Introduction

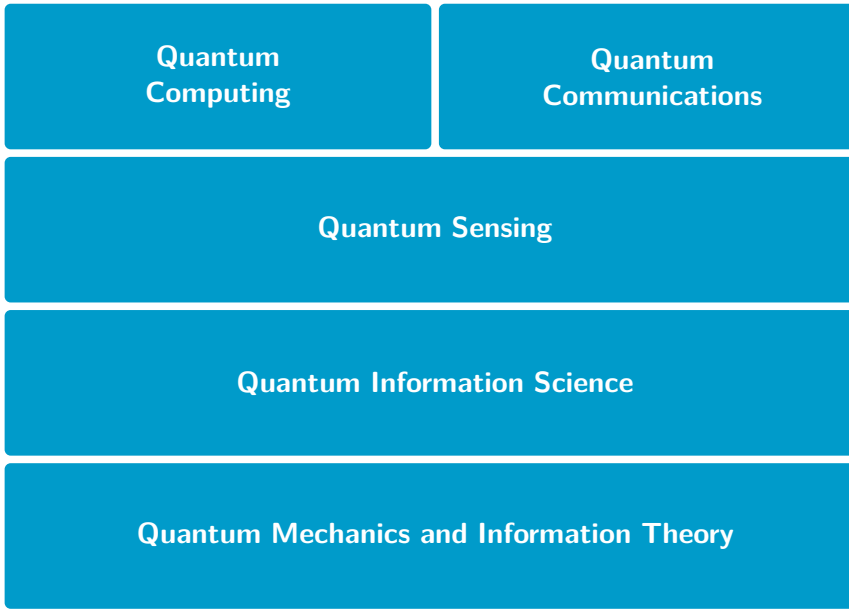
We are at the cusp of a technological revolution, one where technologists master the special physics of the smallest particles; a revolution that promises to provide capabilities that are, somewhat paradoxically, extraordinarily large.

Quantum mechanics explains the interaction of mass and energy at the smallest scales – why a molecule of water gets hot in a microwave oven, or how a uranium atom splits in a nuclear reactor. The rules of quantum mechanics are often counterintuitive and seem incompatible with our everyday experiences. Over the past century, deeper understanding of quantum mechanics has given scientists better control of the quantum world and quantum effects. This control provides technologists with new ways to acquire, process, and transmit information as part of a new scientific field known as *quantum information science* (QIS).

QIS combines quantum mechanics and information theory. QIS is not new – its roots go back to the 1960s. In recent years, however, technologists have made advances in quantum information acquisition, processing, and transmission, discussed in this book as *quantum sensing*, *quantum computing*, and *quantum communications*. Advances in these three classes of technology have moved discussions of QIS from the world of academic journals to corporate boardrooms and government offices. As the capabilities of quantum technologies have become clearer, both governments and companies have increased investment.

As quantum technologies arrive, we need both a clearer understanding of their implications for stakeholders and an open discussion of policies dealing with the impact of quantum technologies. Quantum technologies have *strategic* implications for nation states, they present challenges for decisionmakers such as investors, and they have many practical implications for individuals' lives. This book ex-

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press



From quantum mechanics and information theory to quantum technologies. Quantum sensing is a precursor technology to computing and communications.

plains the political relevance of quantum technologies and begins a policy discussion for their management.

The strategic implications of quantum technologies have ignited a technology race among stakeholders:

- **China and Europe** see QIS as an opportunity to leapfrog US technological superiority. In particular, nations see deployment of quantum technologies an an opportunity to counter the asymmetric advantages the US has gained from inventing the Internet. Seeking superiority carries with it themes of sovereign technology politics, and as a result, the risk of less scientific openness.

  Research groups in China and Europe have achieved fundamental, state-of-the-science gains in some quantum technology fields, renewing calls for large government investment in quantum technologies by the US and other countries. Reports of quantum-enhanced sonar and radar capabilities by Chinese scientists have rattled some US policymakers. Meanwhile, Germany, the United Kingdom, and the European Union (EU) as a collective are also making major investments in quantum tech-

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press

nologies, often with an emphasis on quantum networking and quantum key distribution. These are strategic emphases, because quantum communications could potentially narrow the aperture of foreign intelligence agencies.

- **Corporations** see the potential for billions in profits from the development and use of quantum computing, but the path to success is not clear and is fraught with risk. The most direct path to profit is to use quantum simulators to reduce research and development costs and to enable new discoveries, particularly in chemistry, pharmaceuticals, and materials science. Quantum computing may also enable breakthroughs in operations research and the optimization of business decisions, although existing classical alternatives are superior and may remain so for some time.

  For companies and investors, key issues include: whether quantum computing is a *winner-take-all* technology, that is, does a company have to be the first to develop a quantum computer, or can profit be realized by innovators in second and third place? Companies are also concerned whether paths to profit will be constrained by government technology superiority goals. Governments' competition over technology has already imposed export controls and demands for secrecy. Those controls and secrecy might make it more difficult to recruit the best workers. Companies are also concerned that their hard work will be copied or stolen by other nations or by competitors.

  The good news for companies is that the barriers to entry in quantum technologies are falling, thanks to the development and commercial availability of devices that produce and measure quantum effects, such as single-photon emitters and detectors. Hundreds of companies have some significant emphasis in quantum technologies, some have even brought quantum technologies to the marketplace that you can buy online today.

  Quantum technologies present opportunity and investment risk. Investors need to understand that the complexity and promise of quantum innovations make specious claims of profit and success difficult to evaluate. Given that investors were swindled by miracle narratives in less complex fields, we should be ready

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press

for the charismatic business leader to emerge promising billions based on wondrous yet unsound quantum technology concepts.

- **The US government** views quantum technologies as *dual-use* (both peaceful and military) and as important to the nation's strategic posture. Those invested in maintaining US technological superiority are worried about advances in quantum technologies made outside the nation.

  The US government has promised billions in funding for QIS and is in the process of awarding research projects through the research agencies of the armed forces and through the Department of Energy's National Laboratories. This funding, which represents a strong *industrial policy* approach, will stimulate both basic and applied research in all manner of quantum technologies. Quantum technology development policy is thus like the history of computing, the Apollo Space Program, and the Global Positioning Satellite network – projects as uncertain in benefit as they were costly to the taxpayer. But in each of these projects, unforeseen technologies were developed that eventually devolved to the private business community and to the average consumer.

Quantum technologies are heating fever dreams for nations' technological superiority goals. However, achieving superiority may be much harder in quantum technologies than in nuclear and aerospace programs. Quantum technologies are not in the exclusive control of any individual nation. Not only that, government strategies seeking technological superiority must anticipate the innovative power of academia and resource-rich private companies, as both have basic and applied research programs in quantum technologies.

Quantum technologies are expensive to develop, and require expertise that is in short supply. Much of that expertise is concentrated within organizations that have a commitment to open research and the free flow of ideas. Many of the teams working on quantum technologies are multinational, and virtually all of them have incentives to commercialize quantum technologies, complicating the task of developing tools that would be restricted to use by militaries. Indeed, some quantum technology innovators are shunning public funding to avoid the strings attached to government patronage.

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press

Tomorrow's likely developments in QIS will have consequences for how we will measure and sense the world, for how we will communicate, and for how computing will work for us. These consequences are so profound that we should begin planning for them today.

This book summarizes the state of QIS today in the form of quantum sensing, computing, and communications with the purpose of elucidating policy contours.

Outline of the Book

Part 01, "Quantum Technologies," begins with the highest-level concepts one needs to grasp in order to understand QIS and quantum technologies. Chapter 1 briefly covers what we consider to be the three ideas central to the field: uncertainty, entanglement, and superposition.

Readers wanting deeper treatment of quantum effects in Chapter 1 could turn to the appendixes of this book. We wrote the appendixes to provide policymakers, investors, and others who have to make critical decisions, with the scientific context relevant to today's policy issues. Appendix A provides an explanation of the quantum world: its size, how it is measured, and the meaning of the quantum scale. Appendix B continues the exploration of quantum theory with an exploration of the quantum state and how one measures at the quantum level. This material is presented with a historical lens, summarizing the debates and questions that animated decades of empirical and theoretical research in quantum mechanics.

Part 01 proceeds with the state of the science in quantum technologies. Quantum technologies sometimes provide improvements on classical methods, and in other cases create new capabilities. Quantum sensing is the most promising quantum technology, and thus we begin our journey in Chapter 2 focusing on it. Quantum metrology and quantum remote sensing are the first large-scale deployments of quantum technologies. *Metrology* is the scientific study of measurement (not to be confused with meteorology, the study of weather), while *quantum remote sensing* (or simply *quantum sensing*) refers specifically to the measurement of things in the distance. This chapter explains how the exquisite sensitivity of quantum states make it possible to perform precise measurements on things that are nearby or in the distance (underground, in the sky, or even in Earth's orbit).

Nuclear weapons provided the first significant – and horrific – demonstration of quantum technology. Today, the most visible use

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press

of that technology comes in the form of nuclear power plants. During the same period that nuclear weapons were developed, quantum sensing contributed to the diagnosis and treatment of untold numbers of people. The physics of nuclear magnetic resonance (NMR) spectroscopy was worked out in the late 1940s;[3] commercial NMR spectrometers were offered for sale just a few years later, and in 1977 the first two-dimensional image of a person's chest was produced.

NMR spectroscopy and magnetic resonance imaging (MRI) were game-changers for chemistry and medicine, and examining the history of these technologies from our twenty-first-century vantage point gives us a template for understanding the impact that quantum sensing technologies might have in the future. Quantum sensing possesses a number of affordances that make its strategic value apparent: first, quantum sensing can be stealthy, that is, it is possible to deploy quantum sensors in ways that an adversary may not detect them, making quantum sensors very different than long-distance radar arrays. Second, quantum sensors resist existing electronic warfare countermeasures, thus making it possible to determine one's position, engage in navigation, or make highly accurate measurements of time in the presence of jamming. Third, quantum sensors create several new capabilities, such as the ability to determine one's location underwater or underground (that is, when lacking a clear view of the sky to catch a GPS signal). Fourth, quantum sensing make it possible to detect objects that are obscured by barriers such as walls or those that are buried. This capability makes quantum sensing a potentially destabilizing technology for submarine and aircraft stealth. Finally, quantum sensing includes a curious application called ghost imaging, a technique so sensitive that it enables detection of things not in the direct line-of-sight of a sensor.

Quantum sensing is a precursor technology to quantum computing and communications. That is, in order to have a quantum computer or a workable quantum network, one must first develop control and readout systems focused on sensing individual particles. Some believe that a large-scale quantum computer will never be built. But when it comes to quantum sensors, there have been decades of successful development, continuing refinement, and even commercial availability.

[3]Edward Mills Purcell at Harvard University and Felix Block at Stanford University shared the 1952 Nobel Prize in Physics for its discovery.

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press

For all these reasons, quantum sensing, in our view, is the "killer app" of quantum technologies for at least the next decade. Particularly in the medical field, quantum sensing will benefit humankind in palpable, direct ways. The application of quantum sensing to intelligence, military, and law enforcement uses is more disruptive and harder to address with countermeasures, and thus warrants significant policy attention.

Quantum Sensing

Uses quantum effects to acquire data.

Capabilities

Measurement of magnetic fields, electric fields, gravity, temperature, pressure, rotation, acceleration, and time.

Near-term applications

Could change every strategically important industry: aerospace, intelligence, military, law enforcement, extractive industries, medical, and others.

Outlook

Highly optimistic because of multitudinous commercial applications, government investment because of strategic applications, relative simplicity, and increasing commercial availability of components.

The following four chapters unpack quantum computing – the quantum technology that is most discussed in the media and also most challenging to realize.

To understand quantum computers, it helps to have a foundation in the history of classical computing. This history elucidates many parallels and lessons for quantum computing. Chapter 3 summarizes humankind's development of calculation technologies and the rise of the earliest computers. Like many other technologies, computing required the creation of wildly expensive prototypes and was followed by periods of refinement in both theory and engineering. Over time, these refinements resulted in cost-cutting, and democratization of the technology to large businesses, and ultimately, the consumer. We will show the success of American and British computing prowess as a result of state patronage, and contrast it with a

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press

cutting-edge technology that Germany possessed before World War II that withered for lack of government support.

Quantum computing is a family of approaches for building computers that switch information with quantum interactions, rather than with the electronic interactions that power today's computers. Chapter 4 presents an in-depth history of quantum computing, including the genesis of the field's foundational concepts. Many provocative ideas and engineering projects have a shared genesis with quantum computing including theories of time, theories of emergent complexity, and even whether our own existence is a kind of computer simulation. These ideas were incubated among researchers awash with government support; that support gave them the time and academic freedom to connect the concepts of physics and computing.

Encouraged by thinkers in this environment, Richard Feynman crystallized a vision for quantum computing: that only a computer based on quantum interactions could simulate the complex and probabilistic nature of reality. The *Feynman vision* unifies physics and computing in an effort to understand physical processes. If realized the payoff would be life-changing for humans. Examples abound and are discussed later in this book, but for now consider just one example that could change the prospects for all of humanity: if humans could better understand the basis of a physical process like photosynthesis (one that naturally takes advantage of quantum effects to capture energy efficiently in ways humans have not been able to replicate), we might find ways to harness energy from the Sun far beyond the capacity of existing solar cells. The same insights might allow us to store that energy for when we need it, and then use that energy to grow more food and ultimately feed more people. The Feynman vision is our lodestar for quantum technologies, as it is the most compelling one to support more life and at a higher standard of living.

Not long after Feynman's insight, a different vision for quantum computing arose when scientists discovered quantum algorithms likely to undo encryption systems. These discoveries ignited new interest and investment in quantum computing. They also altered the field's narrative from Feynman's science and exploration vision to something darker: a world where quantum computers are developed to help the world's intelligence agencies discover secrets. Predictions based on this vision hold that quantum computing will bring about a fundamental change to data privacy, a crisis where secrets can no

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press

longer be kept. This *dark vision* for quantum computing is often accompanied by privacy doomsday scenarios that are not in touch with technological and practical realities.

We think the Feynman vision is more likely to take hold, and base our argument in the likely applications flowing from quantum computing in Chapter 5. As a starting matter, the Feynman vision presents more opportunities for profit. Just as importantly, the Feynman vision can be used to scale larger quantum computers. That is, by simulating fundamental processes in chemistry and materials science, an innovator might discover insights making it possible to build a larger quantum computer.

Quantum Computing

Uses nondeterministic nature of quantum interactions to process data.

Capabilities

Simulation in biology, chemistry, materials sciences; will perform some computations dramatically faster than classical computers.

Near-term applications

Simulation of natural processes, optimization, improvements in search.

Outlook

Most challenging and complex quantum technology; requires fundamental science advance to scale devices to have universal, fault-tolerant computing. In the near term, quantum simulators will be the most significant kind of quantum computer.

Large quantum computers do not currently exist and the path to build one is unclear. The encryption-ending vision for quantum computing requires large devices, but also is subject to practical limits that make simple narratives of a privacy doomsday unlikely. In fact, we believe that privacy crisis scenarios, ones defined by shifts in the fundamental assumptions about the power to collect and use data, are likely to come from quantum *sensing*. Quantum sensing is the bigger threat because the technologies are maturing, easier to deploy, and in some cases, countermeasures are out of reach.

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press

We also dispel popular notions about the capabilities and powers of quantum computers. For instance, quantum computers will not "consider all possible solutions to problems" and magically make all computing tasks blindly faster. As we currently understand them, quantum speedups will be limited to a small number of important problems; classical computers will remain in use for all others. Indeed, as they are currently imagined, quantum computers are better thought of as specialized processors bolted onto the side of conventional computers, there to perform specific functions.

Today, some researchers are merely attempting to demonstrate that quantum computers can compute things that conventional computers cannot – what is termed, controversially and somewhat misleadingly, as *quantum supremacy*. Chapter 6 canvasses the state of the science in today's quantum computing landscape.

Quantum computing is still at an early stage: researchers are building the first working prototypes, and others are arguing about whether these machines will ever be more than research curiosities. The fundamental challenge is one of scale: the transistor allowed classical computers to scale for decades. A similar, but so far elusive, breakthrough is necessary to manage the more difficult challenge of scaling a machine that masters quantum states. This chapter discusses the different kinds of quantum computers that have been built to date, their accomplishments, and speculates on what tomorrow's quantum computers might bring.

Quantum communications could be thought of as a merger of quantum sensing and computing. The purpose of this union is to send messages across distances with fundamentally stronger security. Chapter 7 explains the applications and implications of quantum communications. We distinguish between two technologies often combined under the term "quantum communications": quantum key distribution and quantum networking. Quantum key distribution (QKD) involves distributing keys that are information-theoretic secure, thus enabling classical communication over the Internet that is resilient even against an attack with a quantum computer.

The second technology is quantum networking or "quantum internet." Quantum networking involves reengineering network layers to communicate using entangled photons. If achieved, quantum networking will have benefits for confidentiality and integrity; for instance, users would no longer have to rely on network trust as communications become end-to-end. The quantum internet would also

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press

eliminate metadata surveillance, a key advance for communications secrecy.

A quantum network will enable the interconnection of different quantum computers. Interconnection means that one path to building a large quantum computer might be to interconnect several smaller ones over a quantum network.

The outlook for quantum communications is a mixed bag. On one hand, classical alternatives for securing codes against quantum computers – so-called post-quantum cryptography – are well understood and less expensive. On the other, research groups and governments in Asia and Europe are heavily investing in both quantum communications approaches. Their investment might be driven by the realization that while large-scale quantum computing is not currently achievable, quantum communications may be an interim step that primes a nation's technical capacity in the future. Or perhaps China and the EU see the metadata-shielding advantages of quantum communications as an opportunity to shrink the surveillance aperture of the US government.

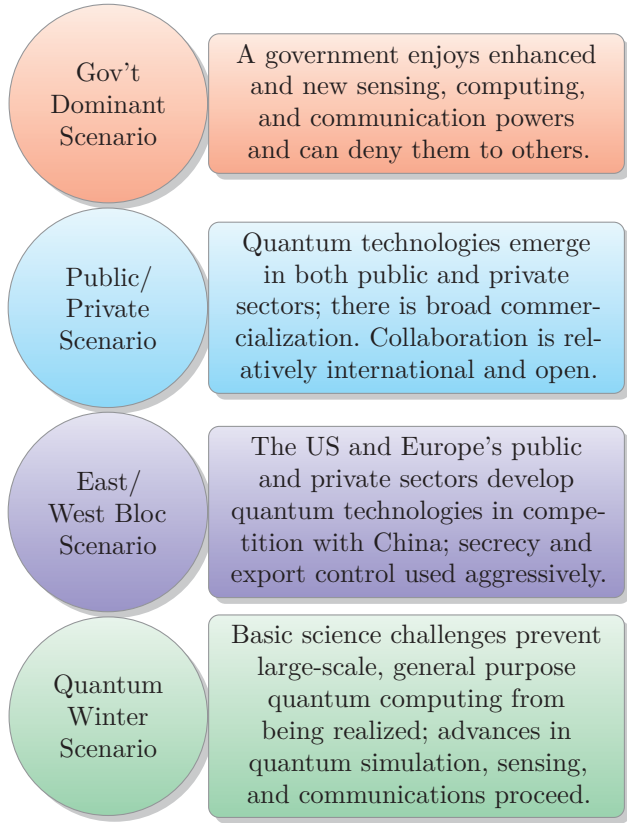
In any case, we believe that it is prudent to move to post-quantum cryptography algorithms as soon as possible, rather than waiting for an announced quantum breakthrough.

Part 10, "Shaping the Quantum Future," turns to the social and policy issues raised by quantum technologies.

There are mechanisms that underlie quantum technologies that will result in a similar development cycle to predecessor classical technologies. We resist heroic innovation narratives that promote quantum technologies as unique and entirely new, because these narratives tend to charm the public, leading to the mistaken impression that existing tools of analysis and comparison are inadequate. Historical comparisons and previous technological revolutions can be used to help understand the implications of quantum technologies. Comparing classical technologies with their quantum counterparts is indeed like comparing dynamite to nuclear weapons: quantum technology is vastly more powerful, but also more specialized: in most cases, quantum technologies will complement, not replace, tools that are in use today.

We anticipate the arcs that quantum sensing, computing, and communications could take in Chapter 8. This portion seeds a policy discussion by modeling four possible futures for quantum technolo-

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press



Scenarios for how quantum technologies could evolve are presented in Chapter 8.

gies. In the first, a government becomes dominant and superior in quantum technologies, enabling it to enjoy the powers of quantum technologies while denying those capabilities to others.

The government dominance scenario is foreseeable because quantum technologies are likely to be expensive and complicated for some time. The expense and complication mean that only large, moneyed institutions will have quantum technologies. Actors with access to outer space will be able to deploy quantum technologies in more powerful ways. Quantum technologies thus have the double whammy of being both institution-empowering and expensive, attributes that mean that masters of quantum technologies are likely to have asymmetric advantages over ordinary people.

In a government-dominant scenario, states and perhaps state-affiliated companies have more power to sense, more power to comprehend sensed data, and more ability to communicate secretly –

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press

and be able to deny these powers to others. To make this explicit, those without quantum technologies will have less sensing, less sense-making, and less privacy from those with quantum technologies. Quantum technologies may result in *strategic surprise*, situations where a nation gains a substantial advantage over competitors, for instance, by using remote sensing to discover hidden facilities or critical infrastructures. The asymmetric advantage is, in a nutshell, why nation states see quantum technologies as a strategic issue much like advances in artificial intelligence.

The second scenario, where public/private partnerships blossom into an innovative landscape that uses quantum technologies broadly, is more likely. We recount the reasons why quantum research is similar to and different from previous technology efforts such as the Manhattan Project and the Apollo Space Program – the most important being that barriers to entry in quantum technologies are lower. Prototype quantum computers can be made for tens of millions of dollars, instead of the billions required by atomic bomb and space research. That price differential means that even startup companies can be strategically relevant in quantum technologies. Strategic surprise in a public/private scenario looks different. Surprise may take the form of a company proposing to eliminate public governance with private governance, perhaps with a smart city that is optimized by a quantum computer.

The third scenario is a variation on the public/private partnership, where such partnerships exist but follow East/West bloc divisions, for instance, separate, quantum technology programs in the US and allied nations primarily competing with China. In both public/private scenarios, innovation blossoms for industrial and consumer applications of quantum technologies. Surprise in a block division scenario might include a different nation taking a fundamentally different approach to quantum computing than other actors and succeeding, causing the other nation to advance in ways others cannot.

Finally, we consider a "quantum winter," a scenario where scalable and general purpose quantum computing cannot be realized in the next 10 to 15 years, leaving just quantum sensing and communications as the most vibrant form of quantum technologies. In this scenario, governments must contemplate surprise coming from other big technology bets. Perhaps one nation squanders billions developing small, ineffectual quantum computers while another becomes technologically superior by focusing on traditional machine learning and automation.

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press

For each of these scenarios, understanding the complex relationships among companies, the market for quantum technologies, and the state is critical for norm development and regulatory capacity. With an understanding of the technology and its possible paths, we turn to the political economy of quantum technologies and policy options in Chapter 9.

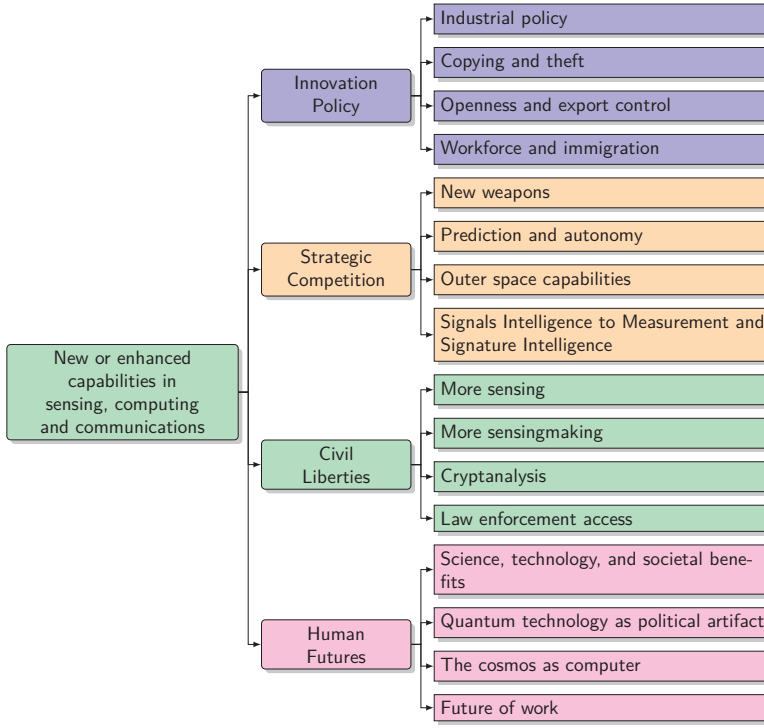
We do not need to draw on a blank canvas when discussing the implications of quantum technologies: many of the questions facing us today faced scientists, engineers, and policymakers during the first half of the twentieth century. This means that we can look to the history of computing and sensing and make reasonable predictions about quantum technologies. The highest-level policy issues include:

Innovation Policy. Although a German inventor had an innovative computer years earlier than the Americans, the German government failed to fund the project. Meanwhile, the US and UK incubated computing in pursuit of military and intelligence needs. Government patronage overcame the initial, high costs of developing computers. Particularly in the US, continued government needs for computing – an *industrial policy* that seeks national technological superiority in computing to this day – kept the industry alive and innovating and eventually created a consumer marketplace. Silicon Valley benefited from decades of Department of Defense patronage, seeding the region for high-technology innovation.

Like classical computing, quantum technologies also require large, multidisciplinary teams to properly develop them. We should cast off romantic narratives about individual, heroic inventors, and see that the path to success will be a group one. Similarly, we must recognize popular libertarian technology innovation narratives that malign or minimize governments' role in technology as specious. If technology development were left to the private sector, America's technical achievements in the twentieth century almost certainly would have happened elsewhere. History suggests instead that governments will be key to the realization of quantum computing, as governments have also been the driver of innovations like global positioning systems and the Internet.

And yet at the same time, the private sector has an important role to play. Barriers to entry in quantum technologies are much lower than in aerospace or nuclear weapons, making private companies strategically relevant in the field. Private sector investment in

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press



The highest-level policy issues implicated by new capabilities and improvements on classical methods from quantum sensing, computing, and communication.

quantum research is substantial, sometimes in parallel with government funding and sometimes separate from it. The balance of public and private funding shapes economic incentives and ultimately what applications will get developed first.

Openness. Sometimes, important technologies are developed by researchers in secret government organizations and then re-invented in public at universities or corporations. One well-known example is public key cryptography, which was first discovered, then discarded, by the UK communications intelligence agency GCHQ. Public key cryptography was then re-invented by a group of US university professors in 1976 and 1977. As a result, US companies commercialized the technology and made billions; UK companies didn't.

Several precursor developments to quantum technologies, such as the transistor and the laser, played important roles in Cold War weapons systems. Fortunately these technologies were developed at organizations interested in commercializing them, rather than keeping them bottled up. We can easily imagine an alternative history

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press

where the transistor was tightly controlled and the computing revolution was delayed by decades, or was centered in Japan rather than the US. Similarly, the relative openness of quantum technologies will affect how these technologies are used but also who can develop further enhancements to these technologies.

While nations develop quantum technologies, governments must make innovation policy tradeoffs. A policy of openness might grease the wheels of innovation and democratize quantum technologies, leading to innovations that are unpredictable and wonderful. Openness might just as well allow nations to free ride on the investments made by others, and even come into parity with the powers developed by China, Europe, and the US. Nations have several levers including export controls, patent secrecy, and classification to shape who can get access to the leading-edge technologies. Nations that fear strategic destabilization, for instance those that fear that quantum technologies will allow detection of stealth jets and silent submarines or compromise legacy communications systems, might pursue something akin to a non-proliferation strategy.

The Value of Basic Research. Many of the breakthrough ideas in QIS that are now attracting billions of dollars in investment started off as fringe ideas in academic and corporate research organizations. This shows once again the value of allowing – and funding – basic research that has no obvious near-term payoff. For policymakers this presents a quandary, because of the challenges posed in distinguishing solid basic research proposals, that deserve funding, from wayward or even crackpot ideas that suck resources but never produce anything of value.

One way to minimize the risk of funding basic research is by increasing the size of research funding in general and earmarking a percentage for basic research, so that funding managers can pursue innovative ideas without risking their own professional reputation, and by giving more leeway to redirect or repurpose funds with minimal administrative overhead. The current path is concerning, because in the five decades since the birth of quantum information science, the amount of US government funding spent on basic research has steadily declined, while the administrative restrictions associated with using those funds have steadily increased.

Immigration Policy. Just as quantum physics and early computing in the US and other liberal nations benefited tremendously from the bright lights from around the world, today's quantum technology

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press

companies assemble experts from all over the world to solve fundamental challenges. Nations that make it easier for skilled scientists to emigrate and to gain access to sensitive new inventions will have advantages in quantum technology development.

The future of the US as a quantum technology power depends on our immigration policy. Many students and researchers working within the US on QIS are foreign nationals. If individuals are unable to remain in the US at the completion of their studies, US universities today will train the nation's competitors of tomorrow.

Virtuous Cycles and Winner-take-all Risks. Computers can be used to build faster computers, allowing computers over time to grow in speed, capacity, and efficiency more quickly than other kinds of technologies. This is known as a *virtuous cycle* and it is not present in most technological endeavors. For instance, faster aircraft do not permit aircraft manufacturers to build significantly faster aircraft.

Classical computing enjoyed several kinds of virtuous cycles, where advances in computing justified investments that produced even faster computing. Quantum computing will likely enjoy such a virtuous cycle once computers have reached the scale that they can be used for simulating basic physics. Quantum sensing may enjoy such a cycle; quantum key distribution almost certainly will not.

A strong virtuous cycle also raises the risk that the first group to make a stable quantum computer enjoys a virtuous cycle that is unachievable by competitors. We have to anticipate the risk that quantum computing may be a winner-take-all technology.

The Risk of Hype. The policy discussion also highlights concerns that the private sector and investors have about the technology. Quantum technology, as a field, is particularly vulnerable to unfounded claims of capabilities and unlikely paths to profit. The precursors for fraud are all present: privately held companies with fewer transparency requirements than others, technology optimism, boosterism, limited availability of independent expertise, complexity, and a class of employees and investors who could make a fortune if a company merely enjoys speculative success. Decisionmakers need to understand whether the quantum market is "frothy." Answering this question requires knowing the difference between quantum foam (a real quantum phenomenon) and quantum fluff (a classical phenomenon as old as markets). Beyond investor losses, one risk of hype is that it could lengthen a quantum winter, making it more difficult

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press

to recognize a thaw where investment in quantum computing becomes fruitful again.

Strategic Competition. Nations are spending lavishly on quantum technologies because of the risk of strategic surprise, the notion that a nation will somehow gain a fundamental, decisive advantage over others. Here too, the history of conflict, military and intelligence investments in technology, and norms of conflict all help predict how quantum technologies might be used. Parallels can also be drawn from existing logistical limits on conflict, such as how nations decide to use limited, valuable resources in situations of uncertainty.

Strategic competition shares space with innovation policy concerns. Nations' strategic goals may rest uneasily with companies' desire for profit from their quantum inventions. Companies will want to sell their products and services for many purposes, and will be concerned with a different kind of secrecy: the protection of their engineering secrets.

New Weapons. At the same time, strategic concerns may motivate greater controls on quantum technologies, especially as quantum technologies' dual-use nature is realized. While use of nuclear weapons comes with a taboo, governments have been willing to use conventional devices that create nuclear-like effects. Quantum simulations intended to improve processes in peaceful contexts could be re-purposed to create new, more powerful, or more discriminate conventional weapons. We have to contemplate use of quantum simulation to create biological, chemical, and even genetic weapons.

SIGINT and MASINT. Even without simulation, militaries will find the intelligence, surveillance, and reconnaissance uses of quantum sensing irresistible. The last half century has been characterized by intelligence power gained by signals intelligence (SIGINT) prowess, but quantum communications might limit that power. The next century may be defined by greater measurement and signature intelligence (MASINT), brought about by electromagnetic and gravimetric quantum sensors. Militaries might soon find it impossible to hide matériel and their current secrecy strategies, such as using underground facilities, may be rendered ineffective.

Complementary Technologies and Space Programs. As with other innovations, the future of quantum technologies will be shaped by the availability of complementary technologies that make adoption of quantum technologies easier or implementations more powerful. In

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press

the former category, improvement of precursor technologies such as lasers and single-photon detectors lower barriers to entry for those who wish to develop quantum technologies. In the latter, nations that have outer space launch capabilities can do more with quantum technologies than nations limited to terrestrial applications.

Civil Liberties. Privacy and fairness tussles loom large as quantum sensing devices become less expensive and smaller so that they can be used in more environments, including mounted on unmanned aerial vehicles. With the power to see through roofs and walls, or as sensing peers into the body and possibly the human mind, society will have to reconsider boundaries and rules on what may be observed.

Not Just Sensing, More Sensemaking. As quantum computing enables more complex *sensemaking* through link analysis and other techniques, those who possess quantum computers will be able to understand more about the world than those who do not. That is, even if two parties possess the same "facts" about the world, the party with quantum technologies might know more about the world.

Cryptanalysis. The most common risk articulated about quantum computers is their potential to undo the most popularly used encryption systems in the world. This risk is real, but as we explain in detail, also greatly overstated. Cryptanalysis will require a large quantum computer, time to perform the analysis, and of course access to the underlying secrets being discovered. The greater near-term risk to civil liberties comes from quantum sensing advances.

Devolution to Law Enforcement Agencies. Powerful tools developed in intelligence and military contexts tend to find their way into the hands of law enforcement agencies, even on the local level, and often without political oversight. How can policymakers prepare intelligence, military, and law enforcement agencies to contemplate the implications of quantum technologies? For many kinds of surveillance enabled by quantum technologies, ordinary people are unlikely to ever develop countermeasures. Window coverings and fences are effective countermeasures against classical privacy intrusions, but to keep up in the quantum age, homeowners would have to install electromagnetic shielding. Norms and laws will have to suffice to protect privacy.

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press

Human Futures. Quantum technologies present tremendous potential for societal benefits, particularly if the Feynman vision for quantum computing is realized. Understanding quantum-level phenomena may make it possible to support more human life and at a higher quality of living while mitigating damage to the environment.

Is our Reality Just a Computer? Existential crises might lurk in the shadows of a bright quantum technology future. As people realize that the basis of these benefits is the random interactions of quantum events, what will this mean for how people conceive of meaning and their place in the universe? Seeing the world as random might unmoor us from ideals of free will, undermine individual responsibility, and spoil the notion of humans' special place in the universe.

Future of Work. In practical terms, quantum sensing and computing might erode the barriers to creating more capable systems. As computers become more capable, humans' range of useful work may shrink, undermining our

Quantum Communication

Uses quantum states to transfer data or to ensure confidentiality and integrity.

Capabilities

Creates fundamentally stronger encryption keys, may enable end-to-end data transmission with quantum states.

Near-term applications

Key distribution systems already realized, works in progress to create more ambitious quantum internet that could block metadata surveillance and even interconnect small quantum computers to create a grid system.

Outlook

Mixed: some applications are less challenging than computing, and implemented in small systems. More ambitious achievements require basic science breakthroughs to store quantum states. Prospects brightened because of massive investment in China and the EU, as well as precursor advances in sensing devices.

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press

value as economic actors. If computers also become more creative than people, the technology will present a challenge to human meaning and value far worse than privacy invasions. *An inevitable downside* of quantum sensing and computing is interference with privacy norms. *The downside* is a future where humans make themselves irrelevant with an invention that outshines our creativity and ability to take action.

Quantum Technologies as Political Artifacts. Before those existential questions are realized, we should contemplate the political norms that may come with quantum technologies. Quantum technologies, like the atom bomb – a quantum weapon – are associated with specific forms of power, authority, and secrecy. Today, elites from educational, government, and (mostly) defense-industrial base companies can understand and employ quantum technologies. For the foreseeable future, much like the history of early computing, powerful institutions will be the exclusive adopters of quantum technologies. Who can understand and adopt quantum technology matters, because their uses of the technology will dominate for some time.

As with early computing, quantum technologies will at first be used to solve the kinds of problems that powerful institutions are concerned about. Quantum technologies could thus be politicized, and a quantum taboo could emerge.

Finally, Chapter 10 ends our exploration of quantum information science. We are at the cusp of a quantum revolution, yet we have not countenanced the social challenges presented by the technology. We have the opportunity to set normative goals for how the technology is applied. The choices will have to be taken and we hope this book helps elucidate our options.

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press

https://doi.org/10.1017/9781108883719.003 Published online by Cambridge University Press