2021 13th International Conference on Cyber Conflict
Going Viral
T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.)
2021 © NATO CCDCOE Publications, Tallinn

Quantum Communication for Post-Pandemic Cybersecurity

Martin C. Libicki
Distinguished Visiting Professor
Center for Cyber Security Studies
U.S. Naval Academy
Annapolis, MD, United States
libicki@usna.edu

David Gompert
Special Advisor
Ultratech Capital Partners
United States
Davidgompert@yahoo.com

Abstract: Current approaches to cybersecurity will become increasingly inadequate as the use of networks grows and hacking becomes more skilled. One response to this problem lies in quantum technologies. In particular, the extreme sensitivity of quantum communication makes interference readily detectable and can provide secure encryption-key distribution. However, this is likely to benefit primarily high-value networks that use encryption, leaving insecure the growing use of mass networks for distributed work. The options to approaching this conundrum are (1) to accept where quantum technology leads, (2) to accelerate the technology in general without regard to how it is used, or (3) to push the technology to include mass use. We recommend a public-private strategy for the United States and its allies to effect both high-end and mass use.[1]

Keywords: *quantum communication, technology policy*

1. INTRODUCTION

As use of the Internet and other data networks has grown, reliable, economic, and durable cybersecurity has proven elusive. While huge funding is shoveled into cybersecurity, the incidence, severity, and costs of cybercrime are escalating. The insecurity is especially acute for people, societies, and nations that rely on free politics, markets, and speech—that is, the United States and its allies—under threat from two main adversaries, Russia and China. Recent disclosures of Russian intrusion

1 The authors would especially like to acknowledge Professor Nathalie de Leon of the Princeton Quantum Initiative, Princeton University, whose input on quantum science has been invaluable. Errors in this paper are, of course, ours.

into important U.S. government systems reveal that cybersecurity, despite expanding investment, has not kept pace with increasingly sophisticated hacking.

Meanwhile, the growth in network use in order to enable distributed work will persist after the pandemic. Because cybercrime increases at about the same rate as network use, and home computers are becoming substitutes for more secure workplace ones, cybersecurity will become even more challenging and expensive, yet ever more vital.

One way to help close the yawning gap between cyber vulnerability and security may lie in quantum technologies. Although practical quantum *computing* is at least a decade away, the dawn of quantum *communication* is here. The sensitivity of quantum transmissions allows hostile interference to be revealed and thereby ensures the safe passage of messages, notably those involved in encryption-key distribution. This raises the prospect of a hack-resistant "Quantum Internet," initially instantiated as secure quantum links within today's digital Internet. A Quantum Internet would not require replacing most of the Internet's infrastructure, and the cost would mostly be borne by those willing to pay for genuine cybersecurity, albeit with a focused government role.

Below, we explain the need for a public-private strategy involving U.S.-allied collaboration to guide investment, overcome technical hurdles, secure high-value networks, and extend the benefits of quantum communication to general public use.

A. Taking Stock

In a nutshell, the use of networks is accelerating; the volume and sophistication of hacking is increasing at the same rate, if not faster; return on investment in cybersecurity is generally discouraging; and the damage can be expected to grow, especially as Russia and China become more aggressive.

Remote work, prompted by the pandemic, has been both efficient and popular with employees and employers alike. If, say, half the growth in remote work due to the pandemic were to remain after the pandemic ends, network use could be up about around 25% from pre-pandemic levels (over and above baseline growth). Adding to the shift of jobs from office to home is the replacement of on-site meetings with off-site ones.

This trend is occurring not only in everyday networks but also in sensitive ones. Valuable intellectual property, such as chip designs, drug formulas, and patent applications, may be exchanged online. A great deal of unclassified but critical government business will be done remotely. The National Security Agency (NSA)

warns that the dispersal of U.S. government work to home offices presents "countless opportunities" for hacking, especially by Russian agents.[2]

Cyberattacks are escalating in proportion to network use.[3] The FBI reports that complaints about cybercrime have increased by 300% during the pandemic, and one cannot be sanguine about post-pandemic cybersecurity.[4] Investment in cybersecurity has been rising fast, from $3 billion in 2004 to $124 billion[5] in 2019, and shows no signs of slowing down.[6] Yet worldwide costs of cybercrime and cyberconflict have been rising at an even faster rate than Internet use has; by one estimate, $600 billion a year is being lost.[7] Though there are always particular successes, the macroeconomics of cybersecurity are generally unpromising.

Whether in time spent, lines of code written, people employed, or funds expended, the effort and expense required to protect, detect, patch, work around, and recover from attack far exceed those of hacking. At its higher levels, investment in cybersecurity shows sharply diminished returns.[8] Firms typically experience a flattening of the curve that relates cybersecurity achieved to cybersecurity investment.[9]

This has been so because the Internet was designed as an open utility to afford access to information, facilitate sharing, and enable collaboration. Open networks tend to have increasing as opposed to decreasing returns on investment, as adding participants benefits those already participating—an economic phenomenon favoring open networks that has propelled the digital revolution.[10] Yet protecting user-friendly systems tends to be harder than invading them, all else being equal. Conversely, the more restrictive networks are for the sake of security—access control lists come to mind—the less useful they may be for users.

2 Lily Hay Newman, "The NSA Warns That Russia Is Attacking Remote Work Platforms," *Wired*, December 7, 2020, https://www.wired.com/story/nsa-warns-russia-attacking-vmware-remote-work-platforms/.

3 Accenture, *Ninth Annual Cost of Cybercrime Study*, 2019, https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.

4 Catalin Cimpanu, "FBI Says Cybercrime Reports Quadrupled during COVID-19 Pandemic," ZD Net, April 18, 2020, https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-covid-19-pandemic/.

5 Gartner, "Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020," Gartner Newsroom, June 17, 2020, https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem.

6 "We anticipate 12–15 percent year-over-year cybersecurity market growth through 2021, compared to the 8–10 percent projected by several industry analysts." Steve Morgan, "Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017–2021," *Cybercrime Magazine*, June 10, 2019, https://cybersecurityventures.com/cybersecurity-market-report/.

7 James Lewis, *Economic Impact of Cybercrime: No Slowing Down*, McAfee-CSIS report, February 2018, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.

8 "A New Kind of Insanity: The Risk of Diminishing Returns in Cybersecurity," Lumen, March 28, 2018, https://blog.lumen.com/a-new-kind-of-insanity-the-risk-of-diminishing-returns-in-cybersecurity/.

9 L.A. Gordon and M.P. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security* 5, no. 4 (November 2002): 438–457.

10 See W. Brian Arthur, "Increasing Returns and the New World of Business," *Harvard Business Review* (July–August, 1996), 101–109.

It is only prudent to anticipate that returns from investing in contemporary cybersecurity will not keep pace with changing threats as they become increasingly sophisticated and gain more opportunities to wreak mischief.

Cyber threats themselves range from lone-wolf cybercriminals to great-power rivals waging cyberwar. Although cybercrime is increasingly harmful, few if any cybercriminals have the means to compromise the encryption of communications. But great powers do.

Russia, although weak in many of the costlier sorts of power, such as conventional military forces, can launch devastating cyberattacks and views Western democracies as prime targets. Meanwhile, its relatively modest reliance on networked data makes it hard to deter by the threat of retaliation-in-kind. Recent disclosures about Russian penetration of important U.S. government networks have shattered faith in U.S. cybersecurity and shown that the ingenuity of Russian offensive operatives surpasses that of U.S. defenders. The ability of Moscow's hackers to smuggle malicious code undetected into U.S. government agencies via system updates of SolarWinds software indicates a dismal return on the more than $19 billion (FY2020) the federal government has invested annually on cybersecurity.[11] Clearly, Russian hackers are besting U.S. cybersecurity.

China, for its part, is developing advanced information technology in order to compete with the United States economically, as well as to challenge it militarily in the vital Indo-Pacific region. Quantum computing, if practical, could offer intelligence advantages to the side that can use it to break many of today's encryption keys within a reasonable time. China might thus parlay a lead in quantum technologies into superiority in cybersecurity. Both China and the United States are quite vulnerable to cyberattack by virtue of their economic dependence on data networks. Consequently, a tacit mutual deterrence is in place.[12] But will this hold if China achieves superiority in offensive *and* defensive capabilities in cyberspace as a result of its technological investments? The Chinese state and its associated technology companies are treating quantum technology as a particularly high priority among them. Even as Google and IBM race to produce useful quantum machines, China's Alibaba and Huawei are doing the same.

China is also putatively ahead of the United States in quantum communication.[13] The Chinese have demonstrated the feasibility of unbreachable quantum links through the

11 "Proposed Federal Spending by the U.S. Government on Cyber Security for Selected Government Agencies from FY 2020 to FY 2021", Statista, February 2020, https://www.statista.com/statistics/737504/us-fed-gov-it-cyber-security-fy-budget/.

12 See David C. Gompert and Phillip C. Saunders, *The Paradox of Power* (Washington, DC: NDU Press, 2011).

13 See David C. Gompert, "Spin-On: How the U.S. Can Meet China's Technological Challenge," *Survival* 62 (2020).

vacuum of space, over short distances in the air,[14] and at increasing distances via very clean fiber-optic lines.

In crafting cybersecurity strategy, it helps to distinguish applications that need high-end security from the mass of users that will only pay for general security. Highly sophisticated threats, such as those from the Russians and Chinese, target critical and well-protected networks, such as those supporting national security, other sensitive government functions, critical infrastructure, key sectors, and vital financial systems. Such attacks can, if successful, have grave effects. At the same time, an increasingly large volume of cybercrime by non-state hackers may undermine use of and faith in less-protected Internet-based commercial and public networks, albeit with less significant case-by-case effects.

At present, only foreign cyberpowers are both able and motivated to attack well-protected networks of importance to U.S. and allied national security. By contrast, common hackers are both constrained and inclined to target less-protected mass-use networks. It must be noted that high-end cybersecurity relies much more on encryption standing up to attack than does mass cybersecurity, where the presence of encryption suffices to send hackers looking elsewhere for weaknesses, notably by hijacking users' computers and then reading traffic from the inside.

B. The Role of Quantum Communication

Adequate cybersecurity could become more expensive yet still be found wanting—unless new options are developed.

Quantum physics offers one such option to make keeping secrets easier. Encryption, which is how secrets are kept, comes in two types: symmetric and asymmetric. Symmetric encryption uses the same key to encrypt and decrypt; it does so very efficiently, but it requires that key to be shared—and in that process, the key is vulnerable to being intercepted. This can be a problem if one party to a conversation can only be reached through an insecure channel. Asymmetric encryption uses one key to encrypt and another one to decrypt. Because the decryption key never leaves home, it is secure, provided that the decryption key (the "private" key) cannot be inferred from the encryption key (the "public" key). Once asymmetric encryption is used to pass the keys for symmetric encryption, the latter can be used to protect communications.

That said, quantum technology can cut both ways in respect to cybersecurity: whereas *quantum communication* could bolster cybersecurity, *quantum computing* could worsen it. In the words of a leading cybersecurity analyst, attacks on cryptography

14 Juan Yin et al., "Entanglement-Based Secure Quantum Cryptography over 1,120 Kilometres," *Nature*, June 15, 2020, https://www.nature.com/articles/s41586-020-2401-y.

systems "always get better; they never get worse."[15] This will be especially true when quantum computing becomes available. Since 1994[16] it has been known that a quantum computer could factor prime numbers in polynomial time, rather than the prohibitive exponential time currently required.[17] The difficulty of factoring numbers into primes is the current basis for believing that asymmetric encryption is secure. If someone discovers how to make factoring simpler, encryption-key security can be compromised. Against this threat, the cryptographic community is developing quantum-resistant algorithms (such as lattice-based cryptography and super-singular isogeny Diffie-Hellman key exchange), but one of the dangers of relying on these is that the security of such systems has yet to be proven. While no such quantum-computing threats are known to endanger symmetric encryption, the latter still has to solve the problem of exchanging keys securely.

This is where quantum communication comes in, specifically for quantum-key distribution (QKD). Thanks to a key feature of quantum physics, particle entanglement, it is possible to *prove* that a message was not intercepted. Martin Giles notes: "The beauty of qubits from a cybersecurity perspective is that if a hacker tries to observe qubits in transit, their super-fragile state causes them to collapse into 1 or 0 digital bits."[18] QKD, in turn, would have two parties use quantum encryption to exchange symmetric encryption keys. If the exchange was tapped, the parties would instantly know and try again. If it was untapped, the parties could use the keys with confidence.

Although prototype QKD systems have been engineered, the bandwidth along all these channels is low: though this is not a problem for exchanging keys or short, highly classified messages, it is a problem for broadband applications. Another challenge is that distances of practical quantum communication (for QKD) are limited to tens of kilometers. Repeating delicate qubits is much harder than repeating digital bits. Although scientists have shown that quantum repeaters are theoretically possible and have developed the various steps that comprise them, they have not yet produced a working prototype.[19] China has performed long-range line-of-site transmission through

15 Bruce Schneier, "New Attack on AES," *Schneier on Security*, August 18, 2011, https://www.schneier.com/blog/archives/2011/08/new_attack_on_a_1.html.

16 P.W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134 (IEEE Computer Society Press, 1994).

17 Researchers have made impressive progress at developing quantum computing since 1994. That said, they have yet to develop a practical instantiation of a computer that can efficiently crack prime numbers (exchange with author, May 2020). And researchers at the Princeton Quantum Initiative believe that codebreaking with quantum computing will not be feasible anytime soon (exchange with author, May 2020).

18 Martin Giles, "Explainer: What is Quantum Communication," *MIT Technology Review*, February 14, 2019, https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/.

19 According to a member of the Princeton Quantum Initiative: "All of the steps involved [in qubit repeating] have been demonstrated experimentally at a proof-of-concept level: people have demonstrated spin-photon entanglement, two-photon interference, remote entanglement distribution, quantum teleportation, and entanglement distillation. They just have not demonstrated a platform that is capable of break-even repeater networks to get to long distances. This is sort of analogous to current quantum computers—people have demonstrated quantum error correction, but only barely break-even, and not in a way that scales to large systems" (exchange with author, November 2020).

space via its Micius quantum-communication satellite,[20] but the practical applications are unclear. The United States has yet to deploy a quantum-communication satellite. The Chinese are also working on drones as quantum-communication nodes, but their ranges are too short to be of much utility.[21]

Granted, quantum communication alone will not guarantee cybersecurity. As a "system-of-systems" problem, cybersecurity requires a vast variety of tasks be done right: e.g., determining authorized users; authenticating their identity; protecting the integrity of applications and data; preventing unauthorized altering of hardware and software; and protecting the inviolability of channels. When hackers defeat these measures, organizations must detect their presence, ascertain and contain their effects, and patch holes that let them enter. They may have to develop plans to work around and recover from attacks. Even if communication links are protected by quantum communication, digital platforms could still be insecure. Other vulnerabilities include poor access control; ill-advised protocols; malware-laden computers, clients, servers or routers; and vulnerable supply chains.

Nevertheless, quantum communication can be a game-changer, at a minimum for safeguarding encryption. Thus the key question is how to proceed strategically.

2. STRATEGIC OPTIONS FOR A QUANTUM INTERNET

The expansion of remote work and associated network use is also occurring in more critical endeavors, such as government and proprietary corporate business. Such remote work challenges cybersecurity at the mass end of the spectrum. Yet the quantum communication technologies under current development are geared to problems at the high end where the quality of encryption is crucial: these require specialized hardware, which remains expensive because of the intricate engineering required to keep error rates for qubits low enough to allow reliably readable results.

This creates a dilemma: the problem of cybersecurity is growing for mass applications, but quantum technology, at least for now, offers relief mainly at the high end. This presents a conundrum: whether, how, and how fast to steer quantum communication development to address both high and mass segments of the Internet. At its core, this is about how markets and governments affect the progress of technology. Markets pull technology, and governments push it.

20 See, for instance, Karen Kwon, "China Reaches New Milestone in Space-Based Quantum Communications: The Nation's Micius Satellite Successfully Established an Ultrasecure Link between Two Ground Stations Separated by More Than 1,000 Kilometers," June 25, 2020, *Scientific American*, https://www.scientificamerican.com/article/china-reaches-new-milestone-in-space-based-quantum-communications/.

21 Anil Ananthaswamy, "The Quantum Internet Is Emerging, One Experiment at a Time," *Scientific American*, June 19, 2019, https://www.scientificamerican.com/article/the-quantum-internet-is-emerging-one-experiment-at-a-time/.

Consider three ways to approach this conundrum:

- Accept that quantum communication technology cannot serve the mass market.
- Push the technology in general but let it find its own markets.
- Encourage the technology to address the mass market.

Below, we take each in turn.

A. Accept That the Technology Cannot Serve the Mass Market

Not every technology benefits a mass user base, and not every technology that benefits high-end users has only high-end potential. Sixty-four years after Sputnik, for instance, rocketry is still the province of countries, corporations, and a few rich individuals (e.g., Elon Musk and SpaceX, Jeff Bezos and Blue Origin, Richard Branson and Virgin Galactic). Yet the orbits that rockets have opened up for use have brought accurate weather forecasting, the Global Positioning System (GPS), and satellite television to the masses.

By contrast, digital technology went down-market towards mass use almost from its inception. In the 1980s, the emergence of fiber optics and personal computers resulted in a mass shift toward distributed processing and broadband data networking. The most important markets for this integration of computing and telecommunications were large decentralized corporations and growing numbers of individuals. Although government funding provided some impetus, it was the ballooning revenues from civilian demand that provided the fuel for research and development that gave life to the digital revolution. Government clients, even the military and intelligence community, lagged at first but eventually climbed aboard, resulting in specialized sensitive networks. Cybersecurity, unfortunately, was an afterthought.

Quantum communication could follow a very different path: because its principal benefit is to bolster encryption, the most obvious application is to secure sensitive domains from sophisticated foreign-power threats. True, countering high-end threats can benefit everyone: we all rely on national security, financial, and critical infrastructure systems. But QKD is not needed for the security of mass networks.

Conversely, even if QKD moves "down-market," it is unclear whether an advance in encryption technologies can improve cybersecurity all that much (even as the reverse is true: advances in decryption generally harm cybersecurity). Two wise cybersecurity experts, Ross Anderson and Bruce Schneier, began their careers in cryptography with a belief that better cryptography was needed to improve cybersecurity. Both concluded that while good cryptography mattered,[22] better cybersecurity was more

22 Even after reaching that conclusion, Bruce Schneier co-designed Blowfish, a symmetric encryption algorithm that was the runner-up in National Institute for Standards and Technology's competition to develop a new symmetric key encryption standard. See Bruce Schneier, "The Blowfish Encryption Algorithm," *Schneier on Security*, accessed April 8, 2021, https://www.schneier.com/academic/blowfish/.

likely to emerge from a much broader understanding of security *per se* and a thorough adjustment in the incentives that decision-makers face when weighing cybersecurity decisions.[23]

Indeed, what kind of relief can technological development in general provide to cybersecurity? Start with the premise that all cybersecurity faults originate in human behavior. True as that may be, the primary implications—whether that cyber insecurity is deeply rooted in human nature and is hence ineradicable, or that cybersecurity is primarily sought through improving human behavior—do not necessarily follow. The most cost-effective path forward in such cases may involve not improving humans but establishing systems that prevent or mitigate the consequences of bad human decisions (or user interfaces that check potentially harmful but reflexive acts). Almost all automobile accidents, for instance, stem from human error. Yet between 1966 and 2014, in the United States, the number of fatalities per vehicle mile traveled fell by a factor of five (from 55 to 11 per billion miles traveled).[24] Are U.S. drivers five times better today (apart from declines in drunken and adolescent driving)? Or is the reduction more a result of better cars (seat belts, air bags, warning systems, frame integrity), better roads (freeways), and more efficient emergency medical services?

Similarly, even if better *user* choices help, the choices made by systems administrators and their bosses may help even more. And better technologies should not be confused with better techniques. Both technology and technique involve know-how. We think of technology as explicit, with universal properties that are globally applicable rather than the solution of a problem that varies by circumstance; it is thus capable of being transferred. Techniques belong to those who have mastered them and are thus far harder to transfer. There is very little "once-and-for-all" in the field of cybersecurity. Measures beget countermeasures, which beget counter-countermeasures, and so on. By contrast, quantum entails the mastery of new physical principles.

Artificial intelligence (AI) has been touted as a technology that can both improve and harm cybersecurity. Results from the Defense Advanced Research Projects Agency (DARPA) Grand Challenge program indicate that AI can spot software vulnerabilities better than humans can.[25] But that cuts both ways. AI can help vendors build more secure software. But AI can also help state-sponsored actors find some software or network vulnerability first. It is unclear whether accelerating the rate by which both

23 See, for instance, Ross Anderson, "Why Cryptosystems Fail," paper presented at the Association for Computing Machinery Conference on Computer and Communications Security (Fairfax, VA, November 1993), https://www.cl.cam.ac.uk/~rja14/Papers/wcf.pdf.

24 Wikipedia, "Motor Vehicle Fatality Rate in U.S. by Year," last modified April 5, 2021, https://en.wikipedia.org/wiki/Motor_vehicle_fatality_rate_in_U.S._by_year. See also the detailed statistics from United States Department of Transportation, "Recent NCSA Publications," accessed April 8, 2021, https://crashstats.nhtsa.dot.gov/.

25 See, for instance, David Brumley, "Mayhem, the Machine That Finds Software Vulnerabilities, Then Patches Them," *IEEE Spectrum*, January 29, 2019, https://spectrum.ieee.org/computing/software/mayhem-the-machine-that-finds-software-vulnerabilities-then-patches-them.

sides discover vulnerabilities will improve cybersecurity.[26] To the extent, however, that AI means machine learning, *and* that machine learning is used to spot network anomalies indicative of an intrusion, there are grounds for believing that AI will improve cybersecurity; if nothing else, it should improve configuration and patch management. But if hacking works by playing against expectation—and especially if hackers have access to AI that they can practice against to improve their ability to work undetected beneath some noise level—there may simply not be reliable corpora of abnormal network behavior to work with.

Furthermore, if a consequence of pursuing a technology is to hasten its adoption by others—as has been the case with digital technologies—second thoughts about the wisdom of doing so may be in order. The most important "other" is China, which, as noted, has actively pursued quantum communication, motivated by a belief in the power of U.S. intelligence agencies to ferret out secrets. But China no longer depends on U.S. technology to bootstrap such efforts, and so a U.S. failure to pursue such a technology would offer no help vis-à-vis China.

Many threat actors, however, cannot finance quantum communication advances or even exploit them at current prices. If further advances in quantum communication become useful, though, then U.S. efforts to thwart hackers by hacking them (e.g., "persistent engagement") might be that much harder. This is an example of what has been labeled the "cybersecurity dilemma."[27] However, an opposing argument can also be made. Hackers are a group that, once burned, might become wise to such efforts and therefore able to resist[28] without the help of quantum communication to mask their doings. Those hackers with less sophistication or resources may not be able or willing to take advantage of even tomorrow's quantum communication. Thus its advent would have little effect on their vulnerability to the various tools of "persistent engagement." Similar conclusions may apply more broadly. Although groups such as drug cartels also have an interest in encrypted communications, commercial technologies carefully implemented (e.g., Signal, Telegram) may suffice, because they are trying to evade national police agencies, not national intelligence agencies. Quantum communication, at this point, is more suited to network architectures with

26 This touches on a long-running debate over whether vulnerabilities are common (in which case, such an acceleration would not make much difference) or sparse (in which case, it would). Ross Anderson ("Security in Open versus Closed Systems: The Dance of Boltzmann, Coase, and Moore," Open Source Software: Economics, Law and Policy, IDEI Presentation, Toulouse, France, June 20–21, 2002. https://www.helpnetsecurity.com/2002/07/09/security-in-open-versus-closed-systems-the-dance-of-boltzmann-coase-and-moore/) thinks that neither attackers nor defenders gain a definitive advantage from open source software. However, empirical work by Andrew Ozment and Stuart E. Schechter ("Milk or Wine: Does Software Security Improve with Age?" Report, Usenix, 2006. http://www.usenix.org/legacy/event/sec06/tech/full_papers/ozment/ozment.pdf) suggests that depletion is possible, and hence, AI would correlate with greater cybersecurity.

27 See Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (Oxford: Oxford University Press, 2017).

28 This is not to say that "persistent engagement" is worthless. Forcing threat hackers to build a more robust attack infrastructure or cover their tracks more carefully detracts from their overall efforts.

few (albeit long-haul) nodes rather those with many nodes, because nodes themselves create opportunities for interception.

B. Let the Technology Find Its Own Markets

The history of technology is rife with instances in which a new capability initially seems irrelevant to the problems of everyday individuals but then—as it becomes more reliable, easier to use, and, especially, cheaper—becomes widespread and benefits almost everyone directly. Automobiles underwent such a shift in the United States from the late 1890s to the early 1920s. Computers did so from the 1950s-era mainframe that only a few organizations could afford to own (and, as importantly, service) to the early 1980s-era personal computers. Conversely, the benefits of many important technologies, notably aviation, filtered down to the masses only through their uptake by organizations (e.g., airlines). And the link between technologies that support national security and those that benefit the population at large is highly indirect.

Will quantum technologies filter to the masses directly, or will their benefits be realized only by and through those who can afford it, such as governments and banks? It is hard to be optimistic that quantum computation and communication will take the direction their predecessors did. A disproportionate share of the technological advances over the last 50 years has come from the ability to manipulate matter at an increasingly small scale. The march of semiconductor performance (known as Moore's Law) has resulted in large part from the constant shrinkage of integrated circuit size from 10 microns (circa 1970) to .007 microns (circa 2021). Sequencing a human genome, which cost roughly $100 million in 2000, now costs under $1000.[29] Similar advances have affected nanomaterial structures. By contrast, technological progress in the preceding 50 years (1920–1970) resulted from the ability to scale up processes so that products once manufactured in factories sized to fill regional needs were now supplied by factories scaled to global markets.

Quantum technologies arise from advances in working at ever-more-precise process control; they are very sensitive to environmental conditions. Progress requires erasing or compensating for all sources of extraneous noise (i.e., unwanted signal). It is a technology which, in spirit, is similar to those which enable precision ballistics.[30] These are not the sorts of technologies that allow rapid advances in scale—at least not in comparison to when a single process (e.g., photolithography) achieves great economics by producing an ever-larger number of products per unit (e.g., transistors per square inch of wafer).

29 National Human Genome Research Institute, "The Cost of Sequencing a Human Genome," National Human Genome Research Institute website, https://www.genome.gov/about-genomics/fact-sheets/Sequencing-Human-Genome-cost.

30 See Donald MacKenzie, *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance* (Cambridge, MA: MIT Press, 1990).

Ironically, insofar as miniaturization has now put cheap microprocessors not only in computers but in computer peripherals and internetted devices (e.g., light bulbs), it has complicated security. There are now many more places for malware to hide.

C. Push Quantum Communication Down-Market

The last option—deliberately encouraging the progression of quantum technology down-market—would reflect the judgment that government support and inducements work and that otherwise cybersecurity for mass use would not be helped. But two questions immediately arise: where would the technology be pushed, and how?

Although quantum communication can improve cybersecurity against the threat of interception, the interception at issue comes from tapping links rather than nodes (such as client machines and routers). Links come in two main types: wired and wireless. Wireline tapping requires operating some device at or very close to the line. The physical proximity and surreptitiousness required for wireline tapping makes it the province of governments and hence of limited usefulness to hackers of everyday users. Although tapping trunk lines can be and is done, the use of quantum channels for trunk lines would greatly exceed the bandwidth currently available to quantum communication (even if it suffices for QKD).

But wireless tapping is easier, since the distance between the tap and the channel need only be comparable to that between two nodes. It does not require a state apparatus to pull it off; infecting devices that the user already has could suffice (even if exfiltrating data undetected takes additional work). With more and more devices capable of being networked via Bluetooth, Wi-Fi, or perhaps 5G, avoiding such interception may become an increasing component of cybersecurity for the home, office, or factory.

Therein lies a dilemma. Internet-of-things (IoT) devices tend to be insecure because they often transmit in the clear. They abjure encryption because generating the processor cycles needed for encryption and decryption can be burdensome for cheap low-power processors. Meanwhile, quantum devices are sizeable and must be highly sensitive to the ambient environment to work reliably. Of course, so were early computers, as those who remember carefully filtered air-conditioned computer rooms will understand. Computers did not evolve to serve personal needs until integrated circuits were developed. If—and this is a huge if—there were ways to reduce quantum communication's read/write capabilities to integrated circuit form, it may be possible to embed quantum communication into any and all radio-frequency (RF) processing chips. As a bonus, because such devices could detect the presence of interception, they could also be used as high-fidelity sensors for listening devices. But none of this will happen soon.

In the meantime, there are other ways to push quantum technology toward mass cybersecurity. They include introducing it into cloud computing, particularly in server-to-server communication, and perhaps developing quantum-as-a-service. But quantum communication must first be proven cost-effective on its own terms before having additional demands thrust on its technological development.

3. RECOMMENDATIONS

Of these strategic alternatives, the authors lean toward the third, which would call for a public-private approach to make the technology robust and push it down-market. This would direct its benefits to those whom we expect to stay online even after the Covid-19 pandemic winds down. At the same time, the economic means to exploit quantum communication for the sake of mass cybersecurity must come mainly from markets themselves: in research and development, to advance the technology, notably to overcome the distance and bandwidth problems; in capital, to augment the existing Internet with quantum links; and in revenue-generating demand, for better security from eager users of every sort. If quantum communication is sufficiently promising, market-demand signals should augment government initiatives to introduce and spread this technology's use and value.

We recommend this strategy for several reasons. Even if highly sensitive links are made more secure, the increased cyber vulnerability of mass networks is, broadly conceived, a national security problem that cannot be ignored lest economic losses mount while information leaks voluminously. Citizens will lose confidence in their access to trustworthy information, in their government's ability to safeguard it, and in the reliability of elections and health of democracy itself.

To implement this public-private strategy, we recommend several specific steps:

- The U.S. government (notably the Department of Energy, the Department of Homeland Security, and the Department of Defense), allied governments, leading information-technology companies, and major universities should jointly commit to developing and deploying quantum communication.
- Concerted, yet still competitive, efforts should be made to overcome range and bandwidth obstacles. A combination of government-funded and corporate research and development investment is needed. Similarly, concerted engineering efforts should be made on cost reduction, especially if the technology can be driven towards a chip-level orientation.
- High priority should be given to domains of direct importance to national security.

- High priority should also be given to the protection of intellectual property rights, coupled with widespread licensing.
- U.S.-allied partnerships should be promoted; European quantum work (e.g., at Delft University) is world-class, as is reflected in current partnerships. Indeed, one of the better venues for such collaboration would be NATO, which already includes cybersecurity among its missions.

Although governments cannot insist that private technology companies team with others who may compete with them, it can galvanize teaming. With its proven capacity for facilitating cooperation in sensitive defense and intelligence affairs, NATO (with arrangements to include Japan and certain other partners) is a natural place to start.

REFERENCES

Accenture. *Ninth Annual Cost of Cybercrime Study*. 2019. https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.

Ananthaswamy, Anil. "The Quantum Internet Is Emerging, One Experiment at a Time." *Scientific American*. June 19, 2019. https://www.scientificamerican.com/article/the-quantum-internet-is-emerging-one-experiment-at-a-time/.

Anderson, Ross. "Security in Open versus Closed Systems: The Dance of Boltzmann, Coase, and Moore." Open Source Software: Economics, Law and Policy, IDEI Presentation, Toulouse, France, June 20–21, 2002. https://www.helpnetsecurity.com/2002/07/09/security-in-open-versus-closed-systems-the-dance-of-boltzmann-coase-and-moore/.

Anderson, Ross. "Why Cryptosystems Fail." Paper presented at the Association for Computing Machinery Conference on Computer and Communications Security, Fairfax, VA, November 1993. https://www.cl.cam.ac.uk/~rja14/Papers/wcf.pdf.

Arthur, W. Brian. "Increasing Returns and the New World of Business." *Harvard Business Review* (July–August 1996): 101–109.

Beech, Mark. "COVID-19 Pushes up Internet Use 70% and Streaming More Than 12%, First Figures Reveal." *Forbes*. March 25, 2020. https://www.forbes.com/sites/markbeech/2020/03/25/covid-19-pushes-up-internet-use-70-streaming-more-than-12-first-figures-reveal/.

Brumley, David. "Mayhem, the Machine That Finds Software Vulnerabilities, Then Patches Them." *IEEE Spectrum*. January 29, 2019. https://spectrum.ieee.org/computing/software/mayhem-the-machine-that-finds-software-vulnerabilities-then-patches-them.

Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford: Oxford University Press, 2017.

Cimpanu, Catalin. "FBI Says Cybercrime Reports Quadrupled during COVID-19 Pandemic." *ZD Net*. April 18, 2020. https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-covid-19-pandemic/.

Cohen, Jason. "Data Usage Has Increased 47 Percent During COVID-19 Quarantine." *PCMag*. June 5, 2020. https://www.pcmag.com/news/data-usage-has-increased-47-percent-during-covid-19-quarantine.

Gartner. “Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020.” Gartner Newsroom, June 17, 2020. https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem.

Gerwitz, David. “COVID Cybercrime: 10 Disturbing Statistics to Keep You Awake Tonight.” *ZDNet*. September 14, 2020. https://www.zdnet.com/article/ten-disturbing-coronavirus-related-cybercrime-statistics-to-keep-you-awake-tonight/.

Giles, Martin. “Explainer: What is Quantum Communication.” *MIT Technology Review*. February 14, 2019. https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/.

Gompert, David C. “Spin-On: How the US Can Meet China’s Technological Challenge.” *Survival* 62, no. 3 (2020): 115–130. DOI: 10.1080/00396338.2020.1763617.

Gompert, David C., and Phillip C. Saunders. *The Paradox of Power*. Washington, DC: NDU Press, 2011.

Gordon, L.A., and M.P. Loeb. “The Economics of Information Security Investment.” *ACM Transactions on Information and System Security* 5, no. 4 (November 2002): 438–457.

Grossman Group. “Nearly Half of Employees Now Working from Home Want to Stay Remote, Study Finds.” PR Newswire. May 14, 2020. https://www.prnewswire.com/news-releases/nearly-half-of-employees-now-working-from-home-want-to-stay-remote-study-finds-301059220.html.

Kwon, Karen, “China Reaches New Milestone in Space-Based Quantum Communications: The Nation’s Micius Satellite Successfully Established an Ultrasecure Link between Two Ground Stations Separated by More Than 1,000 Kilometers,” *Scientific American*, June 25, 2020; https://www.scientificamerican.com/article/china-reaches-new-milestone-in-space-based-quantum-communications/.

Lewis, James. *Economic Impact of Cybercrime: No Slowing Down*. McAfee-CSIS report. February 2018. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.

Lumen. “A New Kind of Insanity: The Risk of Diminishing Returns in Cybersecurity.” Lumen website. March 28, 2018. https://blog.lumen.com/a-new-kind-of-insanity-the-risk-of-diminishing-returns-in-cybersecurity/.

MacKenzie, Donald. *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance*. Cambridge, MA: MIT Press, 1990.

Morgan, Steve. “Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017–2021.” *Cybercrime Magazine*. June 10, 2019. https://cybersecurityventures.com/cybersecurity-market-report/.

National Human Genome Research Institute. “The Cost of Sequencing a Human Genome.” National Human Genome Research Institute website. https://www.genome.gov/about-genomics/fact-sheets/Sequencing-Human-Genome-cost.

Newman, Lily Hay. “The NSA Warns That Russia Is Attacking Remote Work Platforms.” *Wired*. December 7, 2020. https://www.wired.com/story/nsa-warns-russia-attacking-vmware-remote-work-platforms/.

Ozment, Andrew, and Stuart E. Schechter. “Milk or Wine: Does Software Security Improve with Age?” Report, Usenix. 2006. http://www.usenix.org/legacy/event/sec06/tech/full_papers/ozment/ozment.pdf.

Reuters. “Edited Transcript of BLK.N Earnings Conference Call or Presentation 13-Oct-20 12:30pm GMT.” Yahoo Lifestyle. October 13, 2020. https://www.yahoo.com/lifestyle/edited-transcript-blk-n-earnings-123000634.html.

Schneider, Troy. “Nearly 50% of Pentagon Workers Still Teleworking.” *FCW (Federal Computer Week)*. September 17, 2020. https://fcw.com/articles/2020/09/17/pentagon-telework-fifty-percent.aspx.

Schneier, Bruce. “New Attack on AES.” *Schneier on Security*. August 18, 2011. https://www.schneier.com/blog/archives/2011/08/new_attack_on_a_1.html.

Schneier, Bruce. “The Blowfish Encryption Algorithm.” *Schneier on Security*. Accessed April 8, 2021. https://www.schneier.com/academic/blowfish/.

Shor, P.W. “Algorithms for Quantum Computation: Discrete Logarithms and Factoring.” In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134. IEEE Computer Society Press, 1994.

Statista. “Proposed Federal Spending by the U.S. Government on Cyber Security for Selected Government Agencies from FY 2020 to FY 2021.” February 2020. https://www.statista.com/statistics/737504/us-fed-gov-it-cyber-security-fy-budget/.

United States Department of Transportation. “Recent NCSA Publications.” Accessed April 8, 2021. https://crashstats.nhtsa.dot.gov/.

U.S. Patent and Trademark Office, Patent Public Advisory Committee. *Annual Report 2020*. October 30, 2020. https://www.uspto.gov/sites/default/files/documents/PPAC_2020_Annual_Report.pdf.

Vogels, Emily, Andrew Perrin, Lee Rainie, and Monica Anderson. “53% of Americans Say the Internet Has Been Essential during the COVID-19 Outbreak: Americans with Lower Incomes Are Particularly Likely to Have Concerns Related to the Digital Divide and the Digital ‘Homework Gap.’” Pew Research Center. April 30, 2020. https://www.pewresearch.org/internet/2020/04/30/53-of-americans-say-the-internet-has-been-essential-during-the-covid-19-outbreak/.

Yin, Juan, et al. “Entanglement-Based Secure Quantum Cryptography over 1,120 Kilometres.” *Nature*. June 15, 2020. https://www.nature.com/articles/s41586-020-2401-y.

Wikipedia. “Motor Vehicle Fatality Rate in U.S. by Year.” Last modified April 5, 2021. https://en.wikipedia.org/wiki/Motor_vehicle_fatality_rate_in_U.S._by_year.