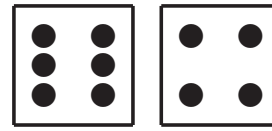

The Quantum Age: Conclusions

We are at the cusp of a quantum technological revolution. Quantum sensing, computing, and communication offer some significant improvements on classical technologies, in some cases they create fundamentally new capabilities.

This book begins a conversation on these consequential quantum technologies, as they reshape how companies and government measure and observe, communicate, and make sense of the world through simulations and problem solving.

Many technologies are deployed by companies and governments on society with weak or underconceptualized plans to deal with the technologies' implications. With Quantum Information Science, attempts to cast implementations of quantum technology as entirely novel are inapt. Novelty narratives may be a product of hype and confusion, but regardless of the purpose of their use, arguments of novelty may flummox policy and planning processes.

This book has explored the invention of many technologies, some novel, some not. We have argued that historical analogy is a good guide for analysis of quantum technologies. When it comes to quantum technologies, some of its most promising applications are (dramatic) improvements on classical methods, such as simulation and code-breaking (see Chapter 5). But we experienced similar breakthroughs 80 years ago, when the first digital electronic computers were deployed for the very same purposes: physics simulations and code-breaking. While quantum does offer entirely novel capabilities,

https://doi.org/10.1017/9781108883719.015 Published online by Cambridge University Press

such as quantum cryptography and quantum networking (see Chapter 7), we believe that these will not be worth the extra expense and complexity for broad deployment for the foreseeable future.

Quantum technologies are quickly arriving. Even if the most hyped promises in quantum computing are not realized in the next decade, in the near term quantum sensing could shift relationships irrevocably. This book has painted the landscape of quantum's implications – from nation-state concerns of strategic conflict, intelligence gathering, and law enforcement activities; to the concerns of companies that may be subject to industrial policy priorities and restrictions; to the level of the individual who may face institutions with great asymmetries in sensing and sensemaking power. We should start deciding now how these technologies will be used, before others make the choice for us.

We are both optimistic and excited about the potential for quantum technologies to improve our lives. A careful overview of the field suggests the contours of those improvements.

10.1 Quantum Computing Winter Is a Probable Scenario for 2030

Chapter 8 modeled possible scenarios for quantum technologies, in order to motivate a policy discussion. We think it important to seriously consider the likelihood of the quantum winter scenario in the near term. Recall that in our quantum winter scenario, large-scale quantum computers simply cannot be realized in the next decade or two. Nor do applications emerge in quantum simulators or smaller-scale devices that are compelling enough to trigger virtuous cycles. In this scenario, quantum sensing advances because of its maturity and sound economic drivers, mostly from medical, law enforcement, defense and intelligence application. But quantum communications loses steam as cryptanalysis threats fade.

We believe that there are two factors that make quantum winter probable. First, no consensus has emerged on a substrate that will enable large-scale quantum computing. In simple terms, whereas computing vendors rushed to adopt the transistor in the 1950s, there is no similar technology that presents itself for quantum computing. Second, no technologist, no company, no actor in the quantum computing space has implemented an application that is truly game-changing – a reason to use a quantum computer rather than a con-

https://doi.org/10.1017/9781108883719.015 Published online by Cambridge University Press

ventional one. To create a virtuous cycle, quantum computing needs an application that ordinary businesses find worthwhile to invest in.

The most pressing risk of a quantum winter scenario is an unwillingness to recognize the possibility and plan for it.

Specifically, we are not concerned about the private companies pouring investor dollars into quantum computing. These companies will be able to shift more quickly than other institutions if a quantum winter comes. We are concerned that a hard freeze may damage our capacity to evaluate when the thaw is upon us – and that nations that fail to pivot quickly will be significantly disadvantaged.

One signpost of a thaw could be the widespread agreement on a substrate for stable, scalable quantum computing.

10.1.1 Public/Private Scenario

We are hopeful that the public/private research and development scenario is the most likely future for quantum technologies. This scenario is most likely because state-of-the-science developments are being achieved in several nations, sometimes in government/private partnerships, but also by private companies acting alone. Today's private sector does not have the commercial landscape of the 1940s. Large, sophisticated technology companies such as Google and Microsoft have more cash on hand than some nation states, and these companies see billions more in profit from materials science, chemistry, and drug development applications of quantum simulation.

In the public/private scenario, significant breakthroughs and applied development continue to occur in both the public and private sectors – not just in the US, but also in quantum technology powerhouses like Canada, China, Germany, the Netherlands, and the United Kingdom. Unlike strategic technology developments of the past such as the atom bomb and global positioning systems that were only in the reach of governments, today the private sector has both the financial resources and scientific capability to make nation-state level investments and realize accomplishments – as evidenced by the recent achievements of the private outer space industry. Governments might try to limit this innovation with export controls. But, again unlike the development of the atomic bomb, no single country is dominant in quantum technologies, meaning that there are likely to be many sellers of controlled technologies.

Innovators will have high-powered incentives to evangelize quantum technologies and find many uses for their inventions outside

https://doi.org/10.1017/9781108883719.015 Published online by Cambridge University Press

defense and intelligence. For all these reasons, we think the quantum technology future is bright, and will be open relative to previous technology revolutions. The public/private quantum scenario is the technology's brightest because of incentive alignment. Quantum technology's greatest contributions to people – and to companies' profit statements – will come not from cryptanalysis but from advances in material science, chemistry, medicine, and every field that could benefit from precision engineering, from consumer durables to manufacture of gadgets.

10.2 Assessing the Next Decade of Quantum Technologies

Whether or not the year 2030 sees us in a quantum winter, we believe that the 2020s will be good times for those involved in the research and business of quantum information technologies.

10.2.1 Prospects for Quantum Sensing

Quantum sensing (see Chapter 2) is already a mature, successful technology. Currently in its first-generation, just one form of quantum sensing – Magnetic Resonance Imaging – has contributed to the treatment of countless people. Other first generation technologies like the atomic clock made it possible to have reliable, worldwide position, navigation and timing devices thanks to GPS.

For the coming decade and perhaps beyond, second generation quantum sensing will be the most exciting class of quantum technology, providing not just improvements on existing methods but new capabilities as well. More exquisite sensing of magnetic and gravitational fields has obvious implications for military, intelligence, and law enforcement, but uses in the private sector will abound: medical imaging technologies that are both more precise and non-invasive; sensing underground deposits of minerals and valuable materials will benefit mining interests; high-precision manufacturing, possibly including futuristic engineering production runs that yield *identical* artifacts because they are assembled at the atomic level.

Contrary to many media and policy narratives, the next novel and troubling threats to privacy will likely come from quantum sensing rather than encryption-cracking quantum computing. Already clever technologists are deploying ever-smaller sensors on satellites and on unmanned aerial vehicles. These technologies will be used to peer into private spaces and the kinds of countermeasures ordinary

https://doi.org/10.1017/9781108883719.015 Published online by Cambridge University Press

people possess – window blinds and doors – simply will not provide protection.

Quantum sensing is a precursor technology for both computing and communication. As such, quantum sensing will directly or indirectly benefit from investment in other quantum technologies. Mastery of quantum sensing is necessary for quantum computing, and as that mastery develops, entrepreneurs will likely find many non-computing uses of quantum sensors to benefit society.

10.2.2 Prospects for Quantum Computing

Quantum computing will be the most exciting form of quantum technology, if large-scale devices can be developed. Quantum computing's biggest potential contributions might change life as we know it. The spotlight on cryptanalysis (see Chapter 5) has left these other uses of quantum computers in the shadows, and as these lesser discussed applications are realized, cryptanalysis will be left in the shadowy recesses of government agencies. It will be similar to what happened with electronic computers: yes, there is cool stuff going on behind the curtain, but there will be so much going on in front of the curtain that most of us won't notice.

Richard Feynman's vision of quantum computers – as simulators for physical systems – is not only more likely, but more beneficial for humankind than code-breaking. We can imagine advances in materials science letting firms create products with new properties; advances in solar cells making energy capture more efficient; simulations in chemistry leading to new classes of drugs and improvements on existing ones; and unraveling some of nature's mysteries, like photosynthesis and nitrogen fixation, enabling humans to feed more people. And that's just the beginning! Just like the personal computer revolution, the quantum computing revolution will produce unimagined uses and benefits. Perhaps cryptanalysis will be remembered faintly, like the old artillery tables that drove computing in the 1940s (see Chapter 4). Cryptanalysis' role will be secondary because the process is harder than popularly understood, because countermeasures are already available, and because companies will generate more profit pursuing other uses of quantum computers.

The fundamental technological challenges in realizing quantum computing (see Chapter 6) are more difficult than those faced by classical computing. Classical computing's breakthrough came with the transistor and then the integrated circuit, together a massive

https://doi.org/10.1017/9781108883719.015 Published online by Cambridge University Press

improvement on vacuum-tube approaches. Semiconductors enabled decades of scaling in power, miniaturization in size, and reduction in cost. Quantum computing has yet to experience its own transistor revolution because of the fundamental challenge of managing quantum states. Scaling a quantum computer becomes more difficult with each additional qubit; the same constraint has not limited classical computing until recently where quantum effects have complicated the development of 7 nanometer chips.

Quantum computing requires a basic science breakthrough similar to the invention of the transistor. That breakthrough must enable the management of an enormous number of quantum states, coherence over long periods, and the ability to measure the managed states. The basic science breakthrough may lie in photonic approaches, or in the topological qubit, or ion traps, but we believe that it is unlikely to occur in superconducting media currently used to make the largest quantum computers. Until scaling is possible, many of the most discussed applications of universal quantum computing simply cannot be realized. Instead, scientists will build special purpose devices that benefit from fantastic computational power, but only perform limited experiments, like the analog devices of early classical computing.

10.2.3 Prospects for Quantum Communications

Europe and China have embraced a focus on quantum communications in both of its forms, quantum key distribution (QKD) and in quantum networking/internet (see Chapter 7). Because these nations have substituted for the market, quantum communications will receive a boost that normal business drivers would not produce. In effect, nations will subsidize the development and marketization of quantum communications, at least in the form of QKD.

Defense against the future is the driving rationale for QKD adoption. If one's secrets must remain hidden for 10, 25, or 50 years, one must have a strategy to address growing computational power from adversaries. QKD, because it is information-theoretically secure rather than relying upon number theory for security, should provide protection against future attackers with large quantum computers. Today many working systems use QKD for distributing keys but AES-256 for actually encrypting data. Although this is likely to be safe, AES-256 *could* be cracked at some point in the future, even using classical or quantum approaches. As the speed of QKD improves,

https://doi.org/10.1017/9781108883719.015 Published online by Cambridge University Press

the time that each AES-256 key is used will decrease. At some point there may be no need for AES-256 at all.

Post-quantum cryptography is an alternative to QKD that uses computationally-secure algorithms that are believed to be resilient against quantum computers. But reliance on post-quantum cryptography may be misplaced; clever scientists could discover a new algorithm that unscrambles ciphertext quickly, or perhaps quantum computers scale massively, so much so that brute force can undo the cryptography. The switch to post-quantum cryptography is essential, but conversion to QKD requires an analysis of institutions' risk appetite and the time value of their secrets. For many companies, operations plans may need only be secret for a business cycle, but for governments, decades-long secrecy requirements may justify extra precaution.

The prospects for quantum internet are weaker than for QKD. It is not clear to us why institutions would adopt quantum internet given implementation complexities. One answer lies in network reliance, or rather the lack of it. The classical Internet is akin to the shared, "party lines" of the early telephone network. Many strangers can listen in. Interception and copying is easy. We use encryption to shield our content, yet encryption cannot prevent revealing forms of investigation based on network metadata – who is talking to whom, how often, and when. Many people use the word *trust* to describe what really is *reliance* on networks, with their unknowable operators, paths, and vulnerabilities. That is, they *trust* the network not to violate their security policy, because they have no mechanism for *assuring* that the network does not. The network is *trusted*, even though it may not be *trustworthy*.

Quantum internet likely takes the majority of SIGINT opportunities out of the equation, making communications end-to-end secure. Operators of a quantum internet need still worry about side channel attacks on endpoint devices and against the people who use them. Availability can be compromised by attacks on the fiber itself, although free-space systems have no such problem. Operators will have to discover countermeasures against tampering and use physical isolation for quantum repeaters. But if the quantum internet is developed, users can deny adversaries the ability to capture their communications *and* deny adversaries access to metadata analysis on communications. Adversaries will not know when or with whom communication is taking place. These metadata-denying advantages

https://doi.org/10.1017/9781108883719.015 Published online by Cambridge University Press

may be the driving rationale behind investment in China and the European Union, in a kind of technological revanche against the "golden age" of SIGINT. Quantum internet would actually bring about intelligence agencies' greatest fear, the notion that communications could "go dark" and not be available for analysis.

10.3 Law and Policy Priorities for the Quantum Age

Chapter 9 presents a full list of policy issues raised by quantum technologies. Our approach recognizes that innovators sometimes present technologies as entirely novel, flummoxing the public and policymakers about potential regulatory implications. Recognizing that quantum technologies are mostly improvements on classical methods, and that many others have implications that are predictable, we draw upon lessons from the history of technology to elucidate likely development cycles and challenges to governance.

If limited to just five challenges and approaches, we think the following are the most significant:

Innovation policy Quantum computing is still in a pre-transistor-revolution phase in its development. To realize scalable, fault-tolerant quantum computing will require an enormous and decades-long commitment of investment in basic research. The US, after a period where policymakers looked to private technology giants to assume more of the responsibility for basic research, now invests billions in QIS research. From the Apollo Space Program to the GPS constellation to the Internet itself, the US government has been a humble driver of innovations that devolve to the general public, accruing to the benefit of all, and in the process, educating and training legions of people. The government stands as a counterexample to the overhyped, popular narrative of the lone inventor who saves the day. The lone inventor narrative is particularly unlikely in quantum technologies, because of the need for multidisciplinary expertise. We are more likely to realize scalable quantum computing with healthy government patronage, more likely to avoid private-company winner-take-all stratagems, and once quantum computing arrives, government programs are more likely to incubate the people necessary to lead a quantum computing revolution.

Immigration To build the expertise and multidisciplinary talent, among the quickest solutions is a liberal immigration policy. Ap-

https://doi.org/10.1017/9781108883719.015 Published online by Cambridge University Press

proaches that ease the burdens with visiting, studying in, and staying in quantum technology hubs will create advantages. We recount how most PhDs in computer science and engineering are "non-resident aliens" in the US, and suggest that liberal immigration policy could let us keep more of those highly trained people in America. The anti-immigration, even xenophobic emanations from the US government during the Trump administration pushed scientists to Canada, Germany, and the Netherlands, countries with high standards of living and major quantum technology centers. We risk a brain drain unless we create a more welcoming environment and ease the burdens to permanent residence in the US.

Strategic competition Similarly, to realize the quantum age, nations should invest in parallel, enabling technologies. Outer space programs are especially critical in this regard. Nations that have space programs will be able to enjoy quantum sensing and communications capabilities in ways that nations limited to terrestrial deployment cannot. Also, we will realize more quantum technology innovation if inventors can rely on and integrate existing components in their products. A visible example comes from Jian-Wei Pan and Chao-Yang Lu's optical Jiuzhang quantum computer (see Chapter 6, p. 250), a close inspection of which reveals it to be constructed of many components from American optics maker ThorLabs. The US needs to carefully weigh the benefits from levying export controls on more quantum technology precursors against the risks that such innovation will occur anyway, but with components manufactured by foreign, state-supported competitors.

Human futures Through no fault of their own, people are inheriting a world where the traditional sources of human value, as worker, thinker, and fighter, will narrow thanks to automation. Even those on the top of the pile, like the computer programmer, are the focus of intense automation efforts. With our American conception of human value so tied to our economic outputs, the fuse on our incentive and reward system shortens with every step technologists make in automation. No one is safe from automation.

The European campaign to enshrine and expand basic human rights could be an effective hedge strategy for technological futures. Embracing a positive rights system (a right *to* some good, such as

https://doi.org/10.1017/9781108883719.015 Published online by Cambridge University Press

education or a basic income, rather than a negative system that is concerned with freedoms *from* government) might help us transition to a world where technology itself has narrowed the workplace.

We ought to be having conversations now about our technical-economic trajectories. Ideas that might seem esoteric now, such as universal basic income, might be the only economic future for most people.

The social benefit scenarios from quantum technologies will be life-changing. But in a highly stratified economy such as ours, those benefits could both be realized and still leave people in a system more feudal than free.

Civil liberties We assess that the greatest threats to civil liberties in the near term will come from quantum sensing rather than quantum computers. As sensing devices are miniaturized and mounted on aerial and satellite platforms, quantum-equipped actors will see more than others, and in some cases, into private spaces.

Nation states should adopt technology-neutral legal frameworks[1] to address advances in quantum sensing that will create new capabilities to peer into private spaces and technological protections.

Chapter 9 discusses one legal approach, the European human-rights-based framework for addressing technological invasions of privacy by law enforcement. Applied with care, the European model is flexible enough to both anticipate new practices and subject them to substantive limits. Under the European model, governments must seek legal authorization to use investigative methods, those methods must be necessary for a specific law enforcement purpose, and the methods must be proportionate. The effect of these high-level principles is to require governments to disclose their surveillance methods, and to limit the creep of powerful technologies into general criminal deterrence efforts, while allowing aggressive techniques when a credible and specific threat arises. There are now case-law examples of European courts limiting new technologies, such as face recognition, and preventing new technologies from being used for general criminal deterrence, and even for general terrorism deterrence.

[1] Not because technology is neutral, but rather because so many US limits on surveillance are keyed to specific technologies or to interference associated with physical touching. A technology-neutral approach would abstract away from the specific technology used and provide legal certainty about acceptable conduct (Koops et al., "Should ICT Regulation Be Technology-Neutral?" (2006)).

https://doi.org/10.1017/9781108883719.015 Published online by Cambridge University Press

Turning to technological countermeasures, it is prudent for institutions to switch now to post-quantum encryption algorithms. Privacy law also suggests several interventions that make sense now, such as limiting data hoarding so that these are not captured decades from now and decrypted.

We are at the cusp of a quantum technology revolution. We hope this book anticipates the social challenges presented by quantum sensing, computing, and communications technologies. It is now up to policymakers and innovators to pursue normative goals for how the quantum age will be realized.

https://doi.org/10.1017/9781108883719.015 Published online by Cambridge University Press

https://doi.org/10.1017/9781108883719.015 Published online by Cambridge University Press