and Space Administration, the National Institute of Standards and Technology, the National Institutes of Health, and the Office of the Director of National Intelligence. In fact, one key observation from this analysis is that the US intelligence community and the US military both have embraced a rich quantum information science research agenda. Furthermore, the Department of Energy is funding quantum technology research in an attempt to promote US superiority in high-performance computing.

In China, many individual provinces have research portfolios in quantum research, supplementing the country's national scientific research organizations. In Europe, individual nations, most prominently Germany, Spain, the Netherlands, and the United Kingdom, have supplemental funding to community-wide efforts. Brazil, Singapore, and Japan also appear prominently. Finally, many private foundations, such as the Alfred P. Sloan Foundation and the Simons Foundation, are active in quantum technology, and their funding contributions may be as consequential as some nations'.

Table 9.6 gives a lower-bound estimate of the number of published papers in quantum technology funded by different nation states. The table is styled as an estimate because funding support data in Web of Science required significant cleaning and some supporters could not be resolved to a country (for instance, some papers are supported by the "Ministry of Education," but many nations have such a body). Also, a single paper can be sponsored by more than one research organization. This table presents two rows for the European Union. The first is EU-community-wide-supported publications plus all the papers funded by individual EU member states (for instance, to recognize the independently funded nation state programs in Germany, the UK, and elsewhere).

Just as patent counting is not an evaluation of patent quality, paper counting is not an evaluation of research quality. Indeed, turning away from the absolute number of papers published to citation met-

[122] Funding agencies within the Department of Defense include the Air Force Office of Scientific Research (AFOSR), the Army Research Office (ARO), the Defense Advanced Research Projects Agency (DARPA), the National Security Agency (NSA), and the Office of Naval Research (ONR). The Intelligence Advanced Research Projects Agency (IARPA) was modeled on DARPA, but is organizationally underneath the Office of the Director for National Intelligence, and not part of the US Department of Defense.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Table 9.6. Support for publications on quantum technologies

Nation	Estimated Number of Papers
China	8006
US	6071
European Union (including national support)	5819
EU alone	2520
Japan	1491
Canada	1425
UK	894
Germany	785
Nongovernmental Organizations (Foundations)	618
Australia	598
Brazil	518
Spain	455
Russia	383
France	280
Austria	253
Korea	249
Papers with no data	4641
Total	35 006

rics, among the most-cited research publications, US and European-funded works dominate.

Web of Science tracks the institutions of authors publishing papers. Institution tracking looks for any matching address, so a single paper can have many institutional affiliations. This is especially true in quantum information science, which is inherently interdisciplinary, and frequently research involves collaboration across institutions. Table 9.7 presents the most frequently appearing institutions in quantum technology papers.

Turning to author national affiliations, Web of Science tracks the addresses that appear in published papers, and categorizes them by nation. Since multiple addresses can appear in papers, a single paper can be affiliated with more than one nation. In quantum technologies, the US has the most authors (Table 9.8).

Web of Science also provides high-level categorization of quantum technology publications, revealing the wide variety of disciplines

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Table 9.7. Affiliations listed by authors on quantum technology publications

Institution	Number Published
Chinese Academy of Sciences	836
Centre National de la Recherche Scientifique (CNRS)	440
University of Science Technology of China	432
University of California System	411
University of Waterloo	346
US Department of Energy	324
Max Planck Society	307
National University of Singapore	305
Massachusetts Institute of Technology	292
University of Oxford	285
University System of Maryland	281
Tsinghua University	276
National Institute of Standards Technology	243
University of Maryland College Park	238
Russian Academy of Sciences	223
Consiglio Nazionale delle Ricerche (CNR)	218
Harvard University	196
University of Tokyo	195
University of London	180
Beijing University of Posts Telecommunications	177
California Institute of Technology	166
United States Department of Defense	165
Delft University of Technology	157
ETH Zurich	156
University College London	154
(affiliation data missing)	247
Total	7250

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Table 9.8. National affiliation of QIS authors

National Affiliation	Authors
US	3973
China	3680
Germany	1451
England	1200
Japan	1114
Canada	1026
Australia	767
India	654
France	630
Italy	618
Russia	453
Spain	448
Switzerland	419
Singapore	383
Austria	370
No regional data	235
Total	17 421

that contribute to the expertise of QIS. This table highlights that many science disciplines, including chemistry, physics, electrical engineering, computer science, and nanoscience, are relevant to the conception and design of quantum technologies. We present this information in Table 9.5

It is important to recognize the limitations of these data. First, the analysis obviously only focuses on published research: research that is classified or simply unpublished is not included. Such omissions are not fatal to our analysis, because the players in quantum technologies today have incentives to publish. Indeed, authors affiliated with or funded by D-Wave, Google, IBM, Microsoft, Lockheed Martin, Rigetti, and Volkswagen, along with scientists at military-affiliated research laboratories, appear in the results. A second, more significant limitation is that paper counting overlooks publication quality. While China appears to be pulling ahead in research output, there are systemic incentive problems documented in some countries' publication practices. China has dramatically increased its scientific scholarly output in the past three decades, in part by giving gener-

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

ous cash awards to authors. A 2017 article found that payments for publication in *Science* or *Nature* came with an average bonus to the first author of $43 783.[123] Lower-tier institutions were willing to pay authors more than higher-tier ones. Publication in the *Journal of the Association for Information Science and Technology* (JASIST) netted the first author on average almost $2500. Given that the average faculty salary for a university professor in China is about $8600, these sums are significant. Payments for publications as a policy were reportedly ended in 2020, but these statistics are clearly influenced by China's former policy.[124]

A third limitation is that some attributes are missing significant data. For instance, in funding organization, about 30 percent of the papers lack any information about the research sponsor: this could be an oversight, or an attempt to hide a significant sponsorship.

Finally, sources of funding are multifarious and referred to in inconsistent ways by authors. As a result, producing these tables required significant data cleaning to address inconsistencies and errors, so unmeasured errors resulting from reporting bias or manipulation may be present.

9.7.2 Quantum Technology's Patent Output

Issued patents are another way to measure the success of research expenditures. A 2017 survey of quantum technologies by *The Economist* reflected a national competition in the patent landscape of quantum technologies.[125] Using data current through 2015, the publication found that the US had by far the most patent 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), Germany (sensing), and Japan (quantum computing and cryptography).[126]

[123] Quan, B. Chen, and Shu, "Publish or Impoverish: an Investigation of The Monetary Reward System of Science in China (1999–2016)" (2017).

[124] Mallapaty, "China Bans Cash Rewards for Publishing Papers" (2020).

[125] Palmer, "Technology Quarterly: Here, There and Everywhere" (2017).

[126] See also Patinformatics, "Quantum Information Technology Patent Landscape Reports" (2017).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

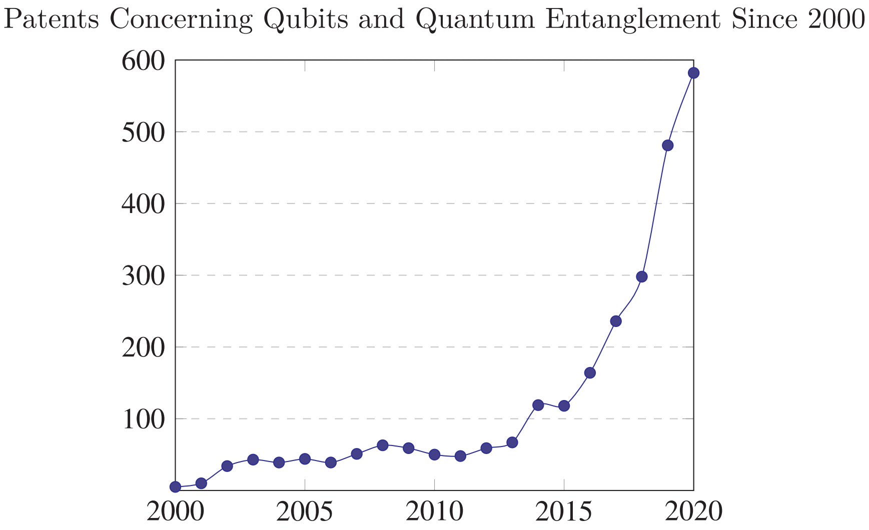

Figure 9.3. Over time, there has been a steady increase in patents published that concern qubits or entanglement. In 2019, 481 such patents were published worldwide. Source: analysis based on Derwent World Patents Index database. For more information, see the sidebar "Who Has Quantum Technology Patents?" on page 453.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Who Has Quantum Technology Patents?

Richard P. Feynman gave a seminal talk, "Simulating Physics with Computers," at the first Conference on Physics and Computation in 1981. Charles Bennett and Gilles Brassard proposed the first quantum cryptography protocol in 1984. David Deutsch formulated a model for a universal quantum computer in a 1985 paper. Peter Shor's RSA-busting algorithm was published in 1994, and Grover's search algorithm in 1996. None of these events resulted in a patent being granted. Starting in the mid-1990s, several large companies were awarded patents in quantum technologies.[a] These entities have more than 30 patents published as of December 2020:[b]

Patent Owner	# Patents
International Business Machines Corp. (IBM)	236
D-Wave Systems, Inc.	157
Intel Corp.	80
Microsoft	74
US Military Branches	68
Northrop Grumman	64
Google	59
Zhejiang Gongshang University	55
Toshiba	55
Lockheed Martin	45
NTT	43
MIT	41
Hewlett-Packard	36
Rigetti	34
South China Normal University	32
Total	1079

[a] In quantum cryptography, British Telecom led the field with 9 patents, while IBM, the University of California, General Electric, NTT, NEC, and the UK and US Secretaries of Defense were also in the mix. In quantum computing, leaders included IBM, Mitsubishi, Silicon Graphics, Hitachi, Lucent, MIT, and the US Air Force.

[b] Based on a search in Derwent World Patents Index for patents published that include the terms "quantum entangle!" or "qubit" since 2000. (The "!" is the Westlaw "root expander" search metacharacter.) The search produces 2650 responses. Responses were cleaned using OpenRefine.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

9.8 Conclusion

Our focus in this chapter is at the national level, with primary emphasis on policy options available to the US and Western governments.

While we believe that there is clearly a role for international agreements, and while we are strong advocates of bringing concepts from modern physics into the pre-college curricula, it is at the national policy level – the level of national sovereignty – where policy goals are most likely to be translated into meaningful dollars spent and policies enacted as laws or regulations.

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

Will Quantum Computers Make Humans Obsolete?

What if humanity realizes the project to build quantum computers and these machines can solve hard problems in the blink of an eye? What then?

As computers can solve hard problems, work that only humans can perform might become trivial. Natural language processing might develop *Star Trek*'s universal translator. As machine text and image generation become more sophisticated, many would be satisfied with less expensive, ubiquitous, quickly generated works of original art and literature that do not require the training and patronage of flesh-based artists.

"Don't worry about such creative destruction," say techno-utopians. "For each job technology obsoletes, another opportunity arises." The flaw with this narrative is that the innovations discussed here are aimed at problems solved using human intelligence and creativity.

Computers need not equal human performance: even if the machines are merely middling, employers interested in saving money, and consumers who value convenience over quality, will satisfice with the mediocre.

Computers will also systematically improve, thanks to the progress of technology. A recent article on the translation industry notes that while the market for human translators continues to expand, much of the work is now "post-editing machine translation."[a] What happens when post-editing is no longer necessary?

In *Homo Deus*, Yuval Noah Harari explains how many who feel secure in their jobs today could be replaced by algorithms.[b] Job security is imperiled by what Harari calls the *great decoupling* of intelligence from consciousness. "For AI to squeeze humans out of the job market it needs only outperform us in the specific abilities a particular profession demands."

Harari observes that our liberal notions of human worth are tied to and justified by the uses of the human body for warfare and for work, an idea echoed by Sun Microsystems founder Bill Joy.[c] When both functions can be performed well enough by computers, what need will the future have for humans?

[a] Tirosh, "Top Translation Industry Trends for 2020" (2020).

[b] Harari, *Homo Deus: A Brief History of Tomorrow* (2017).

[c] Joy, "Why The Future Doesn't Need Us" (2000).

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press

https://doi.org/10.1017/9781108883719.014 Published online by Cambridge University Press