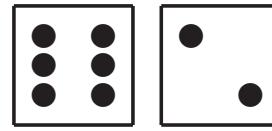

Quantum Technologies and Possible Futures

What are the most likely paths for quantum technologies? Are we facing a future where quantum technologies are the domain of governments, with asymmetric powers to collect information about us and to make sense of it? Or might the future bring some other landscape, where quantum technologies protect the communications of the average person and quantum sensing helps us diagnose and treat illness?

This chapter uses scenario analysis to seed a policy discussion for quantum technologies. We envision four likely outcomes of the quantum technology race, and these different visions provide motivation for contemplating the strategic, political, and social dimensions of quantum technologies. The next chapter considers how different policy measures could address these risks.

8.1 Do Quantum Artifacts Have Politics?

Langdon Winner, in his seminal 1980 article, "Do Artifacts Have Politics?",[1] argued that "technical things have political qualities." This is different from the popular notion that "technologies are seen as neutral tools that can be used well or poorly, for good, evil, or something in between," he wrote.

The notion of technology neutrality is a powerful one, adhered to by many. Such adherents observe that technologies, what Winner calls *artifacts*, are just tools wielded by individuals who decide

[1] Winner, "Do Artifacts Have Politics?" (2018).

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

how to use them. A hammer could be used to build your home or to break your neighbor's windows. But Winner's argument is more nuanced and strikes at a deeper level. It is not that the individual is blameless or without control, it is that the tool shapes the possible and the broader social landscape. Winner argued that some technologies are "inherently political" in two senses. First, a technology can be adopted to settle a contested issue. For instance, internet users may value anonymity at times, but an advertising company that develops web browsers might deploy its software so that users are always identified and no real chance of anonymity is possible. The advertiser's web browser settles the debate between anonymity and perfect identification in favor of its own preferred outcome.

Second, and more problematically, a technology might require a certain political, economic, or social order. These are *inherently political technologies*. To press the point, Winner contrasts forceful examples: nuclear power and solar energy. A society with the power of nuclear fission or fusion cannot allow the technology to devolve to ordinary citizens. Instead, only powerful institutions secured with military-like safeguards can possess these technologies. Indeed, federal rules specify that sites with special nuclear material must have trained, qualified, ballistic-armor wearing guards in possession of assault rifles, shotguns, and handguns.[2] Even with these safeguards, civilian technologies such as nuclear power present fantastic risks. Just imagine if the September 11, 2001 hijackers crashed a jet into the Indian Point nuclear power plant, just 36 miles from Manhattan, instead of the city's World Trade Center. Atomic energy requires centralized political, economic, and social power arrangements because of the risk of misuse, accident, and disaster.

Consider solar power as a counterexample. Solar power is distributed, often on the roofs of homeowners or in community-clustered solar farms. Solar power has its disadvantages and its own costs, of course. But Winner's point about its politics still holds: solar power leads to different political, economic, and social orders. A world that invests billions in solar energy is one where communities and even individuals can have both policy and technical control over energy generation and storage. There is no need for armed police, secrecy, or worry about widespread disaster. In fact, because it is distributed widely and to individual citizens, solar power may be resilient against

[2]See 10 C.F.R. Part 73.

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

the very attacks we are so concerned about with regard to ordinary power stations.

Nuclear power – a quantum technology – was identified by Winner as inherently political. But what about quantum sensing, computing, and communications? There is an obvious path to quantum technologies becoming inherently political. In this path, quantum technologies are shaped by the small elite who understand and can use them for purposes that are political, such as military and intelligence uses. For a historical comparison, consider early computing, which was dominated by military and industrial applications (see Chapter 3). Renowned MIT computer scientist Joseph Weizenbaum characterized the computer as fundamentally a conservative force, one that allowed institutions to maintain and centralize their power.[3] Alas, democratization with the personal computer revolution changed public perceptions and the political possibilities of computing. Today, the personal computer is seen as a tool of creative expression and entertainment and few remember its early uses for artillery tables. But quantum technologies will not necessarily see a personal computing revolution. Today, only an elite few from powerful institutions can understand and use quantum technologies. Quantum technologies might become associated with the needs of this military-intelligence elite, perhaps even earning a "taboo" or taint as did mainframe computing.

8.1.1 Threat Modeling

Threat modeling is a technique for understanding the different ways technology can be used to attack, be attacked, or fail, and helps prepare organizations to mitigate these threats in a systemic way. Threat modeling can be used in software development to understand the complex dependencies and vulnerabilities in enterprise systems and, as a result, develop software that is more secure and resilient. Adam Shostack created a straightforward, four-step model for security threat modeling[4] which we have adapted to anticipate the likely ways that adversaries could use quantum technologies.

In Shostack's model, one begins by defining the problem being analyzed. Quantum technologies, as a field, are too broad for analysis. Some reductionists might argue that most modern technologies must be viewed as quantum technologies – even classical electronic

[3] ben-Aaron, "Weizenbaum Examines Computers and Society" (1985).
[4] Shostack, *Threat Modeling: Designing for Security* (2014).

computers – because their functions are best described using concepts from quantum mechanics such as electrons, photons and atoms. Such reductionist approaches are unhelpful. Instead, here we cordon off quantum technologies from others by restricting our analysis to those technologies that specifically leverage quantum effects in order to perform some useful function.

As discussed in Part 01, our tripartite categorization decomposes "quantum technologies" into quantum sensing, quantum computing, and quantum communication. These three share the characteristic of gaining utility from harnessing quantum effects, but each presents challenges and uses so different that they are recognized as separate fields.

Drawing from our previous chapters, we assume the following in this chapter's analysis:

- All sectors will continue to adopt quantum sensing, resulting in sensors that are less expensive, smaller and more powerful. Some sensors will be mounted on satellites, some will be mounted on unmanned aerial vehicles, while others may be in ground vehicles, handheld, or even in fixed locations.
- Intelligence and military agencies, particularly in countries with space programs, will implement quantum sensing devices to detect both hidden matériel and to understand adversaries' infrastructure, as discussed in Chapter 2.
- Programmable quantum computers that are large enough to solve useful problems (as discussed in Chapter 4 and Chapter 5) will be built within 10 years.
- Quantum Key Distribution will be *selectively* adopted to secure data in transmission; most users will be content using post-quantum-computer encryption schemes for the majority of uses, as discussed in Chapter 7. These algorithms will be standardized, broadly deployed, and become the default encryption technology for key exchange.

8.1.2 Future Quantum Technology Scenarios

In Shostack's framework for threat modeling, analysts define a problem and then ask broadly, "what could go wrong?" In the computer security context, the most relevant risks are known by the mnemonic

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

STRIDE: **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service, and **E**levation of privilege.[5]

Turning to quantum technologies, the dynamics go far beyond STRIDE. Quantum technologies could alter world order, with certain nations gaining important advantages over others. For example, quantum sensing might impart such a dramatic advantage that it causes nations to focus their initial attack on each other's satellites. Competition for advantage could also alter innovation strategies, with some nations racing ahead in hopes of being the first to achieve benefits, while others might realize that their optimal strategy is to copy – or steal – the innovations of first movers.

To explore what could "go wrong" – and go right – this chapter explores four high-level scenarios[6] for quantum technologies:

- **Government Superior and Dominant**: where a government possesses more capabilities than all others and can deny others the ability to acquire or use quantum technologies;
- **Public/Private Utopia**: a landscape where companies and governments share different levels of prowess in quantum technologies;
- **Pubic/Private East/West**: a version of the public/private landscape colored by East/West bloc competition;
- **Quantum Winter**: the possibility that quantum technologies ultimately fail to be consequential, similar to the "AI winters" that chilled the field of artificial intelligence in the 1970s and 1980s, where hype cycles were followed by disappointment and dormancy.

8.2 Scenario 1: Government Superior and Dominant

One possible future scenario is a world where a major government – likely the US or China – achieves superiority in quantum technologies, and uses that superiority both to maintain their technological dominance and as an enabler to take actions without significant interference by others governments.

This scenario is based on the concepts of *deterrence theory*. Nations mostly seek superiority not to win conflicts, but to prevent

[5] Shostack, "The Threats to Our Products" (2009).

[6] Heuer Jr. and Pherson, *Structured Analytic Techniques for Intelligence Analysis* (2015).

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

conflicts from happening. For example, for decades the US military strategy has been to create a war-fighting force that is so superior to other nations, and so omnipresent throughout the world that other nations dare not attack. This level of military supremacy, in theory, produces an alignment that makes conflict less likely. Two pieces of historical evidence in support of the theory are the post-World War II peace in western Europe – the longest in history – and the fact that all US conflicts since 1945 have either been conflicts of choice, or (in the single case of Afghanistan) the result of an attack by a non-state actor.

As a definitional matter, superiority only means that one actor is stronger than all others. Left unchecked, competitor nations will start nipping at the heels of a superior state until they reach technological parity. Thus, to maintain technological superiority, a nation must pursue *dominance*: a level of superiority reaching supremacy, where one both enjoys freedom of action and can (at will) deny freedom of action to others.

What would the path to quantum technology dominance look like? Is dominance even possible? We believe that the possibility for dominance depends on whether quantum computing is a winner-take-all (or winner-take-most) technology.

8.2.1 Winner Take All

At first, quantum technologies would appear not to present a winner-take-all opportunity. Consider quantum communications. American, Chinese, and Dutch scientists have all demonstrated major achievements in quantum communications, publishing their work in scientific journals. The underlying hardware for photonic transmission and capture (such as single-photon emitters and detectors) is commercially available and can be found in many physics labs. But most importantly, quantum communication technology does not appear to benefit from a *virtuous circle*: breakthroughs in quantum key distribution do not themselves create new tools for developing better breakthroughs.

But unlike quantum communications, quantum computing is likely a domain in which dominance is possible. It's true that competition is booming in the private sector and companies are experimenting with an array of different physical systems to create quantum computers. Likewise, none of this research is being kept secret. Instead, scientists and their corporate backers are apparently competing for

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

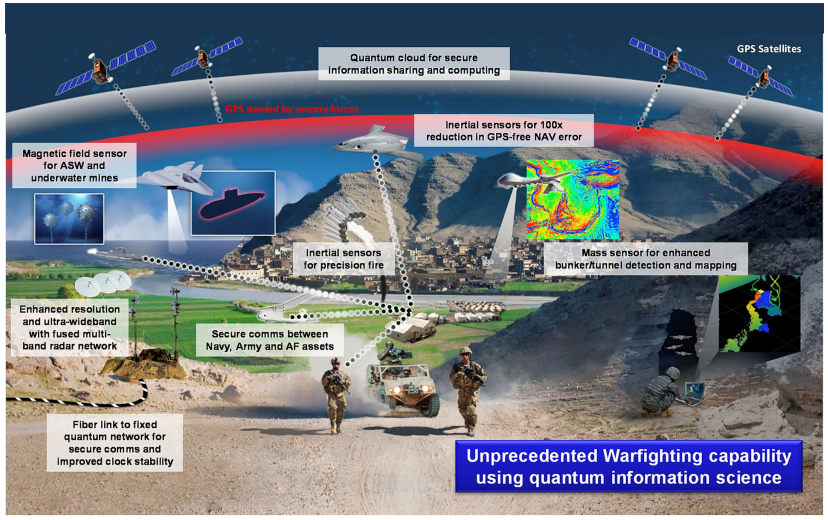

Figure 8.1. A 2018 vision of quantum technology use by the US Army Research Laboratory.

academic glory by publishing their findings in prestigious journals like *Science* and *Nature*.

But while the detailed scientific papers that are appearing may have hundred-page appendices explaining all of the science, they do not come with detailed technical information that is necessary to actually manufacture the underlying scientific apparatus. Such information would easily run to tens of thousands of pages, and in any event would be largely unusable, because using such information requires mastery of manufacturing processes and operational know-how that is built upon years of practice.

Unlike quantum communications, quantum computing does enjoy a virtuous circle, in that advances in quantum computing could almost certainly be used to develop more powerful quantum computers.

Consider this scenario: A nation develops an intermediate-scale quantum computer. Perhaps it does so by carefully observing commercial activities, and uses a different approach that has been less researched but that appears, in light of new discoveries, more promising. Instead of publicizing this achievement, or using it for cracking encryption keys, this nation focuses on understanding materials science. Specifically, that nation would attempt to build a larger quantum computer based on the insights that only it can gain from its

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

more complex view of the underlying physics of materials. Just as classical computers help one build larger classical computers, the same strategy could be important to gaining superiority in quantum computers. In this scenario, quantum computing is a winner-take-all technology. The early winner learns secrets of materials and physics that allow it to race ahead of competitors. This winner might even dangle false leads to competitors – not fake science, but perhaps apparently promising paths that lead to dead ends.

Secrecy will be a key element of winner-take-all dominance. Thus, one signpost of the government-dominant scenario is the public appearance that the government has no quantum computing program in the space at all (perhaps it signals that it has given up), or that inexplicable holes exist in the publicly available literature, but there are indicators of an aggressive quantum program operating below the surface.

An important factor in maintaining dominance is crushing competitors' will to compete. In quantum computing, such a strategy could be accomplished by eventually revealing the existence of a superior quantum program and selling commercial access. Such access would necessarily be subtly restricted. For example, users could be restricted to less powerful machines, or could be prohibited from solving particular kinds of problems. Recall that quantum computers have control systems run by classical ones; these classical computers can function as a filter to prevent certain unwanted uses of the dominant actor's quantum computer. Such access would quench funding for commercial competitors, and would likely cause scientists entering the field to concentrate on applications rather than underlying systems design: why spend billions trying to discover something that has already been discovered elsewhere?

A government that pulls ahead in quantum computing will also likely be superior in quantum sensing. This is because sensing and metrology are antecedent to computing. That is, one must master the management and manipulation of a large ensemble of qubits. That technical ability implies a mastery of smaller systems used for sensing.

To use quantum sensors in a way that helps in a competition with nations, sensors need to be deployed. Nations with sophisticated unmanned aerial vehicle technology and access to outer space will have more ability to sense without restriction.

Space programs are a source of national prestige and scores of nations have one. However, only about a dozen nations have realized a satellite launch capability. The United States has the most satellites in space (1007), followed by China (323) and Russia (164).[7]

Other nations are dependent upon launch-capable states. And these launch-capable states are unlikely to facilitate a competing nation's quantum sensing advances, particularly if they allow the launch-dependent nation to somehow leapfrog others. This is consistent with Henry Farrell and Abraham Newman's theory of *Weaponized Interdependence*.[8] According to duo, nations take advantage of economic and technological choke points for both surveillance and control of adversaries. In the case of quantum technologies, there are not good options to prevent adversaries from building or buying components, but launch-capable states could deter the most powerful implementations of those technologies – by controlling outer space.

Government Dominant

A government enjoys advanced quantum technologies and can operate without significant interference from adversaries.

Key Policy Characteristics

Industrial policy, secrecy, export control, non-proliferation-like strategies.

Key Enabling Factors

Making the right bet on qubit substrates, winner-take-all virtuous cycle, access to outer space.

Strategic Surprise

Sensing technologies that can see adversary matériel, illumination of low-observable (stealth) technologies, cryptanalysis, secretive weapons development.

Outlook

Rich private sector with high-powered incentives to commercialize makes government-exclusive control of quantum technologies unlikely.

Commercial launches might appear to be a promising way to evade the space launch choke point, however, just like seafaring vessels, satellites have a national "flag." Nations regulate such launches

[7] Union of Concerned Scientists, "UCS Satellite Database" (2021).
[8] Farrell and Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion" (2019).

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

with domestic and international law. If a nation sought to use an American company, such as SpaceX, to launch its quantum sensing network, the payload must be licensed and would be subject to review by multiple agencies. Such review explicitly considers whether the satellite would endanger national security, raise foreign policy concerns, or undermine international obligations.[9] Regulations promulgated by the Trump administration require private remote sensing companies to disclose many details about the architecture and capabilities of sensing systems, including resolution and collection rates, and whether the sensor can "look" off-axis. Imaging of other "artificial resident space objects" requires special permission – meaning that the proposed device may not look at other (potentially secret) satellites. It seems unlikely that countries without space launch capability will be able to purchase such capability to achieve quantum parity with those that have it.

The advantages of a space program go beyond sensing. United States Naval Research Laboratory (NRL) scientist Marco Lanzagorta speculates that satellite-based quantum communications systems will enable advances in submarine communication. As long as the water was sufficiently clear and lacking in turbidity, NRL predicts key distribution is possible as deep as 100 m, and at a rate hundreds of times faster than existing very low frequency communication methods.[10] This may change the "lone wolf" strategy of submarine operation.[11] Existing communications require alterations to optimal speeds and paths, ones that might help an adversary track a submarine. Thus, faster and more flexible transmission could enable more communications without detection.

The winner-take-all scenario could also happen in the private sector. For instance, Microsoft has pursued *topological* structures to develop a quantum computer while its competitors have used superconducting systems. If the topological approach turns out to be the winning medium, Microsoft could race ahead in a way its competitors could not, at least for now. Microsoft could also keep important aspects of its engineering a trade secret by selling its quantum computers as a service rather than as standalone devices. Locked in a

[9] See e.g. 15 CFR Part 960 (2020).

[10] Jeffrey Uhlmann, Marco Lanzagorta, and Salvador E. Venegas-Andraca, "Quantum Communications in The Maritime Environment" (2015).

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

vault-like data center, each Microsoft employee working on the program would only see a small part of the overall project – enough to use it and contribute, but not enough to duplicate a working system. Microsoft would then be able to maintain dominance in quantum computing much as IBM maintained its decades-long dominance in computing, and as Google continues to maintain its dominance in Internet search.

A private-sector winner-take-all outcome is very different from a government one. With the rise of the power and wealth of corporations, private companies with a quantum computer could make far more money selling to other companies than to governments. Furthermore, the sale to governments for military and intelligence purposes can be lucrative, but these activities come with other restrictions and complications that ultimately narrow options for selling one's technology. Thus, a private winner-take-all outcome would drive a great evangelizing of the technology and its uses outside defense and intelligence. A dominant company would want to sell its cloud service to every industry in almost all nations. Access to quantum computing for non-military purposes would likely be democratized, even if the devices themselves were carefully controlled. Military applications would likely remain available to the host country – which in the case of Microsoft, would likely be the US.

Combined quantum technologies may have real and lasting consequence for nation-state conflict. Indeed, some military technology experts refer to quantum sensing and communications as the "atomic bomb" of information theory, and urge us to contemplate a quantum "strategic surprise."[12]

What would strategic surprise look like in a government-superior and dominant quantum technology world? In this section we look at strategic surprise in three areas: cryptanalysis, nuclear weapons, and remote sensing.

8.2.2 Strategic Surprise: Cryptanalysis

Quantum cryptanalysis is the most obvious example of strategic surprise that could be enabled by quantum computing, and it is the motivating example that is primarily responsible for the interest in quantum computing over the past two decades.

[12] Marco Lanzagorta, "Envisioning The Future of Quantum Sensing and Communications" (2018).

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

In order to foresee the implications of quantum cryptanalysis, it is important to first understand how cryptography is used today. Here we focus on three purposes of encryption: protecting stored data ("data-at-rest"), protecting data that is sent over the Internet ("data-in-flight"), and authenticating software ("digital signatures").

The most broadly used encryption algorithm today is the Advanced Encryption Standard (AES).[13] There are basically two versions of AES in use: AES-128, which has a 128-bit secret key, and AES-256, which has a 256-bit secret key. Both of these algorithms are considered uncrackable with classical computers for the foreseeable future.[14] However, given that Grover's algorithm can speed up this kind of search so that it takes only $\sqrt{2^{128}} = 2^{64}$ operations, it might be possible to crack an AES-128 message using a fully realized quantum computer. It would still be impossible to crack an AES-256 message.

AES is a secret-key algorithm, meaning that both the sender and the recipient must agree on the same key. In practice, these keys are randomly created for every encrypted hard drive, and for every individual web page or email message as it is sent over the Internet.[15] The keys are then encrypted using a public key cryptography algorithm such as RSA or the Diffie–Hellman key exchange protocol. The security for both of these algorithms rests on the difficulty of factoring large numbers, so an attacker with a functioning quantum computer would be well positioned to decrypt the information sent over the Internet today provided that three things are true:

- The future attacker has a copy of the information that the attacker wanted to decrypt. Presumably this information would be obtained through a search of an office (to get an encrypted hard drive), a wiretap or other interception technique.

[13] Dworkin et al., *Advanced Encryption Standard (AES)* (2001).

[14] The best approaches for cracking AES-128 typically require on the order of 2^{128} mathematical operations. If an attacker has a billion computers that can perform a billion operations per second, then the attacker can perform $10^9 \times 10^9 = 10^{18}$ operations per second. However, $2^{128} = 10^{38}$, so the hypothetical attacker would require on the order of 10^{20} seconds, or 3168 billion years.

[15] This section only considers encrypted messages sent over the Internet. Native wireless communication protocols, such as those used to set up LTE cellular telephone calls, are generally less secure due to the need to have backwards compatibility.

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

- The future attacker knows the protocol that was used to send the information. This is generally not a problem because most information is sent using standard protocols.
- The future attacker has been allocated sufficient time on the quantum computer to actually crack the key.

So clearly, a functioning quantum computer does not mean the total collapse of data confidentiality. Instead, it creates the possibility that a well-positioned attacker could decrypt or forge selected messages.

Encrypted Data-at-Rest

Whether or not a fully realized quantum computer could decrypt stored data has everything to do with the way that the data are encrypted. If the data are encrypted with AES-128, or if they are encrypted with AES-256 and *that* key is encrypted with a *c.* 2020 public key algorithm (that is, one that does not offer post-quantum resistance), then the public key could be cracked. However, a common construction for disk and document encryption systems is to take a user-supplied *passphrase*, compute the *cryptographic hash* using an algorithm such as SHA-256, and use that hash to encrypt the AES-256 key. As near as we can tell, SHA-256 is quantum resistant, and the speedup afforded by Grover's algorithm would be insufficient to achieve a single cracked passphrase within the expected lifetime of the Sun. But 5 billion years is a long time, and it's possible that a flaw will be discovered in SHA-256 or AES-256 that would obviate the need to crack the code using brute-force search before the Sun becomes a red giant and engulfs the Earth.

This means that data-at-rest encrypted *today* might be crackable at some point in the future when quantum computers are available. However, it is relatively easy to design data-at-rest systems to be quantum-resistant, and many of today's systems encryption systems have already been redesigned to take that possible future threat into account.

Encrypted Data-in-Flight

Whereas data-at-rest is a message that you send to yourself in the future, data-in-flight is data that you send to someone else. The fundamental difference between these two scenarios is how the intended

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

user gets access to the decryption encryption key. In the first case, since you are sharing the key with your future self, you have it now – just don't lose it! But when Alice sends her encrypted message to Bob, Bob typically doesn't have the key that was used to encrypt the message. This is the problem for which public key cryptography was invented. The modern solution is that Alice generates a random message key and uses that to encrypt the message, then encrypts the message key with Bob's public key and sends the encrypted message key along with the message. Bob receives both the encrypted key and the message, decrypts the message key with his public key, and uses the decrypted message key to decrypt the message.

As we discussed earlier, technologists are working hard to develop and deploy post-quantum public key cryptography algorithms. If they succeed in developing algorithms that are just as efficient as RSA and Diffie–Hellman, the world will likely transition to them. Such a transition would probably take five to ten years, given the speed of similar cryptography transitions.[16]

If workable quantum computers become available, the data-in-flight with its privacy most likely in jeopardy will not be data being sent at some point in the future, but the data that was sent between 1995 and today that was captured and archived by various national intelligence agencies.

There is no information that is both public and trustworthy regarding the systematic recording of telecommunications in the world today. For example, around 2011 the National Security Agency broke ground on its Utah Data Center, a massive data warehouse costing over a billion dollars.[17] It has been speculated that one purpose of this facility is to warehouse all the data the NSA collects for future analysis. A 2013 article in *Forbes* estimated the capacity of the facility at 12 000 PB stored on 10 000 racks of equipment. To convey the size of this storage, the article notes that all the "voice recordings of all the phone calls made in the US in a year would take up about

[16] For example, the first attacks on the cryptographic hash MD5 were discovered in 2006. See Black, Cochran, and Highland, "A Study of The MD5 Attacks: Insights and Improvements" (2006). Yet Microsoft still allowed limited use of the MD5 algorithm for certifying root certificates as late as 2013. See Microsoft Corp., "Microsoft Security Advisory 2862973: Update for Deprecation of MD5 Hashing Algorithm for Microsoft Root Certificate Program" (2013).

[17] National Security Agency, "Groundbreaking Ceremony Held for 1.2 Billion Utah Data Center" (2001).

272 petabytes,"[18] although the likely target of the data center is not US, but foreign communications (as the NSA is generally prohibited from collecting inside the United States). Such data would be prime targets for decryption if they are encrypted and the NSA were to later acquire a quantum computer.

More concerning for US readers than possible surveillance by the US government (which is regulated) may be the electronic surveillance activities of China, Russia, and other governments against US and European targets. Russia and China[19] are also known to have extensive capabilities for Signals Intelligence (SIGINT) and are presumably collecting worldwide, although once again, hard details are somewhat elusive. The Global Signals Intelligence market was said to be $12.8B in 2018 and expected to rise to $15.6B by 2023, according to a market research report,[20] with much of the growth coming from China and India.

In general, it seems prudent to assume that any message transmitted today in any part of the world might be might be captured, indexed and archived by anywhere from two to five governments or non-government organizations, and that the message might be unlocked at some point in the future if sufficient need arises.

Forged signatures

A third application for quantum cryptanalysis will be to crack the keys that are used to sign software updates, electronic documents, and websites.

Digital signatures are an aspect of cryptography that is less publicized than protecting the secrecy of web browsing and email, but it many ways they are more important, because they provide for the underlying security of the computers themselves. Virtually every program that runs on a modern computer is digitally signed by the computer's manufacturer, the operating system vendor, or the software publisher. The computer then verifies these signatures when it boots and as it runs. Companies like Intel also use digital signatures to validate updates for the microcode that runs inside microproces-

[18] Hill, "Blueprints of NSA's Ridiculously Expensive Data Center in Utah Suggest It Holds Less Info Than Thought" (2013).

[19] China's SIGINT capabilities go back to the 1950s, see Hagestad, "Chinese IW Capabilities" (2012).

[20] Wood, "Global $15.6Bn Signals Intelligence (SIGINT) Market by Type, Application and Region – Forecast to 2023 – ResearchAndMarkets.com" (2019).

sors. These updates make it possible for Intel and others to fix bugs in microprocessors after they have shipped to customers.

Digital signatures are similar to traditional wet-ink signatures in that they are typically used by an author to sign something that the author has written to demonstrate the author's authorship. However, in practice, an author can sign anything that the author wants. Authors can also be tricked into signing documents unknowingly or be forced against their will. But whereas an ink signature is bound to a particular piece of paper, a digital signature is linked to a specific sequence of bits. If just one bit changes, the signature is no longer valid.

Digital signatures are written with an encryption key that is unsurprisingly called a signing key. These keys are typically certified by organizations that are unsurprisingly called *certificate authorities*. These certifications are also performed using digital signatures. The certifications are verified with the certificate authority's *public key certificate*, which is supplied with the computer's operating system.

To give a palpable example, you rely on these certificates (and thus on these certificate authorities) when you visit the website of your bank or other important services. When the browser visits the putative bank website, the bank sends its certificate to the browser along with a reference to the issuing certificate authority. If the web browser accepts that certificate authority, the browser signals (typically with a lock icon) that the connection is secure, and in some cases, avers the identity of the website as belonging to a certain company. If the certificate is compromised or certificate authority was dishonest, an impostor could masquerade as your bank, and you would be none the wiser.

Although there are different algorithms used for digital signatures than for message secrecy, the algorithms are based on the same underlying mathematics. As a result, a quantum computer that could be used to crack the public keys that are used to encrypt messages, and thus make it possible to decrypt those messages, could also crack the public keys used to verify digital signatures, and thus allow signatures to be forged.

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

Hashing, Digital Signatures, and Grover's Algorithm

Another way that quantum computers might be able to attack digital signatures is by searching for *hash collisions* in cryptographic hash functions.

A cryptographic hash, sometimes called a digital fingerprint, is a number that results from running an input document through a special kind of one-way digital function. These functions are designed so that no matter the size of the input, the output is a constant size – for example, the US Government's Secure Hash Algorithm #1 (SHA1) always outputs 160 bits (40 hexadecimal characters). Cryptographic hash functions are further designed so that roughly half of the output bits change in an unpredictable manner if a single bit in the input changes.

For example, here we apply SHA1 to the strings *hi* and *hh*, which differ by exactly one bit:

String	Bits	SHA1 (hex)
hi	01101000 01101001	c22b5f9178342609428d
		6f51b2c5af4c0bde6a42
hh	01101000 01101000	d3fc13dc12d8d7a58e7a
		e87295e93dbaddb5d36b

Digital signature systems actually sign hashes of documents, rather than the documents themselves. So if it is possible to find two documents that have the same hash, there is no way to tell if a digital signature from the first is moved to the second.

Quantum computers, using Grover's algorithm, could offer a speedup in finding such collisions, which could be used in attacks to place malware on other computers and otherwise enable attackers to fool recipients about the integrity of files. In order to offer such speedup, however, it might be necessary to implement the entire cryptographic hash function as a set of quantum gates. Grover's algorithm gives a speedup of a square-root, so roughly speaking it would make a 512-bit hash as secure as a 256-bit hash. Since 512-bit algorithms such as SHA-512 and SHA-3-512 are widely deployed today, and since a work-factor of 2^{256} is considered unbreakable, Grover's algorithm is unlikely to have an impact on the security of today's digital signatures absent additional mathematical developments.

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

False software signatures are valuable because with a single hostile software update, even just a somewhat sophisticated attacker can take over a computer and capture all information from it instead of laboriously decrypting individual files and communications.[21] A malicious update allows the attacker to operate the device as a regular user, and thus avoid the time-intensive requirements of investigating a suspect through their communication logs or through interviewing people who conversed with the suspect.[22] Not limited to mere communications surveillance, a hostile update can covertly enable the computer's microphone and camera, and perform searches on the user's files. If the computer is used for web-based banking, the update can transfer money out of the user's bank account. If the user accesses their work computer from home, the work network can be equally compromised as well.

8.2.3 Forged Signatures and Our Legal Realities

Digital signatures are used throughout the digital economy. The ability to forge signatures would render virtually every computerized system vulnerable to some kind of attack. This includes web servers, the Internet's underlying domain name system, embedded firmware, vehicle control systems … practically everything. A nation with the capability to create fake software updates could take over the industrial control systems of other nations, and corrupt devices such as radar systems or targeting systems that are relied upon to compute properly during a conflict.

Digital signature attacks are real and can have dire consequences for victims. Consider the attack on the Dutch certificate authority, DigiNotar, whose certificate authority public keys were relied on by popular web browsers including Google's Chrome, Microsoft's Internet Explorer and Mozilla's Firefox.[23]

In 2011, intruders thought to be working for the Islamic Republic of Iran hacked DigiNotar's systems and issued over 500 certificates in the names of popular web services including Gmail and Facebook. Combined with the Islamic Republic's control of the Iranian's internet connections, these certificates allowed the holders of the corre-

[21] T. Li et al., "Security Attack Analysis Using Attack Patterns" (2016).

[22] Vidas, Votipka, and Christin, "All Your Droid Are Belong to Us: A Survey of Current Android Attacks" (2011).

[23] Hoogstraaten et al., *Black Tulip Report of The Investigation into The DigiNotar Certificate Authority Breach* (2012).

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

sponding private keys to intercept communications between users in Iran and these services, allowing the theft of content such as email messages and postings, as well as passwords and other information. Services belonging to the US Central Intelligence Agency and Israel's Mossad were also allegedly targeted. The DigiNotar attack shows that as individuals in repressive states use the Internet to organize and communicate with the outside world, attackers who can issue false certificates (or crack the private keys of certificates already in use) gain a powerful ability to monitor, change, and block these activities. They can identify participants in communications and masquerade as the activists themselves, all while the users think their communications are protected by advanced encryption.

The DigiNotar incident is a clear demonstration that technologies such as encryption – thought to be the ultimate technical guarantee against spying – often require extraordinary reliance on unknown third parties.[24] We must rely on these third parties to both properly design and to properly operate these systems. This includes anticipating attacks on confidentiality and integrity, and finding ways to upgrade existing systems to be resilient against future adversaries.

Imagine a future where this reliance on encryption deepens by spreading to more contexts, when not only web communication but all sorts of societal functions depend on digital signatures. As governments consider "e-government" services, the most radical approach is to go "digital first" with documents of record. Estonia has done so, meaning that the nation's official document of record is computerized rather than on paper.[25] In Estonia, citizens and businesses can use an electronic identity infrastructure to hold a record of their personal information, and then use this system to avoid the noisome paperwork that major (or even minor) life events trigger. For instance, babies can be registered with the government (i.e. obtain a birth certificate) without paperwork, prescriptions are requested online and filled, taxes can be paid online, citizens can vote online, one can create a corporation online quickly, and one can pay for myriad services, from public transportation to parking fines, all online. Of course many nations provide services like this, but in the US, for instance, there is no single identity architecture and the different

[24] Arnbak and van Eijk, *Certificate Authority Collapse: Regulating Systemic Vulnerabilities in The HTTPS Value Chain* (2012).

[25] Heller, "The Digital Republic: Is Estonia The Answer to The Crisis of Nation-States?" (2017).

services tend to be developed and offered by different entities, for better or worse.[26]

As nations implement similar e-government approaches, they become susceptible to integrity attacks that are impracticable in a paper-record society, or even in a society that provides the same services from disparate entities with different systems. As such, quantum computing attacks on signatures could affect the documents that define our legal relationships, spreading uncertainty, allowing people to cheat, and making it difficult to determine what the "ground truth" is. Adversaries could do this by forging signatures and subtly altering important records. Imagine if an adversary changed property lines, changed ownership records or taxes, edited contracts or other negotiated legal instruments, altered voting registrations or actual vote tallies, or even revised another nation's laws by forging the certificates that guaranteed the authenticity of information. We have long lived in a world with fake news,[27] but what if we also lost bearings on the fundamental integrity of legal processes with "fake law"? We have to anticipate that attacks on integrity will alter our fundamental legal relationships, making it easier to cheat and to hide cheating. And technologies such as blockchain may be of no use, since it is the hashes of documents that are typically put on blockchains, rather than the documents themselves.

[26] Competitive pressure has prevented a single identity architecture from emerging in the US. In particular, banks have been resistant to a collectivized identity regime, because the process of customer identification and authentication itself helps banks control the customer relationship and prevent churn to competitors. In addition, many retailers have resisted single-sign-on offerings from Google and Facebook, despite the probability that these options are more secure, because single sign-on (SSO) jeopardizes branding and because of the risk that Google or Facebook might use the authentication system to compete against the retailers relying on the system. For instance, imagine using Google's single sign-on to login to a pharmacy. Because the company has access to user email, it knows the user is refilling a prescription for birth control, and so it offers an advertisement for a competing pharmacy, or competing treatment, or perhaps even an issue-advocacy message protesting the use of birth control. Or maybe it decides to enter the pharmacy business based on intelligence from these sources.

[27] Plutarch describes the mob massacre of second-century reform politician Tiberius Gracchus and supporters by patricians who were enraged by false accounts that he sought a crown. Plutarch, *Lives. Vol. 10, Agis and Cleomenes, Tiberius and Caius Gracchus, Philopoemen and Flamninius* (1921).

8.2.4 Attacks on Passwords and Other Authentication Systems

Usernames and passwords are the default security mechanism for most computing services. Developed in the days of the mainframe, usernames identified the account that should be billed for using the computer, and the password prevented one person from accidentally spending from the wrong account. Decades later, passwords are the primary control not for just for billing, but for protecting information. Thus using a quantum computer to attack passwords would also seem to be a more strategic use than decrypting single messages.

An authentication system generally consists of three parts:[28]

1. The *user* who seeks to use it to prove their identity. The user may do this by knowing a password or a PIN, or by participating in a biometric challenge.

2. The computer that receives the password and uses it to identify. (The *relying party*.)

3. The service or database that the relying party uses to verify the identity. (The *identity provider*.)

There are many ways to attack these systems. For example:

Attack 1 The attacker can intercept the communication between the relying party and the identity provider and convince the relying party that the identity provided by the attacker to the relying party is correct. (A *proxy interception attack*, also known as a *machine-in-the-middle* (MITM) attack.) Section 8.2.2 (p. 317) would be applicable here as well.

Attack 2 The attacker can pretend to be the user and repeatedly guess new username/password combinations until one succeeds. (An *online password-guessing attack*.)

Attack 3 The attacker can break into the identity provider's computer and steal a copy of the registration database containing hashes of user passwords. With a password dictionary, the attacker then hashes each password in the password dictionary to see if

[28] While this section uses the standardized terminology of the OpenID protocol and the FIDO alliance, the example is intended to be sufficiently general as to apply to any authentication system.

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

the hashed dictionary password matches a hash in the stolen database. (An *offline password-guessing attack*.)

In the case of Attack 1, these communications are generally protected by public-key cryptography. Today's recorded communications might be crackable with a quantum computer in the future (see Section 8.2.2 (p. 317)), so passwords recorded today might be divulged at some point in the future. Fortunately, there's a simple mitigation: once quantum computers become available to your adversary, change your passwords.

In case of Attack 2, online password-guessing attacks are limited by how many passwords can be guessed every second, how many passwords can be guessed before the user's account locks out, and the password guessing dictionary used by the attacker. None of these should be directly affected by quantum computers. Attackers might be able to use quantum computers to construct better password guessing dictionaries, but this would be of minor use in an online attack.

In case of Attack 3, modern identity providers encrypt passwords with one-way algorithms: there's no way to decrypt the encrypted password, so attackers try encrypting millions or billions of potential passwords to see if any of them match the encrypted passwords under attack. Some algorithms are stronger than others, and increasingly attackers have enough computer power that they can try all possible passwords that a person can type. This is the reason that contemporary password systems require you to type a password that includes uppercase letters, lowercase letters, and symbols: it increases the number of possible passwords that an attacker has to try (see the sidebar "Password Complexity Is Complicated!" on page 327).

Quantum computers may offer some quantum advantage to attackers conducting offline password attacks, but the advantage is likely to be minimal. As modern password encryption schemes do not rely on number-theory based constructors (see Section 7.1, p. 260) that would be susceptible to Shor's algorithm, current thinking is that the maximal quantum speedup would be through the use of Grover's algorithm – that is, reducing the work for cracking each password. Like other quantum computing capabilities, this kind of attack would be dependent on a large device that could implement the entire function as a series of gates without losing coherence (i.e. the quantum computer would have to be large enough to store the

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

Password Complexity Is Complicated!

With an 8-character password comprised solely of lowercase letters, there are $26^8 = 208\,827\,064\,576 \approx 2 \times 10^{11}$ possible passwords. If an attacker can try a billion (10^9) passwords a second, it takes on the order of 200 seconds to try them all.

Password complexity rules attempt to increase the number of possible passwords. For example, any one of those characters can be an uppercase letter, a lowercase letter, or a number, then each character can be one of $26+26+10 = 66$ possible characters, so the total number of possible passwords increases to $66^8 = 360\,040\,606\,269\,696 \approx 3 \times 10^{14}$. The added complexity increases attack time to 300 000 seconds or 83 hours.

Unfortunately, such calculations are subverted by the way that people actually guess passwords. Faced with a requirement that an 8-character password must contain an uppercase letter and a number, the typical user will add a single uppercase letter and a single number to their password. An attacker now merely needs to try all passwords containing 6 lowercase letters, 1 uppercase letter, and 1 number. There are $26^6 \times 26 \times 10 = 80\,318\,101\,760$ such combinations. For each of these combinations, the digit can be in any one of 8 positions ($\times 8$) and the uppercase letter can be in any of the remaining 7 ($\times 7$), so an attacker will start by trying these $26^6 \times 26 \times 10 \times 8 \times 7 = 1\,729\,928\,345\,600 \approx 1 \times 10^{12}$ combinations.

While password requirements increase attack burdens, they decrease the usability because of user error. Requiring longer passwords but allowing them to be all lowercase is a viable alternative. A 16-character, all-lower-case password increases the number of potential passwords to at least $26^{16} \approx 4\times^{22}$. This is dramatically more secure than eight-character passwords with case restrictions, and is probably easier for most people to remember.[a]

[a]For an excellent overview of password security and usability, see Bonneau, Cormac Herley, et al., "Passwords and The Evolution of Imperfect Authentication" (2015). Meanwhile for a comprehensive analysis of alternatives to passwords, see Bonneau, C. Herley, et al., "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes" (2012).

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

entire set of possible passwords). Thousands of iterations would be required for each password. According to the 2019 National Academy of Sciences report, this process would require 2.3×10^7 *years* to break a single password.[29]

As we write this book in 2021, however, the most valuable passwords are not stolen by brute-force attacks on encrypted databases, but by targeted attacks on key individuals. The fateful email dump of John Podesta, Hillary Clinton advisor and former White House Chief of Staff, illustrates this. Among the most powerful people in America, Podesta used the 10-character password "Runner4567" to protect his Google Gmail account. This password was elicited from Podesta by a phishing attack, so its complexity was not relevant. Podesta's Gmail account was not protected by a second-factor. Thus, once his password was obtained, it allowed a Russian disinformation machine to access and publicize years of archived email messages.[30]

Security incidents where entire user databases are captured by attackers are another source of high-value passwords that does not require quantum computers for analysis or cracking. Cyberintelligence firms estimate that 35 such incidents occur a day, leaving full customer databases online and unprotected.[31] These security incidents provide much simpler means than quantum computing to break into accounts. Indeed, cyberintelligence companies show that many customer databases stolen and circulating online have failed to implement countermeasures and thus the passwords are available in free text. Because users reuse passwords, these databases can be used for online password guessing against individuals, or at scale in what is known as a "credential-stuffing" attack. For instance, in a credential-stuffing attack, if just 1 or 2 percent of users in a compro-

[29] Grumbling and Horowitz, *Quantum Computing: Progress and Prospects* (2019), p. 98.

[30] Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (2020).

[31] 4iQ, "2020 4iQ Identity Breach Report" (2020). Because of the volume of incidents, services such as "have i been pwned?" have in excess of 10 billion credentials that have been aggregated from misconfigured or hacked services. Oftentimes the attacker, or someone who found the database stolen by the attacker, provides this information directly to cybersecurity intelligence companies. Most of this activity is not well known publicly, because losses of customer databases, even if enormous and sensitive, are not always subject to security breach notification laws. As of this writing, haveibeenpwned.com/ makes over 610 million plain-text passwords available for services that wish to prevent users from choosing passwords that are already widely available.

mised database use the same password for Facebook or Gmail, that could result in hundreds or thousands of compromised accounts that can be quickly scanned for the presence of gift cards or other forms of stored value.

Tasking, Targeting, and Deconfliction

Organizations that possess quantum computers will need to carefully consider both their quantum computing capacity and the *key value* of keys that they wish to crack. In all likelihood, each quantum computer will be used to crack a single key at a time. Cracking time will be a major barrier to the widespread use of these machines: the National Academies estimated that a strong RSA key would take 28 hours to crack,[32] while a 2019 Google paper proposed a method that would require 8 hours.[33]

Quantum computing resources will therefore be limited and rationed. Even if the first working machine costs $100 billion to build and each additional machine can be built for the cost of a modern laptop, there will still be far fewer machines than messages to crack. Some process will need to be adopted for allocating the use of these machines.

Military doctrine envisions a process involving *targeting*, *tasking orders*, and *deconfliction* for making such decisions. Targeting "is the process of selecting and prioritizing targets and matching the appropriate response to them, taking account of command objectives, operational requirements and capabilities."[34] Once targets are chosen, a military command will issue a *tasking order*, which is a "method used to task and to disseminate to components, subordinate units, and command and control agencies projected targets and specific missions as well as general and specific instructions for accomplishment of the mission."[35]

To illustrate why this process is important, consider an organization that is able to intercept wireless messages between a target's phone and a publication service such as Twitter. Each wireless message might contain a tweet destined for immediate publication, a

[32] Grumbling and Horowitz, *Quantum Computing: Progress and Prospects* (2019).
[33] Gidney and Ekerå, "How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits" (2019).
[34] Curtis E. LeMay Center for Doctrine Development and Education, "Introduction to Targeting" (2019).
[35] Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms* (2020).

tweet scheduled to be published at some point in the future, a direct message to another user, or perhaps a status check, polling the service for other messages posted by other users. Some of these messages are clearly more valuable than others, but they all require the same level of effort to decrypt. And here's the problem: with a well-designed encryption system, there is no obvious way to tell which message is which before it is decrypted. Encrypted messages are easy to create, so a smart adversary can generate many worthless ones to soak up the capacity of another state to decrypt. This is why obtaining and evaluating external information can be a critical part of the tasking and targeting decisions. Indeed, metadata, which is typically not encrypted, will be important to providing hints about key value.

The term *deconfliction* describes systematic management procedures to coordinate the use of resources by various stakeholders. Quantum cryptanalysis will require multiple layers of deconfliction. At the most basic level, management will need to assure that resources are not used to crack the same key more than once. More strategically, management will need to decide whether the results from cryptanalysis can be directly exploited, or the results will need to be closely held to prevent adversaries from learning the extent of the organization's cryptanalytic capabilities.

Another area that might be of concern is how much information is revealed to adversaries through the use of information gained through quantum cryptanalysis. A nation will change its behavior depending on if it thinks an adversary has possibly one functioning quantum computer, if the adversary is known to have one functioning quantum computer, or if the adversary is known to have a thousand such machines. Countries that have publicly known but nascent quantum cryptographic capabilities might seek to project that they have significantly more capabilities than they in fact do, to keep their adversaries off-balance, while countries that have vast capabilities may seek to keep them secret, in order to lull their adversaries into a false sense of security.

In sum, quantum cryptanalysis is a threat, but one that we consider to be overhyped. Simply put, quantum computers will not magically break all encryption quickly, as sometimes implied by the news media and even by some policy analysts. Instead, attackers will carefully choose and focus their cryptanalysis resources on high-value keys, presumably ones that cannot be attacked using other intelligence trade-craft.

Those other methods of attack also provide context. One tends to look to technology for dramatic intelligence gains, when in reality, simpler approaches may do. For instance, many of the great US intelligence losses have been the result of insiders: John Anthony Walker (1968–1985), Robert Hansen (1979–1981, 1985–1991, 1992–2001), Jonathan Pollard (1984–1985), Ana Montes (1985–2001), Chelsea Elizabeth Manning (2009–2010), and Edward Snowden (2009–2013). Consider Snowden, of whom we likely know the most. Despite his clear technical talents, Snowden's attack was straightforward: privilege escalation, password acquisition, and a mass exfiltration of documents he had access to by virtue of his job.[36] Even in a world with quantum computing, traditional spycraft, including recruitment of insiders and placement of assets, is likely to remain a reliable, effective, and far less costly modality for accessing protected secrets.

8.2.5 Strategic Surprise: Nuclear Weapons

Simulating nuclear physics (presumably for weapons testing) was the existential reason that Feynman proposed quantum computing in the first place. We therefore reason that once governments have functioning quantum computers, they will use them for this purpose – to simulate the action of current and proposed nuclear weapons.

The connection between computing and weapons delivery and design runs deep. The original mechanical, electromechanical, and electronic computers were developed for the purpose of targeting munitions. Later, the design and operation of nuclear weapons drove the development of electronic computers in the 1940s, and supercomputers since the 1960s.

Prohibiting testing was a major diplomatic priority of the Soviet Union, particularly in the last decade of the Cold War. Aside from reducing the overall stockpile of weapons, Soviet strategists were worried that continued testing was a key precursor to President Reagan's anti-ICBM technology, known as the Strategic Defense Initiative (SDI).[37] Mocked as "star wars," SDI made it clear that space

[36] US Congress, House Permanent Select Committee on Intelligence, "Executive Summary of Review of The Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden" (2016).

[37] Hoffman, *The Dead Hand: The Untold Story of The Cold War Arms Race and Its Dangerous Legacy* (2009).

was a new domain for military conflict, and raised military spending to levels that the Soviets ultimately could not afford.

Today there are comprehensive test bans in place prohibiting nuclear testing in outer space, in the atmosphere, and underground. As a result, governments must turn to computers to simulate the "physics package" of nuclear weapons. But more than a simple replacement for testing, computers make it possible to explain many possible designs without producing a blast, radiation or fallout. For this reason, quantum computers might end up significantly accelerating the development of novel physics packages with particular characteristics, such as very-low yield, enhanced radiation, or fallout with particularly short half-lives. As such, quantum computers might paradoxically enable the creation of nuclear weapons with fewer barriers-to-use.

Indeed, with quantum computers, simulations of ICBM flight, the design of warheads, and their destructive potential will all improve, but in the privacy of computing, hidden from satellites and possibly other forms of intelligence gathering.

8.2.6 Quantum Strategic Surprise: Chemical, Biological, and Genetic Weapons

Nuclear weapons occupy a central place in the modern psyche. We all live less than 30 minutes from an attack that could end life on Earth. Not as much attention is devoted to the potential of gigadeaths from chemical, biological, or genomic weapons. This may be because of the worldwide consensus against so-called "weapons of mass destruction" that emerged from World War I. The first international ban on chemical and biological weapons was the Geneva Protocol of 1925, formally known as the Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare. In 1972 many countries entered into the Biological Weapons Convention, which prohibited the development, stockpiling, testing, acquisition and retention of such weapons (although the Soviet Union continued to develop and stockpile such weapons in violation of the treaty, as it was sure that the US was doing the same[38]). In 1997 the Chemical Weapons Convention placed additional restrictions on chemical weapons and their precursors.[39]

[38]Stern, *The Ultimate Terrorist* (1999).

[39]The earliest regulation of chemical weapons came in 1675 with the Strasbourg Agreement's limitation on use of poison bullets. Hardesty, "Safety, Security and

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

Yet the risks of chemical, biological, and new agents made possible through synthetic biology are significant and both the understanding and development of these weapons could be accelerated through computer simulation. Such activities are easy to hide in plain sight: the difference between a vaccine and a bioweapon is whether or not the infectious agent is killed before it is put into the delivery system.

In fact, even conventional weapons could become more powerful with quantum simulation. Chapter 5 discusses the modeling of nitrogen fixation as a quantum computing application with tremendous human benefit. The flip side of that simulation is that nitrogen is a key ingredient in explosives. Governments will be intensely interested in developing more powerful explosives along with syntheses that are safe, cheap, and energy-efficient. And remember, unlike nuclear weapons, there is no taboo associated with using conventional weapons.[40]

As nations agree to forbear from nuclear testing or development of bio-warfare agents, inspection and monitoring efforts are necessary to ensure compliance. Nations must be able to demand access to facilities and to make sense of the equipment and materials found. Elaborate confidence-building measures have been developed to foster international trust in different areas of weapons control.

The 1992 Treaty on Open Skies (from which the US withdrew in the last days of the Trump administration on November 22, 2020) is an example of a confidence-building measure. Under that agreement, nations agree to a regime of aerial inspection of countries using limited sensors.[41] The idea is that these overflights allow political leaders to be confident about estimates of other nations' military capacity. The idea may seem antiquated in the era of the spy satel-

Dual-Use Chemicals" (2014).

[40] While nuclear weapons have retained a taboo, governments have been willing to use conventional weapons that have nuclear-like effects. In 2017, President Trump ordered the use of the Massive Ordnance Air Blast (MOAB), an enormous conventional bomb with a yield of approximately 10 tons of TNT, to destroy an ISIS base in Afghanistan – roughly a thousandth the yield of the US nuclear weapons that destroyed Hiroshima and Nagasaki in 1945. In 2019, Trump boasted that the US could kill 10 million people in Afghanistan, a quarter of the country's population, in a week relying only on *conventional* weapons. About 200 000 died in the Hiroshima and Nagasaki atomic attacks.

[41] The Treaty on Open Skies bans collection of electromagnetic signals in the radio band, and tops resolution of optical sensors at 30 centimeters, infrared at 50 centimeters, and side-looking radar at 3 meters.

lite, but aerial platforms generally have higher resolution, more flexible targeting, and lower cost of operation than platforms in space. Also, over 30 nations have signed the treaty, and many of these nations do not have significant space programs. It is unclear if Open Skies overflights could be supplemented by more precise quantum-sensor-based position, navigation, timing (PNT) technologies (see Section 2.3.2, "Sensing Location" (p. 51)). Even with low-resolution images, a high frame-rate camera paired with quantum PNT and advanced post-processing could produce ultra-high-resolution images.[42] These could be further enhanced with sophisticated spectral analysis. And this is before one even considers the possibilities of using quantum-enhanced sensors.

Inspection and monitoring is where quantum computing could address issues of strategic surprise for nuclear weapons, but not for chemical or biological.

Nuclear weapons Even underground nuclear detonations are detectable remotely, through seismographic evidence and through atmospheric monitoring for ionizing radiation. Quantum sensors should make such detection efforts more accurate.

Chemical and biological These weapons are more difficult to detect, as they do not emit particles or radiation that are readily measured at distance.

Testing chemical and biological weapons requires large, secret facilities to experiment with delivery mechanisms, especially those involving aerosols. The testing itself must be carefully done, as accidents, such as the 1979 Sverdlovsk anthrax incident, signal cheating.

To detect such facilities, the Convention requires nations to identify vaccine manufacturing facilities, to share information about labs that might have weapons capacity, and to release data on outbreaks caused by toxins.

Cheating becomes easier when chemical and biological weapons can be simulated in a computer. Barriers to development are lower if compounds can be simulated, and if delivery methods could be modeled, and thus enhanced, without creating elaborate facilities that have to both test agents and hide evidence of wrongdoing from others. Computer-aided research could bring a nation closer and closer to a quicker, more effective development and stockpiling cycle.

[42] Note that the treaty requires disclosure of attributes such as frame rate frequency.

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

Here again, confidence-building measures can reduce the risk of these weapons. Such measures include records keeping, access to records, and on-site inspections. Indeed, the Biological Weapons Convention provides many layers of reporting and information-sharing requirements to surface illegal activity. However, it is vital that governments adopt and transition integrity mechanisms to digital signatures based on post-quantum algorithms as soon as they are available so that the records will continue to be regarded as authentic and unimpeachable.

8.2.7 Strategic Surprise: Remote Sensing

Quantum sensing will enable improvements in intelligence, surveillance, reconnaissance, positioning, navigation, and timing, and these improvements will have both strategic and tactical value.[43] Consider gravity. Using interferometry, we have created extraordinarily sensitive gravity wave detectors that ring when black holes collide. But much similar technology has been deployed into earth orbit to detect the location and movement of large masses on the Earth. (See p. 67 for details.) The small number of countries with space and quantum technology programs might be able to develop sensing platforms that combine gravity and electromagnetic sensing to detect not only other nations' underground natural resources, but also matériel. Quantum detection power exceeds classical abilities, because camouflage (tin-roofed airline hangars, concrete domes, or inflatable structures) and tactics such as operating at night can obscure heavy matériel from classical satellite observation, but camouflaged matériel will have signatures detectable using other sensing technologies.

We might imagine uses of satellite-based quantum sensors that would impose massive costs on a defender. Imagine that a nation maps out an adversary's entire critical infrastructure using quantum sensors from aircraft or satellite. This adversary cannot directly attack this infrastructure, because that would start a war. So the adversary nation does the next best thing: it anonymously publishes the map of every utility wire and natural gas pipe in a region. This kind of release could even be disguised as an "open data" effort. But such a data dump would elucidate dependencies in power infrastructure that could enable less sophisticated actors, say terrorists or even

[43] Gamberini and Rubin, "Quantum Sensing's Potential Impacts on Strategic Deterrence and Modern Warfare" (2021).

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

criminals, to attack and cause much larger outages than they could without the information.

Quantum sonar and radar provide another area for strategic surprise. The US invented and broadly deployed stealth technologies that absorb radar and other energy.[44] Stealth, known as low-observable technologies, gave the US and its allies an advantage in airpower. But the assumption that US stealth aircraft are practically undetectable by radar and that its submarines operate with near-perfect acoustic stealth may be threatened by quantum sensing. Low-observable technologies can still be seen with the kinds of lasers described in Chapter 2. In addition, these quantum sensors themselves are "stealthy," meaning that detecting an adversary's sensing may be impossible.

The implications for quantum technologies and submarine warfare cut both ways. On one hand, several kinds of quantum sensing could be deployed to detect submarines. On the other, submarines may gain additional stealth through quantum communications, which gives some advantages over existing methods (see Figure 7.4).

Turning to submarine detection, scientists have mapped out photonic, gravimetric, and electromagnetic sensing approaches,[45] as well as proposals to use quantum computing to improve passive sonar.[46] Because they are large, weighty vehicles full of electronics and heavy metals, submarines have a geometry and composition unlikely to occur naturally. Sensitive quantum magnetometers or gravimeters (see Figure 2.7) could be installed in the ocean to create a fence to detect matching geometries. Knowing more about where submarines are has important implications for national security, because submarines are both part of a tenuous strategy to intercept first strikes by ballistic missiles, but also their stealth and survivability help make a "second strike" possible in a nuclear conflict. Upsetting assumptions surrounding submarine stealth with quantum radar and sonar endangers key aspects of nuclear deterrence strategy.[47]

[44] Rich and Janos, *Skunk Works: a Personal Memoir of My Years at Lockheed* (1994).

[45] Marco Lanzagorta, Jeffrey Uhlmann, and Salvador E. Venegas-Andraca, "Quantum Sensing in The Maritime Environment" (2015).

[46] S. E. Venegas-Andraca, M. Lanzagorta, and J. Uhlmann, "Maritime Applications of Quantum Computation" (2015)

[47] Schelling, *The Strategy of Conflict: With a New Preface by The Author* (1980).

Unmanned aerial vehicles (UAVs), popularly known as "drones," have emerged as a key surveillance tool and offensive weapon as a result of technological, political, and cultural changes. Faced with the rise of Islamic militant violence and the failure of some states to police or exclude terrorists, President George W. Bush turned to drones to surveil militants with powerful sensors and then attack when the opportunity presented. Presidents Obama and Trump continued and expanded the program, in part because public support for fighting foreign wars, already weakening, further deflated after the second war in Iraq, but also perhaps because the growing documentation of the horrific impact of war on the war-fighter has made Western societies less tolerant of individual sacrifice in pursuit of geopolitical objectives.

UAVs have enabled successive presidents to use force in multiple theaters without committing troops, and to argue that their use of force is more proportionate and discriminant than traditional bombing campaigns. As we write this, it is publicly known that US drone strikes have been carried out in Afghanistan, Iraq, Libya, Pakistan, Somalia, Syria, and Yemen. Drones may also have been used to attack aircraft using missiles, and the US Air Force is developing a drone for aerial combat.[48]

Critics of the UAV program argue that UAV strikes are indiscriminate and disproportionate because of civilian casualties. These arguments find support in part because of the design of UAVs. Consider the "smart bombs" of the 1991 Persian Gulf War: these gave the military the chance to (very selectively) show footage of what appeared to be precise strikes against targets. This footage helpfully ended right at the moment of impact, leaving any human suffering off-screen and thus abstract. By contrast, the loitering capability of drones along with their more powerful sensors enables pilots to make final targeting adjustments as they see people running from Hellfire missiles and then carefully document the carnage, by attempting to count and even identify bodies and parts of bodies. One result of this is that UAV pilots, despite operating equipment far from the battlespace (often in Las Vegas, Nevada), frequently experience post-traumatic stress disorder (PTSD) symptoms similar to their forward deployed colleagues.[49]

[48] Pawlyk, "Air Force Will Pit a Drone Against a Fighter Jet in Aerial Combat Test" (2020).

[49] Wallace and J. Costello, "Eye in The Sky: Understanding The Mental Health of Unmanned Aerial Vehicle Operators" (2017).

Executives are unlikely to give up the UAV program since they see strikes as necessary, and see civilian casualties as proportionate to the gains of disrupting terrorist organizations. But could quantum computing improve the targeting of UAVs, allowing them to find flight behaviors that allow them to fly autonomously in contested situations while being invulnerable to most countermeasures?

Berkeley professor Stuart Russell envisioned this scenario in a popular video titled *Slaughterbots*, in which swarms of quadcopters armed with tiny explosives pursue human targets using face recognition, setting off their charges that can "penetrate the skull" and "destroy the contents." A mysterious group obtains the technology and uses it to selectively eliminate political opponents. Russell appears at the end, urging viewers to support a ban on "killer machines," weapons that use computers to select targets and to make the decision to attack. In *Ghost Fleet*, P. W. Singer and August Cole describe a near-future war with China, where UAVs play a major role. Singer and Cole portray fighting UAVs that can perform maneuvers physically impossible for human pilots (because of gravity-induced loss of consciousness) but also perfectly disciplined, such that the drones can fly just above the ocean and obscure their presence by banking into high waves. Clearly, as the offense gains advantages through automation, defensive forces will also have to adopt automaticity.[50]

Two other military innovations point to quantum sensing as a consequential technology. First, increasingly conflict can be waged at great distances and with hypersonic vehicles. Nations have developed hypersonic missiles (those that travel faster than five times the speed of sound yet maintain the maneuverability of a cruise missile) and even railguns capable of firing over 100 miles. These weapons have created great worry both because of their speed and because their use will occur with even fewer warning signs than ballistic missiles. Quantum-enhanced sensing may provide earlier warning signs when these weapons are used.

Second, developments in electronic warfare will change how conflict is waged, and these changes could make quantum technologies a source of superiority. Consider that, in recent conflicts, the Russian armed forces have been able to test out their electronic and cyber warfare capabilities, showing them to be clever and capable.[51] Other

[50]Singer and Cole, *Ghost Fleet: a Novel of The Next World War* (2015).
[51]Creery, "The Russian Edge in Electronic Warfare" (2019).

evidence is mounting that nation states are using GNSS (Global Navigation Satellite System)/GPS (Global Positioning System) jamming and interference regularly.[52] A 2019 report by C4ADS found almost 10 000 suspected incidents of interference with GPS and other navigation systems, and estimated that "Russian forces now have the capability to create large GNSS denial-of-service spoofing environments, all without directly targeting a single GNSS satellite."[53]

Quantum sensing may be a possible solution to GPS jamming and other forms of electronic warfare. Companies and governments are developing "quantum positioning systems" to operate in GPS-denied environments.[54] Like the inertial and celestial guidance systems of the past, quantum positioning, navigation, and timing might perform a backup role to GPS.

8.2.8 Quantum Strategic Surprise: QKD and Quantum Internet

In quantum communications, advances may be so obvious as not to be surprises because there are already articulated concerns surrounding communications confidentiality and integrity. A nation that races ahead in quantum communications might not just deploy quantum key exchange technology, but may create entirely new communications systems and protocols to pursue confidentiality and integrity. However, it is not immediately clear to us why a nation would want to go beyond QKD and pursue a quantum internet. We believe that simply using QKD combined with AES-256, or even QRNG combined with post-quantum encryption protocols, would likely be sufficient to secure communications.

A quantum internet protocol, based on quantum effects, would not just provide randomness and thus strong encryption, but also reveal whether messages have been intercepted at all. This would be strategically relevant because currently, one can never know whether or where a copy of a communication has been made. Perhaps a nation that is skeptical of QKD or AES security might want this extra layer of assurance for confidentiality and integrity. Perhaps quantum

[52] The Coast Guard tracks and publishes incidents of GPS jamming, interference, and failure. Department of Homeland Security, US Coast Guard, "GPS Problem Reporting" (2018).

[53] C4ADS, "Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria" (2019).

[54] Jones, "MoD's 'quantum Compass' Offers Potential to Replace GPS" (2014).

internet plans are products of a lack of trust in one's own network, or distrust of employees, who might be bribed or extorted to undermine the confidentiality and integrity of communications. Finally, knowing about interception means knowing whether adversaries have collected metadata about a communication. Metadata, even of encrypted transmissions, are surprisingly revealing. Nations have long sought clever methods to prevent metadata capture; perhaps excluding adversaries from access to metadata is worth the expense and challenges of developing a quantum internet. However, these technologies are sufficiently far in the future (decades?) that we do not consider them to be a credible policy issue in the near term.

A second implication of quantum internet is the ability to connect distant quantum computers through photonic entanglement. Consider IBM, which in 2020 claimed that it had 18 operational quantum systems. Presumably with quantum internet networking, it could link these systems to create more powerful ones. For instance, its Raleigh 28-qubit system combined with its 53-qubit Rochester device would be larger than any single device. Such a quantum network need only be a few feet from node to node.

Large implementations of quantum internet, however, would require infrastructure coordinated over a great distance, instead of just within IBM Research's lab. Practically speaking, and in the near term, quantum internet infrastructure is likely to depend on satellites, and this shapes the ability of governments to intercept information.

Experiments in dark fiber networks are promising, but quantum states degrade as photons travel through glass and this limits the distance over which fiber can be used to transmit information. Traditional networks use repeaters to cover great ranges. But until fully quantum repeaters are invented – ones that could hold the state in memory and still amplify it to traverse more fiber – each one of these repeaters offers an opportunity for classical interception and analysis.

It would seem that European nations would be poised to implement quantum communications, as relatively small countries could run optical links between cities. For instance, the Netherlands, where some of the most advanced achievements in quantum communications have occurred, might want to connect its seat of government (The Hague) with its capital (Amsterdam), which are only 32 miles apart.

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

Small nations and regions can use optical fiber to communicate, but larger ones will have to also use satellites to overcome the problem of repeating light signals. Satellite transmission is the only medium today that can distribute entangled photons over great distances. This is why China's Micius satellite is an important achievement. Recall that the satellite-linked base stations, combining both fiber optic and free-air transmission, create an entangled photonic channel. This means that the Chinese can beam quantum keys to two distant base stations simultaneously. However, nations that use satellites for quantum communication will need to focus attention on the security of these satellites similar to the ways that they must secure their physical, land-based fiber networks.

These developments in quantum communications are not a surprise we can foresee them and predict corresponding countermeasures. Intelligence and law enforcement agencies already have techniques to address strong encryption. With regard to what we might one day call the "classical internet," interception is easy and not detectable. Much of the Internet's traffic flows through the geographic borders of the United States, but, even for traffic that does not, "prepositioned devices" can quietly copy light from fiber optics at the bottom of the ocean. Because transport and content encryption is used to obscure these communications, and because content is so voluminous, intelligence and law enforcement agencies focus on metadata rather than content. After all, any major governmental or terrorist action requires coordination amongst many actors, activity that is revealed quite nicely by metadata in the form of link analysis. Even when content is at issue, adversaries can hack into devices and cloud services, often through the simple approach of password guessing. Thus, advances in quantum communications are likely to place even more emphasis on attacks using stolen passwords, hacked programs, metadata analysis, and human spies.

8.2.9 Quantum Strategic Surprise: Secrecy and Leakage

Secrecy will be important in a government-superior and -dominant landscape. Governments will seek to keep their quantum computing and sensing advances secret, because there are always countermeasures. The need for secrecy could limit the power that governments can exercise in a practical sense. Knowing a thing is helpful of course, but acting on knowledge can reveal sources and methods. Govern-

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

ments will have to generate cover stories and distractions from quantum programs, lest adversaries deploy countermeasures.

IARPA's Director articulated a series of questions for new proposals that help elucidate the risks of the government-dominant scenario. One asks: "If the technology is leaked, stolen, or copied, would we regret having developed it? What if any first mover advantage is likely to endure after a competitor follows?"[55] Indeed, whatever competitive advantage comes from the government-dominant approach is time-limited and could be perverse. It is time-limited, because the world is leaky and eventually the engineering secrets will diffuse to other nations and even companies. It is perverse because the government-dominant secrecy will hobble the broader market for quantum technologies. While government is dominant, secrecy excludes the private market from working its magic and training thousands of quantum computer programmers and engineers. Thus, the secrecy creates a short-term advantage that might be outweighed by a longer-term deficit in workforce and economic benefit. In fact, one could imagine quantum technologies diffusing in a copycatting country while the source of the innovation continues to treat it as a state secret, not allowing diffusion and growth of the technology in its own country. (This is largely what happened with electronic computing: the UK insisted on secrecy, and the ideas developed there took root in the US.)

To what extent will a government-dominant approach be leaky? In the US, our "five eyes" allies will probably learn, indirectly or not, about the nation's quantum technologies. Theft is a major risk as well. But one form of immediate technology dispersion comes from willingness to share with law enforcement. Law enforcement agencies would find much utility in quantum sensing. Sensitive magnetometers would allow detection of weapons and bombs, even at a distance, in public or even when concealed in a home or vehicle. Just as radiation detectors, X-ray technology, and sensitive microphones are used at the border, new quantum sensors might be used to detect contraband. Unlike physical searches, which focus on certain objects and occur at a discrete time, a quantum sensor "search" might happen remotely, passively, and continuously. A government-dominant scenario explored by the Center for Long Term Cybersecurity envisions

[55]The full list of questions developed by Jason Matheny is reproduced in Danzig, "Technology Roulette: Managing Loss of Control As Many Militaries Pursue Technological Superiority" (2018).

that quantum computers will put law enforcement ahead of every cartel and organized crime body.[56] But law enforcement agencies of less democratic countries might use the same capabilities to pin and skewer protest and opposition movements.

One obvious law enforcement use involves quantum sensors designed to detect contraband. A quantum sensor that could only recognize guns (perhaps it has been trained on a model of the most popular firearms), molecules of particular explosives, and of course, illegal drugs, would be useful with minimal privacy implications. Such a sensor's machine learning could be trained on every contraband item imaginable and be copied to other devices. The sensor would never tire, and be used continuously. Of course, there could be mission creep – why not detect counterfeit luxury handbags? Perhaps the sensor could even be mounted on aircraft and drones to detect weapons caches inside buildings through the roofs of private homes.

Finally, a government-dominant and -superior scenario has implications for the long-term success of quantum technologies. Technology sovereignty – the desire to have domestic champions – is needed to maintain both a strong and secret quantum technology industry. Thus, at the highest level, the secrecy and emphasis on government uses of the technology have long-term practical and public perception consequences. On a practical level, military and law enforcement uses might displace other pro-social uses of quantum technologies, such as drug discovery and materials optimization. The societal benefits of new classes of drugs could save many lives and improve the lived experiences of people. But a government-dominant approach might discount those benefits while seeking to retain its intelligence edge.

From a public perception perspective, it is important to reflect that attitudes towards computing are more positive today in the personal computer era than in the era of the mainframe. Before the personal computer revolution, only governments, militaries, and large businesses could computerize. Early computing empowered already powerful institutions. A government-dominant quantum computing landscape might feel like a replay of the mainframe era.

In recent years, some employees of Silicon Valley companies have renounced the Valley's defense department roots and have pledged not to work on the "business of war." This is a delicate position because many of the technologies developed by companies like Google

[56] Center for Long Term Cybersecurity, "Cybersecurity Scenarios 2025" (2019).

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

are dual use: computer vision projects for automated driving are easily repurposed for UAVs and autonomous weapons. Nevertheless, in a government-dominant quantum world, these employees might see quantum technologies as carrying the "taint" or "taboo" of the business of war. Military-first uses may make public perception of quantum technologies negative, even dangerous. Between the secrecy and quantum taboo, other humanitarian uses of quantum computing could be impeded, with consequences for medicine, materials science, and other scientific discovery.

8.2.10 Countermeasures in a Government-Dominant Scenario: Disruption, Denial, Degradation, Destruction, and Deception

Nations that could not compete in quantum technologies would likely prioritize development of quantum countermeasures. Indeed, all adversaries – quantum capable or not – would be likely to invest resources in some kinds of countermeasures. Such measures are typically classified as "D5" tactics: disruption, denial, degradation, destruction, and deception.

Experimental work suggests effective D5 tactics. For instance, the Chinese scientists discussed in Chapter 7 who achieved satellite-based quantum entanglement and communication had to generate millions of photons in order to overcome channel loss. The scientists had to manage beam diffraction, pointing error, and absorption and turbulence caused by clouds and the atmosphere generally. These challenges raise two vital points: first, interference similar to ordinary atmospheric events – even sunlight and rain, and in the case of underwater communication, water turgidity – can degrade quantum technologies based on photonics. Thus natural events might be simulated to stealthily interfere with the technology. We could imagine weather modification, such as cloud seeding, as a D5 countermeasure to some quantum technologies.[57]

Second, there is very little photonic loss in outer space; thus, there is incentive for operational systems to be placed in high orbit – much higher than the low earth path used in the experiment, and within the reach only of superpowers. One could imagine escalation and even a desire to develop space-based weapons in response.

[57] T. J. House et al., *Weather As a Force Multiplier: Owning The Weather in 2025* (1996).

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

Space Force

The elevation of the Space Force by President Trump has been met with some derision, perhaps because detractors imagine *Star-Trek*–like struggles with people in outer space.

In reality, Space Force will work to manage threats to satellites, the targeting of which will be key in conflicts with the US, China, or Russia. Threats to satellites can be earth-based, but also come from other space vehicles. Although such efforts are veiled in secrecy, strategic opponents are reported to have developed space-borne anti-satellite weapons.[a]

For example, an object that appeared to be space debris "made 11 close approaches to one of the rocket's discarded stages. Such an elaborate space dance would be possible only if the object had thrusters and enough fuel to maneuver very precisely." Sciutto also notes that China has "a satellite with a grappling arm capable of lifting other satellites out of orbit. China has now conducted multiple successful tests of this 'kidnapper satellite,' some of them at geostationary orbit, where America's most sensitive space assets reside, including satellites for communications, surveillance and early warning of a nuclear launch."

[a]Sciutto, "A Vulnerable US Really Does Need a Space Force" (2019).

Each application of quantum technologies has different vulnerabilities. Still, several quantum technologies are uniquely resistant to existing D5 tactics and are being evaluated to operate in their presence. For instance, quantum clocks and location devices are seen as supplements to jamming-vulnerable GPS, and to guard against Digital Radio Frequency Memory (DRFM) jamming. A DARPA project focused on "micro-PNT" seeks to create chip-size quantum positioning systems (QPS) for UAVs, Unmanned Underwater Vehicles (UUVs), and navigators for missiles that do not rely on GPS.[58]

Quantum illumination enhances radar at a very low energy level, suggesting it will not be as susceptible to traditional jamming efforts. Recall that quantum radar involves sending entangled photons into the sky to detect things like missiles and jets, especially those that are cloaked with some kind of "stealth" technology. Thus like pho-

[58]Shkel, "Precision Navigation and Timing Enabled by Microtechnology: Are We There Yet?" (2010).

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

tonic communication, methods that interfere with the generation of entangled photons and that scatter them in the atmosphere may be effective to counter quantum illumination.

Quantum communications security is likely to be less consequential than metrology and sensing developments. This is because D5 tactics can be directed at other aspects of communications activities. Modern encryption algorithms are (almost by definition) never the weakest link in communications. Classical encryption affords such great security that the only known attacks are on the ways that keys are created or extremely clever "side channel attacks" that detect information that leaks out of a presumably secure system. These might include detecting subtle power or frequency variations when a computer codes 0 or 1. Attackers also know that human deception is relatively easy and simple phishing attacks frequently work, as do attacks on cyber infrastructure.

The awareness of surveillance that quantum communications affords is a new factor that might prove more intriguing and useful than communications confidentiality. Recall that because of the no-cloning theorem, Alice and Bob can know something or someone is interfering with their communication: there is no way for Eve to eavesdrop on Alice and Bob, but an attempt to do so will alert Alice and Bob that something is amiss! It is too early to say how nation states will react to this signaling. One could imagine D5 strategies that attempt to poison the channel by engaging in constant attempts to intercept or block photons. Perhaps Alice and Bob can never generate a secure key if some foreign intelligence agency interferes with the QKD. Another (more likely) D5 scenario would be to simply attack Alice and Bob's devices before they communicate, so that one could obtain information before it is encrypted or after it is decrypted.

On the other hand, if denial or degradation of terrestrial-based fiber networks becomes routine, nation states could make their communications harder to reach through using point-to-point satellite QKD.[59]

[59] Satellites could also use QKD for secure satellite-to-satellite communication. Another option for satellite-to-satellite communication is to use the 57 GHz to 64 GHz band. Oxygen has significant radio absorption at 60 GHz, so any such signals will not reach from space to the ground. For this reason, the 57 GHz to 64 GHz band is available for use without license in the US, allowing gigabit wireless communications over distances of roughly 1 km, but only when it is not raining.

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

Finally, D5 tactics might be effective against quantum computers because the devices are so sensitive to environmental interference of all kinds. Simply creating a "noisy" environment with heat, wireless radio signals, and so on, might be sufficient to cause decoherence in quantum computers. Of course, they could also be targeted with conventional ordnance as well. For the foreseeable future, quantum computers will be large, intricate and delicate devices. They will be terrestrially based, in places where human expertise, a lot of electricity, and supercooling helium is available. As the next sections will make clear, these affordances make quantum computers subject to legal and policy interventions perhaps not possible against other quantum technologies, such as metrology and sensing devices that can be miniaturized and deployed in outer space.

Quantum interferometry and communications can be satellite-based, and thus the physical devices are out of reach of most nations' ability to physically destroy them. With powerful quantum intelligence, surveillance, and communications on satellite platforms, quantum technologies might in the coming years be another pressure encouraging the expansion of military force in space.[60] Thus, the handful of countries that both have space programs and quantum achievements might have incentives to invest in anti-satellite weapons. (The development and testing of anti-satellite technology does not appear to be illegal under the Outer Space Treaty, although the treaty does prohibit placing nuclear weapons in orbit, establishing military bases, or conducting military maneuvers on "celestial bodies."[61]) During times of crises, a nation with such capability might find it irresistible – or simply necessary – to destroy satellites in order to impair reconnaissance powers and communication routes of their adversaries.

8.3 Scenario 2: Public/Private Utopia

The government-superior and -dominant scenario naturally focuses on security-relevant developments, and thus government dominance takes on a certain patina. The government-dominant scenario helps elucidate how powerful, well-resourced actors might pursue a quan-

[60] Rabkin and John Yoo, *Striking Power: How Cyber, Robots, and Space Weapons Change The Rules for War* (2017); J. Yoo, "Rules for The Heavens: The Coming Revolution in Space and The Laws of War" (2020).

[61] Ortega, "Placement of Weapons in Outer Space: The Dichotomy between Word and Deed" (2021).

tum technology agenda. However, that scenario should not detract from a scenario we think more likely: that the private sector makes significant advances in quantum technologies and outperforms government labs, just as it did in electronic computing and cryptography.

In both electronic computing and in cryptography, the private sector's emphasis on information sharing and commercialization eventually overcame government's first-mover advantage. From the 1950s through the late 1970s the US government had the fastest computers in the world at its disposal and the most mathematicians specializing in cryptography in its employ; neither was true by the end of the twentieth century. Today the US government still has an impressive array of systems at its disposal, but nearly its entire infrastructure is assembled from commercial off-the-shelf systems. And while official statistics are not available, it is widely assumed that there are more cryptographers at universities and corporations than are directly employed by the government.

We believe that the same outcome is likely in quantum technologies as well. The benefits to individuals in terms of both prestige and salary, combined with the commercial benefits that will accrue to their employers, will be substantial in the coming years: this will create incentives to further democratize quantum technologies. Governments will purchase off-the-shelf systems and will surely contract with corporations to build secret devices. But the age-old pursuit of profit drives actors in this scenario to apply quantum technologies to solve all sorts of problems, all over the world. Quantum technology won't be put back in the bottle.

We see a number of factors and incentives combining to make a mixed government/commercial scenario the most likely one. Chapter 4 discussed the many efforts being made by cutting-edge technology companies in quantum research. This reflects the overall trend of private-sector investment in research and development in the US. In recent years, US research and development has continued to grow and the most recent figure pegs it at $580 billion annually.[62] But R&D characteristics have changed. The private sector is investing more money than ever in R&D, with pharmaceutical development being a leading contributor. The federal government's investment

[62] Congressional Research Service, "US Research and Development Funding and Performance: Fact Sheet" (2020).

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

has largely flattened, although it is still primarily focused on basic research rather than applied research, technology development, or market creation.

Aside from a focus on development, private researchers operate with different incentives and constraints than those working in government labs or even universities. Private-sector researchers may have the advantages that make it possible to make breakthroughs in quantum computing. But private researchers *do* operate with constraints – they must have champions within the company willing to protect their funding for years. They must be able to show progress and results, and defend these goods against competing demands that directly contribute to the bottom line of a competitive firm.

The good news for these private researchers is that many of their companies are sitting upon huge amounts of cash. As of this writing, Amazon, Google, and Microsoft all have cash reserves in excess of $100 billion – meaning that these individual companies have more money in cash than the GDP of many Low or Middle Income Countries. Furthermore, private researchers have an advantage over academics in that they can devote their time to building devices instead of teaching, chasing funding grants, and earning tenure – although, even in corporate labs, there is still the pressure to publish in top-ranked journals.

Private researchers also have an advantage over government lab scientists because they are freed from the secrecy constraints imposed by security clearances. Although private companies can be very secretive, their researchers do not have to undergo the extensive background checks and hassles associated with maintaining a security clearance, which has implications for personal freedoms and for one's workforce in profound ways.[63] Private companies can also hire the best and brightest from all over the world, as citizenship and attendant concerns about loyalty will be less important than in government employment. Of course, hiring such individuals carries risks, but as we saw in Section 8.2.4 (p. 329), the government's background investigation process has not prevented the theft of secrets.

[63] Ben Rich laments that as Lockheed's Skunk Works took on sensitive projects, a huge portion of otherwise reliable employees had problems passing drug screens associated with the clearance process. Rich claims that 44 percent of applicants tested positive for drugs. Rich and Janos, *Skunk Works: a Personal Memoir of My Years at Lockheed* (1994).

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

Private sector researchers will not only be freed from many constraints that competing academic and government scientists face, their incentives will run towards non-national-security-related uses in the long term. This is because quantum technologies have so many commercial uses. Simply put, much more money can be made in commercial uses of quantum technologies because there are more buyers and a broader spectrum of uses outside national security. In the short term, companies may affect a national-security lilt, recruiting retired generals to their boards and emphasizing their DOD Projects. But this posture is likely temporary as companies use government projects for initial funding, and then sublimate company efforts to more broadly appealing commercial applications.

Quantum computing will have a host of non-security-related consequential uses. Competitors investing in quantum computing are focused on simulation of quantum mechanical events, in order to develop drugs, new synthetic materials, and engage in high-energy physics experiments. Some see quantum computing as a tool that will help us discover a room-temperature super-conductor or easier-to-control nuclear fusion. Others are focused on quantum computing's parallelism as a mechanism to build machine learning tools that can make sense of high-dimension datasets. The benefits could be legion. In any area where dimensionality is so high as to make analysis intractable or coarse, we can envision quantum computing making more sense of the world. Whether those applications are automobile traffic flow or logistics in the form of train or airplane scheduling, we can imagine a future with less waiting and more efficiencies.

8.3.1 How Quantum Technologies Could Change Governance and Law

As we explored the superior/dominant scenario above, we saw how nations might use quantum technologies to better understand other nations. In a world where private companies have quantum computers and sensing, their capabilities will similarly be trained on other companies and individuals, but this time in the search of profit. Thus, a threat discussion needs to contemplate how quantum technologies will contribute to power shifts between companies and individuals. Uses of quantum sensing and computing to govern human activity could displace democratic processes and become laws unto themselves.

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

Quantum sensing and computing will reinvigorate grand schemes to perfect society. Technological revolutions have long brought about utopian ideals for redesigning societies. These are "revolutions from the top," and they typically threaten individual autonomy in profound ways. In *Seeing Like a State*, Yale political scientist James C. Scott discusses several generations of social reformers who use new scientific insights to design putatively better systems – from more productive forests, heartier tomatoes, to more efficient cities. Scott terms these efforts "high modernism," an almost religious belief in technology to reorder natural and social systems. The most dangerous form is "*authoritarian* high modernism," where the coercive power of the state combines with scientism, creating a force that overrides markets and individual preferences in the pursuit of some ideal.[64]

Scott warns that high modernists, in their zeal, tend to discount complexity, local knowledge, and in particular *metis*, the ancient Greek word used to convey skills and learnings acquired by the skillful and clever. The concept of *metis* is best represented by Odysseus, the resourceful yet perhaps unprincipled[65] hero who solves problems pragmatically with little concern for ideological or moral purity or truthfulness. High modernist plans often fail to consider *metis*. After all, the point of *metis* is to act in a way that cannot be predicted by those who lack it.

Quantum computing could be enabling technology for several large-scale social experiments. High modernists will see it as the tool that can finally incorporate *metis* and other local knowledge, creating a kind of master system. We might imagine intrusions into the economy, our living circumstances, our bodies, and even our minds. As such, high modernist plans directly regulate people and become a form of law and governance through architecture and technology rather than through deliberative self-governance.

Friedrich Hayek and the Austrian School of Economics have definitively won the debate over the primacy of centrally planned or market-led economies. As Hayek recognized, there is just too much information in the forms of preferences, supply, and demand for a central

[64] J. C. Scott, *Seeing Like a State: How Certain Schemes to Improve The Human Condition Have Failed* (1998).

[65] "Tell me about a complicated man" begins Emily Wilson's translation. See Homer, *The Odyssey* (2018). Compare with Lattimore: "Tell me, Muse, of the man of many ways" and Fitzgerald: "[sing] of that man skilled in all ways of contending."

planner to sense and make sense of it. The twentieth century showed planned economies to be slow adapting and both the Soviet Union and China have shifted to more free-market economies, often with aggressive state industrial policy or other economic action. But perhaps central planning will be revisited if a sufficiently large quantum computer could make sense of the multifarious signals of an economy.

In such a scenario, the utility-maximizing individual loses its primacy and even its agency in favor of an economic oracle in the form of a quantum computer.[66] One could imagine a long period of transition where data-heavy, sophisticated companies demonstrate winning strategies by ceding human instinct and control over marketing, advertising, logistics, and other functions to a quantum computer. Perhaps the first adoption will come from financial services firms trading securities, as this is a field where computers already automatically analyze and conduct trades. Or perhaps it could be Amazon.com, Inc., with its huge marketplace, computing power, and fantastic logistics system. If these first movers experience success, they will pull away from competitors, offering lower prices while finding savings and efficiencies identified by the quantum economic oracle. Their successes could have a snowball effect that convinces other sectors of the economy to trust more in automated analysis and execution. But if this happens, one of the most important bastions of the liberal economic order – the notion that the emergent effects of individual decisions make the best free market – could end in favor of an increasingly centrally planned and coordinated economy.

The displacement of governance and law is most palpable in corporate efforts to reshape our lived environment. Efforts to perfect our lives, such as "smart homes" and even "smart cities" require tremendous sensing capabilities and computers for sensemaking. Efforts such as Google's "Sidewalk Labs" foresee a revolution in urban planning, based primarily around redesigns and new thinking on mobility. Among the ideas are to create an urban infrastructure that can change as needs shift throughout the day. Traffic lanes might change direction automatically and vehicular movement would be optimized to accommodate multiple modes of transportation, the need for parking, and so on. Embedded sensors and mobile phone tracking are key for these endeavors, and instant sensemaking is necessary

[66] Evgeny Morozov explores attempts to perfect central planning with computers in 1970s Chile, in Morozov, "The Planning Machine: Project Cybersyn and The Origins of The Big Data Nation" (2014).

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

because the second-by-second decisions to control the environment could mean accidents or even death.

Like the quantum-computing planned economy, the smart city reflects the pathologies of high modernism, with its displacement of democratic governance and law. High modernists present these plans by showing only the benefits and omitting their less appealing implications. For instance, despite all its benefits, the smart city requires that individuals obey an arbitrary, unknowable authority – the algorithms that replace the laws and institutions and people that make up a government. Usually implicit in smart city schemes is that people would have to give up control over driving, a privilege thought to be a freedom for many Americans. And once that privilege or freedom is waived, the individual's needs can be subordinated to others. One's vehicle might stop to optimize overall traffic. One could imagine waiting for minutes as another flow of traffic is prioritized, perhaps to address a fomenting traffic problem elsewhere in the city. No longer would the car be the instrument of the individual's immediate self-interested needs.

Public/Private Utopia

Governments and the private sector advance state of the science, eventually commercializing sensing, computing, and communications.

Key Policy Characteristics

Industrial policy, need for liberalized export controls, relative openness in innovation and immigration.

Key Enabling Factors

Diverse set of competitors, market for components, availability of trained workforce.

Strategic Surprise

Entrepreneurs use quantum sensing and computing to shape society to their liking and increasingly to displace public governance with private decision-making systems.

Outlook

Because quantum technologies are in reach of even well-funded startups, a public/private outcome is the most likely scenario.

There is no "opting out" of the system because the smart city is so interdependent. Even outside the car, individuals will have to submit to the system. A

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

pedestrian might have to wait (or qo quickly) to ease traffic pressure far from view. Already, in cities that are testing automated vehicles, such as Las Vegas, Nevada, pedestrian barriers first erected to address drunken drivers plowing into sidewalks are being enhanced to make it nearly impossible for pedestrians to jaywalk because automated vehicles are flummoxed by unpredictable pedestrians. Planners will have to design-in coercive architecture in order to ensure that individual autonomy cedes to the oracle and to the vehicles that could run over the individuals.

Both the planned economy and the planned city require individuals to sublimate their immediate self-interest for the goal of shared efficiencies and gains. For instance in a 2019 blog post, Ford describes how it used Microsoft "quantum-inspired" technology to simulate optimal traffic routes in Seattle. The team claimed it could achieve an overall 8 percent reduction in traffic over a population of 5000 drivers, but this reduction requires an alternative to what we are used to – "selfish" routing.

Giving up on selfishness in favor of overall efficiency raises a series of practical, political, and even emotional challenges. Central planning and control is a particularly difficult state to achieve because it asks individuals to pit their immediate, felt emotions and needs against the abstract idea of collective benefits. These collective benefits are real. Minor efficiencies can indeed add together to create significant savings for individuals, but these are far more subtle than the immediate rush of, say, putting the pedal to the metal. And those most trusting of their inner instincts who are tempted to ignore the commands of the smart city are probably the ones least capable of self-reflection (and self-restraint).

For collective schemes to work, officials must also explain the trust model carefully and convincingly and these models must be subject to political scrutiny and consent. If some class of people, such as the ultra-wealthy in Russia who put emergency lights on their cars to evade traffic, get preferred treatment and quicker routes, this must be explained and accepted in some way by the system's participants. In modern cities, busses and high-occupancy vehicles enjoy reserved car lanes, but we can both readily observe this compromise and agree to it because of the social interests in efficiency. Google co-founder Larry Page is known for his hatred of automobile traffic and has invested in "flying cars" to solve the problem. As one sees Page's car move swiftly through the smart city, will one think that like the

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

Russian oligarchs, the designers of the system get special treatment?

8.3.2 Implications for Human Primacy

How will a quantum-planned economy or society coexist with populist instincts to celebrate "independent" thinkers? Will *metis* be cherished, or be seen as sand in the gears of a fantastically efficient society?

On a deeper level, will the "intelligence" of these systems represent a turning point in the view of human intelligence and analysis as fundamentally special? The pendulum could swing back to a worldview where elites – the small number of people who operate and understand quantum technologies – have more command over ideas and the matters of what is correct and incorrect.

One could imagine a transition period where the veracity and benefits of quantum technology predictions make life better. Perhaps quantum computers could ease the transition by finding effective communication strategies to explain the sacrifices that individuals make for the broader efficiency of the system, or more directly, the benefits that the individual receives by forbearing from what appears to be the most self-serving, available option.

As the primacy of the individual recedes, how might humans seek to regain the status of being special? One could imagine genetic research and prediction would receive new attention in a world with quantum computers, leading to pressures to change both lifestyle and choices in reproduction.

Genetic prediction and personalized medicine (sometimes called precision medicine) was much hyped at the start of the Human Genome Project in the 1990s. Some scientists predicted a complete revolution in therapies flowing from the project, in which the US government invested billions. Heralds of the project conceived of discoveries of single genes that would predict morbidity, and thus relatively simple treatments and behavioral interventions. Yet decades later, the hype remains, but with little to show for it because so many diseases are not genetically determined and, among those that are, hundreds of genes may be involved in disease. In addition to the complexity of multiple genes, our health is a product of contingent environmental and behavioral variables, many of which are essentially unknowable. This is why, 20 years after the launch of the Human Genome Project, the leading business-to-consumer genetic testing company is still in essence an entertainment product, carry-

Embracing Probabilities

Several different theories have emerged to help explain the counterintuitiveness of quantum phenomena and the differences with classical physics. The Copenhagen interpretation, pilot-wave theory, and the theory of many worlds compete to account for quantum phenomena and provide some meaning for them in our lives.

In the soft sciences, experts are comfortable in conceiving of case outcomes, rules, and even facts probabilistically. Turning to law and policy, prediction of uncertain events, of court or regulatory decisions, is the stock-in-trade of lawyers. Law professors expect their students to predict that a court will "probably" come to a certain conclusion. They even teach that "facts" have some subjectivity. We do not know a jury's verdict and cannot observe a jury deliberation until it concludes. We could think of a verdict unsealing as a measurement of an uncertain process.

The law is rife with probabilistic standards to address the problem that there is imperfect knowledge of events, and what knowledge that does exist is colored by observer bias and misinterpretation.[a]

The law is satisfied establishing facts despite uncertainty, and does so by setting burdens of proof (e.g. preponderance of the evidence) and by assigning them (e.g. to be established by the plaintiff) so that matters can go forward and have resolution, even an imperfect one. As consequences become more grave, the law imposes higher burdens of proof and assigns them strategically, often to disadvantage the state.

The law lives with probabilistic standards because they embody a method that if applied systematically will produce justice, if not always a just outcome in each encounter with the law. That method must evolve with time, as society is shaped by new technologies, new norms, and new understandings of human behavior and expectations. In a systems-level sense, an embrace of a probabilistic universe does not threaten our basic methods and institutions.

[a]We allow police to check persons for weapons based on a "reasonable suspicion" that a suspect is armed. We allow the state to arrest people if officers reasonably have "probable cause" to believe that the suspect has committed a crime.

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

ing a lengthy "quack miranda warning" to disclaim the health claims the company implies with its marketing.[67]

But if the barrier to personalized health is the complexity of genes, behavior, and environment, might quantum computing's dimensionality be the answer? The promise of precision medicine is that knowledge about genes will create opportunities to act and prevent disease. As the knowledge puzzle begins to reveal a picture, a complementary development by Jennifer Doudna, CRISPR-Cas9,[68] provides a fast and low-cost way to manipulate genes. To take the decision now to alter a human is widely considered to be reckless and irresponsible. But might our attitudes change as quantum computers provide us with what we think is understanding of the relationships between genes and phenotype and the environment and disease? Combined, these developments could shift the risk–benefit calculus surrounding genetic manipulation.

What if personalized health still doesn't deliver the expected benefits? Advocates will say that the quantum computer needs more data, and there will likely be a movement to collect even more information about the inputs to a person's health: what you consume, where you walk and travel, the air you breathe, and details of physical activity. Only then will we learn the degree to which the messiness of health outcomes is determined by random chance out of control – which for many people, may be the most frightening insight of all.

Turning to our mental states, online advertising remains one of the chief reasons that companies surveil and make sense of ordinary people and their private activities in a quest to decipher their thoughts and preferences, termed *surveillance capitalism* by Shoshana Zuboff.[69] Despite the surveillance aperture of the online advertising model, online advertising itself is still quite coarse. Online

[67] In various places 23andMe describes its service as surfacing "health dispositions." At the bottom of several of its customer care pages is a disclaimer that includes the text: "The test is not intended to tell you anything about your current state of health, or to be used to make medical decisions, including whether or not you should take a medication, how much of a medication you should take, or determine any treatment." See 23andMe, "Choosing Which Reports to View" (n.d.).

[68] Emmanuelle Charpentier and Jennifer A. Doudna earned the 2020 Nobel Prize in Chemistry "for the development of a method for genome editing." See Doudna and Charpentier, "The New Frontier of Genome Engineering with CRISPR-Cas9" (2014).

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

platforms have voluminous amounts of data on users. Some platforms not only know what websites people visit, where they go in the physical world, who their friends are, and how they spend money, they also know what people choose not to do (for instance, if one writes a message on a service, edits it, or decides not to send it). But advertising remains coarse, in part because of the size of the surveillance aperture.

Many people are familiar with the experience of being "retargeted" when considering an online purchase: search of "cheap mattresses" on Google, for example, or read a few reviews, and pretty soon mattress advertisements will show up on many websites that you visit. If you go to a website to actually make a purchase, then change your mind at the last minute, you'll start seeing advertisements for the specific mattress that you almost bought: this is "retargeting," and it appears to be effective in getting consumers to consummate their purchase.

The problem with today's information economy becomes clear *after* you click the "buy" button for the mattress. Despite the fact that a mattress is pretty much a once-a-decade purchase, you'll continue to see advertisements for mattresses. They won't go away for weeks. That's because the advertisers don't take into account that you've made that purchase decision and have stopped looking, even though the data should be relatively available.

Because of the data volume, no company can fully make sense of people, thus two strategies are taken: place users into an abstract category that captures their commercial characteristics (male versus female, high income versus low income household, etc.), and/or throw out old data.

As companies build larger quantum computers, advertisers – and other companies with surveillance incentives such as insurance firms – will take advantage of extra dimensionality to both create finer profiles and to analyze more historical data. What this means for people is that quantum computers will be yet another technology that makes individuals' desires, personalities, and lives more legible to powerful decisionmakers. The converse is likely not true – ordinary people will not train these same technologies to scrutinize powerful companies (other than to decide whether to invest in them).

Quantum sensing, in fact, might be the technology that fundamentally erodes what it means to be an individual. It is no accident that Google is a center for thinking about quantum technologies,

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

but also about the concept of "technological singularity," a series of speculative technical advances that seek to create computers that can build faster, more intelligent computers, which would create more intelligent computers still. All of this seems pretty frightening, except that part of the singularity religion is that the computers we create will bring us along for the ride with advanced technologies that can unmoor humans' minds from physical bodies and allow them to merge with machines, creating some kind of advanced symbiotic "intelligence" – and achieving immortality in the process. To join the computers at this acme of intellectual accomplishment, we would need to make sense of and "copy" the structure and physical representations of memories and knowledge in the brain. This may be the ultimate use case for quantum teleportation.

For path-dependent reasons, these exciting and troubling applications of quantum computing are obscured in many accounts of the technology. The discovery of the Shor and Grover algorithms early in the history of quantum computing caused cryptanalysis to far overshadow other applications – even Feynman's existential quantum application of simulating physics. We think this is unfortunate. It is obvious that new and faster drug development and discoveries that lead to fusion energy are more consequential than code-breaking. In fact, it might be Grover's algorithm, so often presented by the media as a code-breaking tool, that delivers some of these breakthroughs, because Grover's underlying utility is that it speeds up mathematical search algorithms.

Quantum communications is promising but not as exciting as quantum computing in this scenario. Strong encryption has long been available to people, although it was awkward to use until recently.[70] In a short time however, a number of companies developed high-quality, widely adopted, usable communications tools with end-to-end encryption, such as Signal, software funded by former Facebook executives upset by the company's depredations of privacy.

If democratized, QKD could accelerate the trend of putting even stronger encryption into the pockets of ordinary people. But for most users, the difference between an encryption system that is computationally secure and one that is information-theoretic secure is not meaningful.

[70] Whitten and Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0" (1999).

Quantum sensing, if we key this field's birth to NMR and MRI machines, has already contributed to the treatment and health of untold millions of people. As quantum sensors become smaller and can operate at ordinary temperatures, they can be moved closer to the patient, allowing for greater resolution.

In fact, medical uses for quantum sensors might be the "killer" application with a market for both in-facility and in-home devices that is vastly larger than military and intelligence ones. Consider how many people avoid diagnostic tests that we know are effective because of the indignities and fear associated with the test process itself. Imagine how many people would be delighted to replace an uncomfortable, invasive physical examination with a passive one performed by a quantum sensor. One's annual checkup might include a comprehensive body scan that could be compared to previous captures in order to detect unwanted changes in the body. Of course, full-body scans have been marketed to consumers for decades, but existing ones irradiate the body, produce false positives that result in dangerous procedures, and have not demonstrated a general medical benefit. The passive nature of quantum sensors with added resolution, paired with individuated analysis, offers a scenario with earlier diagnosis and, we hope, better health outcomes.

One could even envision an in-home device that provides a regular medical scan of individuals. Perhaps people with high genetic risk of cancer would be the first willing to pay for such a device. These individuals might have a daily scan for diseases of concern, and to be able to make other measurements about the body.

More broadly, a public/private scenario could include many forms of self-surveillance brought on by quantum sensors. Consumers have broadly bought into the "Internet of Things," internet-connected devices in the home, many of which make health and fitness claims. The demand for such devices is substantial, creating a virtuous cycle of new products with interesting new features, and stimulating competition among different vendors to provide operating systems for the home. But in practice, many of these devices are abandoned soon after they are bought, because their usability is poor and the services that they provide are trivial.

Internet of Things devices based on quantum sensing, because of sensitivity and passive information capture, could be a winning technology of the home. Consider a technology developed by MIT professor Dina Katabi that uses in-home radio waves to passively

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

measure many kinds of physiological phenomena. Movement, breathing, heartbeat, and sleep patterns all subtly affect the low-power electromagnetic waves that are emitted by Katabi's device, reflected by water in the body, and then measured upon their return.

Katabi earned an Association for Computing Machinery prize for its development, and has expanded use cases for the technology into important areas such as fall detection, and contexts such as the hospital, where such passive monitoring would nicely replace the various devices to which patients are tethered. One can see why this technology might displace existing Internet of Things devices and be purchased for every hospital room: no one needs to wear anything or worry about finding the right charger for their tracker. There's no device to abandon, and so the sensor becomes more like a smoke detector that can be placed and function for years without user futzing. One can also imagine the quantum technology improvement on the approach: with even more precise timing and more resolution, more insight about the internals of the body can be had.

Industrial and commercial users may be the leaders in adoption, as well. For similar reasons of convenience, employers might want Professor Katabi's device to monitor worker efficiency and health. Perhaps with accurate and quick measurement of worker activity, one could train a robot to replace those workers, with their pesky breathing and heart rates and illnesses.

Oil services firms are among the biggest early investors in quantum sensing research and development. The industry clearly sees the potential for greater extraction activities brought on by quantum sensing. Absent more regulation on oil exploration and extraction, environmental threats will likely emerge as a problem in a private-sector-dominant quantum sensing world. Perhaps quantum sensing will drive a new wave of extraction activities, not only for oil and shale, but also for rare-earth materials and minerals. But one could also foresee a host of more complicated scenarios – more precise sensing might reduce exploratory drilling and prospecting activities, or it might make extraction more precise. For example, regulators could require detailed surveys of underground water flows before drilling or mining permits are granted.

8.4 Scenario 3: Public/Private, East/West Bloc

The previous section discussed a series of quantum technology successes brought about by enthusiasm and cooperation among govern-

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

ments and the private sector. In a way it described a technology utopia, a mythical, perhaps perfect place. Yet it should be remembered that *utopia* is a combination of the Greek words for "no" and "place" with a Latin -ia ending. A more realist version of the scenario takes on a Cold War patina, one where East races West in its pursuit of quantum technology dominance.

Technology development is a focus of national competition, with economists increasingly elucidating the links between government incubation of basic research and private-sector payouts.[71] Historians too are making the connections between Silicon Valley's rise and generations of government investment in infrastructure and military research efforts.[72] Technology research occurs on a canvas with increasing nation-state divisions. After decades of public policy that sought Westernization of China through empowering its middle class, the US changed direction under Presidents Trump and Biden. Europe's cohesion strains under economic pressure and from immigration tensions that contributed to the 2016 "Brexit" referendum on the United Kingdom's membership in the European Union.

Technology competition is now a major topic of international relations.[73] Consider that after Brexit, the European Union excluded UK companies from participating in its Galileo satellite navigation program. The UK is struggling to establish its own "sovereign" space program. The US, UK, and EU face a common challenge in China. China's Belt and Road Initiative proposes a major reinvestment in infrastructure across Asia, Africa, the Middle East, and even Europe itself. Participants will not only receive funding for massive capital projects, but also new strategic partnerships with China. In 2019, the Italian government signed a memorandum of understanding to join the Belt and Road Initiative. Liberal observers are concerned that as China's infrastructure and investment spreads, a new Silk Road will speed China's sphere of influence, bringing authoritarianism, China's breed of state capitalism, and the spread of China's military presence elsewhere in the world.

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

[72] Nash, *The Federal Landscape: an Economic History of The Twentieth-Century West* (1999); O'Mara, *The Code: Silicon Valley and The Remaking of America* (2019).

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

Under President Trump, the US took increasingly aggressive measures to cabin China's technical might. These have included a new focus on export controls; strategic deterrence of China's most competitive companies, such as Huawei; imposing restrictions on suppliers to Chinese firms in order to harm the country's competitive posture; the threat to allies to withhold intelligence support unless they remove Chinese components from their networks; and even the criminal prosecution of faculty members alleged to have received funding from China that was improperly disclosed.

These trends could produce a scenario where two factions, one including China, Russia, and perhaps even some Westernized nations enticed by Belt and Road, and a second representing the US, Japan, and Europe, compete to reach quantum technology superiority.

The East/West bloc scenario is not necessarily a *dystopia*. Viewed through a practical lens, a quantum technology national competition – on sensing, computing, and communications – is a less risky one than tussles focused on weapons systems. It is more akin to the outer space race than an armaments race, as is the competition between the UK and the EU for sovereign space programs. Such national competitions are also likely to prompt huge amounts of public investment in research.

East/West Bloc Scenario

Governments and private sector collaborate, but in sharp competition divided between China and the US and EU.

Key Policy Characteristics

Secrecy, limits on immigration, and industrial policy in pursuit of technological sovereignty.

Key Enabling Factors

Bloc scenarios are more likely if quantum technologies are more difficult to create than currently thought, and if countries choose technology stacks of differing effectiveness.

Strategic Surprise

A nation achieves superiority by pursuing a successful quantum computing substrate that others cannot.

Outlook

More dependent on international relations than any single technology. Decoupling, technology/data sovereignty make a bloc scenario more likely.

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

Governments won't be able to complete that research alone; much funding will flow into universities and the private sector. Indeed, to take the UK's post-Brexit space race as an example: instead of building its own program at the cost of billions, the UK is investing in domestic aerospace company OneWeb.

Secrecy and export controls would be one cost of the competition scenario. These controls could slow down innovation and the democratization of quantum technologies. They might also posture development towards military and intelligence uses of quantum sensing and computing rather than to ones that will directly benefit people in their lived experiences. For instance, development in a market economy might naturally flow to healthcare applications of quantum sensing. But in a scenario where worries surrounding technology leaks abound, the government will not want powerful and potentially portable sensing technology in every hospital.

Indeed, some early entrants to the quantum computing race, such as D-Wave Systems, sold devices to clients. But as covered in Chapter 4, quantum computing is likely to evolve into a cloud model. The East/West bloc scenario might cement the cloud approach in fact. This is because the cloud model provides companies a thick veil of secrecy for the devices themselves. The secrets of engineering, the hard-won tradecraft learned in assembling and maintaining a quantum device, all stay in a secure room available only to company technicians. The cloud model allows companies to secretly implement enhancements and keep them proprietary in a physical sense. Of course militaries will demand to have on-premises devices, and these will be guarded like their cloud-based siblings. But it won't be possible for a company to simply buy a device and reverse engineer it in order to learn the easy way.[74]

Experts from these different blocs may be unwilling to participate in knowledge exchange opportunities and even employment at international firms. In fact, East–West competition could bring about the same sort of lifetime employment and loyalty that was seen during the Cold War research boom.

In the long term, the competitive scenario presents a mixed picture for technology development. Many innovations are path-dependent, a result of initial development success that leads to waves of

[74]Some speculate that Google's purchase of a D-Wave Systems machine in 2013 was for the purpose of reverse engineering the device.

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

greater investment and lock-in to certain assumptions. For instance, in classical computers, silicon is the medium that dominates architecture, and hardly anyone considers alternative media. In quantum computing, everything from hardware to software is up for grabs. The medium for mastering quantum effects could be based on several competing alternatives, from topological approaches touted by Microsoft to the superconducting circuits used by Google and IBM. No matter what physical medium is chosen, control systems and software matters must be settled.

With so much so uncertain, East and West may choose different quantum computing paradigms, different technology stacks, and different software approaches. The divergence could be dramatic and the differences important. The divergences could identify the best hardware and software and possibly undo the path dependence that might happen without competition.

For instance, if the West pulls ahead in quantum technologies and establishes a software stack written in English, language alone will provide the kind of advantage that makes it easier for English speakers to enter the field, as it did in both the first computer revolution and the first two decades of the Internet.

At the same time, secrecy could result in siloed approaches, or even the identification of a certain approach as virtuous or lacking virtue.[75] One need only look to the history of steam and electricity to see an example where a dominant technology (steam) was romanticized as honorable and superior in attempts to resist electrification. We might see similar values attributed to hardware and software approaches; some might be called "red" instead of merely different and possibly better.

One would hope that after current hostilities and suspicions de-escalate, a period of cooperation would follow, and this period would benefit from the experimentation and different paths chosen by East and West. We could imagine a new period where globalism trumps nationalism, and an opportunity presents itself to identify the best of approaches explored by different factions.

But during the period of conflict, what we are willing to do to win might surprise us. Take intellectual property theft. It is safe to say that American norms towards intellectual property are relatively pious. A large group of innovative American companies have saber-

[75] Juma, *Innovation and Its Enemies: Why People Resist New Technologies* (2016).

rattled for years about China, complaining of dramatic losses of trade secrets, lost revenue from pirated movies, and about eerily similar copies of domestic inventions. Intellectual property theft became an executive-level concern during the Obama administration, resulting in a complaint to President Xi.

The desire to win may also change our attitudes toward stealing innovations. These attitudes are malleable, if one takes an historical perspective. When the US was an upstart nation struggling to develop an industrial base of its own, our forefathers were impious towards intellectual property and unrestrained in their appropriation of others' inventions.[76] In pursuit of technological superiority or sovereignty, might we adopt the tactics of using spycraft to steal and copy others' innovations?

8.5 Scenario 4: Quantum winter

Consider the shade cast on quantum computing by quantum computing skeptic Mikhail Dyakonov:

> "In riding a bike, after some training, we learn to successfully control 3 degrees of freedom: the velocity, the direction, and the angle that our body makes with respect to the pavement. A circus artist manages to ride a one-wheel bike with 4 degrees of freedom. Now, imagine a bike having 1000 (or rather 2^{1000}) joints that allow free rotations of their parts with respect to each other. Will anybody be capable of riding this machine? …
>
> "**No, we will never have a quantum computer**. Instead, we might have some special-task (and outrageously expensive) quantum devices operating at millikelvin temperatures."[77]

[76] Ben-Atar, *Trade Secrets: Intellectual Piracy and The Origins of American Industrial Power* (2004).

[77] Dyakonov, *Will We Ever Have a Quantum Computer?* (2020).

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

What if, as some critics like Dyakonov argue, quantum computing is just too complicated and too hard a problem to solve – at least for the next few decades?[78] What if, as happened in artificial intelligence in the 1970s, and in cold fusion, quantum technologies experience a "winter," a period where enthusiasm and funding for the entire class of technologies lags?

In the quantum winter scenario, quantum computing devices remain noisy and never scale to a meaningful quantum advantage. Perhaps research on quantum computers and machine learning leads to optimizations for classical algorithms, but classical computers remain faster, more manageable, and more affordable. In this scenario, "quantum" might remain a serviceable marketing term, but companies will soon figure out that classical supercomputers, simulators, and optimizers outperform them. After a tremendous amount of public and private monies are spent pursuing quantum technologies, businesses in the field are limited to research applications or simply fail, and career paths wither.

Quantum Winter

Large-scale quantum computers do not emerge within a decade.

Key Policy Characteristics

Policymakers recognize failure, reallocate funding. Need mechanism to reassess, recognize thaw.

Key Enabling Factors

Scaling strategies unsuccessful, as mid-size quantum computers don't trigger virtuous cycle of device growth.

Strategic Surprise

Nations reorganize educational systems, spend billions in quantum computing that never produces new innovations; nations that invested in other technologies pull ahead and prosper through automation and advanced services.

Outlook

While quantum computing flounders, quantum sensing still flourishes. Quantum communications loses steam as the cryptanalysis threat diminishes.

[78] Dyakonov, "When Will Useful Quantum Computers Be Constructed? Not in The Foreseeable Future, This Physicist Argues. Here's Why: The Case against: Quantum Computing" (2019).

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

In this scenario, funding *eventually* dries up for quantum computing. Academics and scientists in the field either retool and shift, or simply appear irrelevant, even embarrassing. As the winter proceeds, hiring priorities shift to other disciplines, further sidelining quantum technologies as a field. Even where important developments are made, they are given short shrift, viewed with skepticism, or simply seen as irrelevant to computing praxis.

One of the greatest risks of a short-term failure scenario is whether we are willing to recognize it. One sign that quantum winter is approaching would be for quantum technology advocates to continually "move the goalposts," and insist that grand discoveries are around the corner if we just keep funding the dream. The politicians, military leaders, scientists, and CEOs who invest in quantum technologies will become diehard defenders of them – until they stop or are replaced. If we do not recognize failure, investment in quantum computing will continue to be at the expense of other, more promising fields. To take a current example mentioned above, the billions of dollars invested in precision medicine have not delivered on promises of revolutions in therapy or life extension. Its advocates, perhaps because their professional reputations are tied to its promise, keep the faith.[79] Meanwhile, public funding for precision medicine has appeared to come to the detriment of tried-and-true investments, such as public health interventions.[80]

The primary danger of a quantum winter isn't the wasted resources and careers – it's that research abruptly stops, resulting in economic dislocation and delaying discoveries that aren't around the corner, but may be just over the horizon. The AI winters (there were two) stunted some research efforts that eventually proved successful, and killed others outright. The failure of modern AI systems to incorporate systematic approaches for knowledge representation and explainability – two hallmarks of the earlier AI waves – may be a lasting negative impact.

A quantum winter would be in keeping with the boom/bust cycle of many technologies in the West. Before the bust, there is general technology optimism, boosterism from news media and investors, emphasis on growth over sustainable operations, and inability to criti-

[79] Marcus, "Covid-19 Raises Questions About The Value of Personalized Medicine" (2020).

[80] Bayer and Galea, "Public Health in The Precision-Medicine Era" (2015).

cally judge innovations – all could contribute to a refusal to recognize failure. Then comes the bust.

Quantum technologies, because of their complexity and the secrecy surrounding their research and development, are well poised to fall victim to these dynamics. Consider the relatively recent failures among firms that have presented themselves as "technology companies" such as office-space-leasing firm WeWork and German payments company Wirecard AG. Sometimes investors give traditional companies a pass by placing them in special categories with less oversight, because the firm is seen as a "technology" company instead of an ordinary one that uses technology. This regulatory misclassification, with looser scrutiny because of "technology," appears to have helped Wirecard AG evade earlier detection.[81] Private companies also enjoy less transparency, and in some cases, loose norms that enable inventive accounting. Ordinary investors might be confused by these norms, because publicly traded companies have more defined benchmarks and different scrutiny from regulators.

Modern, privately traded "technology companies" can manipulate key benchmarks surrounding sales and use them to make it appear that they are much more promising than in reality. For instance, the recent craze over home-delivered "meal kits" and claims surrounding booming subscriber statistics omit the key problem that firms pay huge amounts of money to acquire new customers, most of whom cancel soon thereafter.[82] Or take the enthusiasm surrounding electric kick scooters. To the public, these companies appear to be enormously successful because scooters appeared on every corner, seemingly overnight. The technology press fanned the optimism, but a few outlets, such as *The Information*, reported on the underlying economics of scooter business models, which reveals them to be unsustainable.[83]

[81] Storbeck and Chazan, "Germany to Overhaul Accounting Regulation after Wirecard Collapse" (2020).

[82] "[M]eal kit subscription services are plagued with an incredibly high churn rate – 19 percent of US adults have tried a meal kit service, but of that 19 percent, only 38 percent are still subscribing." See PYMNTS, "The Meal Kits Crowding Problem" (2018). Transparency into these pathologies tends to come from third parties, such as payment companies, that have incentives to accurately report how people are using their accounts.

[83] These scooters cost about $500, on average only receive a few rides a day, these rides generate just a few dollars, and the scooters only last a few months. Vandalism, operator injuries, confiscation by authorities, and simple theft also create

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

Throughout history, publics have fallen victim to secretive, cult-like profitmaking claims. From Charles Ponzi's international postal stamp arbitrage scheme to Elizabeth Holmes' drop-of-blood-testing Theranos to Wirecard AG's illusory successes in payments, these schemes work because of the same elements currently present in technology generally – optimism, boosterism, secrecy, and a network of people invested who could make a fortune if the company succeeds in the short term. In-the-know insiders often cannot whistle-blow because companies pressure them with non-disparagement agreements and threats from lawyers (and sometimes even the government). When attacked, company loyalists defend the firm, and markets tend to ignore claims of impropriety until the charade plays itself out. Ponzi, Theranos, and Wirecard all had leaks pointing to the truth of their operations, but the promise of profit kept investors optimistic.[84] And such schemes are not restricted to the West, as the Russian company MMM demonstrated in the 1990s.

When the state is invested in the technology enterprise, the technology could itself become part of national identity. Consider the Soviet campaign of Lysenkoism. Lysenko proposed an alternative to Mendelian genetics that aligned with Marxist theory and was embraced by Stalin. For decades, Lysenko's view reigned in the Soviet Union, with adherents to mainstream genetic theory ejected from academia and some even executed.

If a nation bets big on quantum information science, will it be able to admit failure? Or is it more likely that big bets will come with a kind of psychological investment in the technology?

Many of the elements that obscured the dead-end truths about other technologies are present in quantum technologies, and the stakes are growing. Quantum technologies' complexity, the elite na-

losses overlooked by many. In October 2018, authorities removed over 60 scooters dumped in Oakland's Lake Merritt.

[84] Going back to Ponzi, he enjoyed a chorus of support from individuals who were indeed paid early in Ponzi's schemes and thus had made demonstrable gains from the fraud. It was difficult to counter these first investors' successes (Zuckoff, *Ponzi's Scheme: The True Story of a Financial Legend* (2005)). Theranos used elaborate efforts to hide shortcomings of the firm, ranging from Secret Service-like security and seclusion for Elizabeth Holmes to a high-powered law firm (Carreyrou, *Bad Blood: Secrets and Lies in a Silicon Valley Startup* (2018)). Wirecard AG hired a former special forces soldier and the former head of intelligence of Libya to investigate its critics in what it called operation "Palladium Phase 2" (Murph, "Wirecard Critics Targeted in London Spy Operation" (2019)).

ture of its scientists, secrecy mandates, incentives to maintain funding, incentives to appear innovative and profitable, and lack of third parties in a natural position to inspect and report on performance, all could combine to obscure the prospects of quantum technologies. Quantum information science itself could also become a form of nationalistic Lysenkoism, because the concepts of indeterminacy and entanglement provide endless fodder for philosophical exploration and even breathing room for strained religious doctrines, such as mind–body dualism.[85]

The failure scenario has different implications for quantum communications and sensing. In communications, many of the underlying technical achievements have been made to support deployment of commercial technologies. QKD-based hardware is commercially available today for militaries and companies interested in it. If quantum communications fails, it won't be because the technology doesn't work: it will be because the technology isn't needed, or because its use is limited due to network effects, or other market conditions, or prohibitions on its use that cause firms not to adopt the technology.

In sensing too, the failure scenario does not mean that quantum technology is a complete bust. Quantum sensors have worked for decades in the form of medical imaging devices, and sophisticated, well-heeled entities will continue to invest in them. For instance, the oil and gas industries, early patrons of the supercomputing industry, are already poised to take advantage of quantum sensing. Governments will continue to create demand for satellite-based sensing, and for sensing to counter electronic warfare capabilities as discussed in Chapter 2. They just might avoid using the word *quantum*.

This means that even in a quantum computing failure scenario, quantum sensing technologies would still likely create national winners and losers. From a military and intelligence perspective, quantum sensing, when paired with a satellite network, will give nations a different aperture. It will be difficult to hide heavy matériel from these nations, and low-observable stealth technologies will become more detectable.

Yet the public might be a loser in the failure scenario. The failure scenario will lack the virtuous cycle of competition, research,

[85]Deepak Chopra has written several books tying quantum physics to healing, and specifically the remission of cancer. Professor Chopra was awarded the *Ig* Nobel prize in 1998 "for his unique interpretation of quantum physics as it applies to life, liberty, and the pursuit of economic happiness."

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

and price reduction that gave rise to the personal computer. Instead, we are likely to see a much slower growth cycle of quantum sensors and communications – just as we saw with AI from the early 1990s through the mid 2010s. Cutting-edge industries will be willing to invest and experiment because the payoff could be high. But the advantages of quantum encryption and quantum sensing will more slowly diffuse to other players. Industries that depend deeply on sensing, such as healthcare, will be willing to invest in quantum sensors. But without a virtuous cycle, these sensors will never enter the consumer marketplace and will only remain in reach of businesses.

Other losers include big-ticket government investments. The billions spent on quantum technologies and artificial intelligence – priorities voiced in the Trump administration budgets – come at a cost to the budgets of the National Institutes of Health and the National Science Foundation. As such, the quantum science and artificial intelligence priorities displace the priorities that would have been identified by expert program officers at those agencies. The commandeering of such a large amount of money also assumes that American research universities and companies have the capacity to perform so much research in quantum information science. As paylines at agencies become more constrained, principal investigators will be tempted to jam "quantum" into their proposals to support their ordinary work.

Governments and companies are pouring billions into quantum technologies. Where does a quantum failure scenario leave the people and institutions who have invested their money and careers into quantum technologies? Alas, the outlook for these people will remain bright even in the failure scenario. The skills and training required, and the multidisciplinarity of the quantum technology enterprise will be adaptable to other fields.

8.6 Conclusion

Exploring technology scenarios helps us envision how governments, companies, and people will use quantum technologies. Governments will prefer to be both technologically superior and dominant in quantum technologies, and use this advantage to supplement military power. But we are no longer living in the Cold War military/industrial research era. The private sector competes with governments in development, and there is good reason to believe that the private sector could build a quantum computer before or soon after a government does. Unlike stealth jets and bombs, development in quan-

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

tum technologies is likely to have many potential buyers and many unforeseen uses, much like the modern personal computer. Private companies seeking economic return will broadly democratize access to quantum computing services. Yet we must also contemplate the possibility that it is simply too soon for the quantum age, that investments won't pay off in the near term but possibly decades in the future.

In this chapter we have presented four visions of the future: three that imagine different ways that successful quantum information technologies might be employed by nations and corporations, and a fourth in which quantum sensing and communications are widely used but quantum computing is a bust. These scenarios painted many problematic futures that are brought about by or accelerated by quantum technologies. The next chapter turns to policy options to advance the good while mitigating the negative effects of this innovation.

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press

https://doi.org/10.1017/9781108883719.013 Published online by Cambridge University Press