STRATEGIC STUDIES QUARTERLY - PERSPECTIVE

Surviving the Quantum Cryptocalypse

Jon R. Lindsay

Abstract

The quantum threat to cybersecurity is an example of a self-denying prophesy: the more credible the threat narrative, the more concerted the effort to counter it. Quantum computing poses a security threat because digital encryption currently depends on the computational difficulty of certain mathematical problems such as factoring large numbers that would be exponentially easier to solve with a quantum computer. Although experimental machines are not yet powerful enough to undermine public encryption, they do demonstrate that quantum computers are able, under some circumstances, to outperform the fastest classical supercomputers. Indeed, the quantum threat is so credible that the scientific community has been working on cryptographic countermeasures that will soon be certified for public use. Research is also well underway on new quantum networks that can enhance cryptographic security. The size of the quantum window of vulnerability depends on relative rates of engineering progress in quantum computing and quantum-safe alternatives, as well as political considerations about how long secrets need to be protected. There are reasons to be cautiously optimistic that countermeasures are maturing faster than the threat. Nevertheless, the quantum threat should be taken seriously, which is precisely why it might never materialize.*

*****

The security of almost every digital application on classified and unclassified networks relies on a small number of cryptographic protocols. The security of key protocols such as Rivest-Shamir-Adleman (RSA) relies on the computational intractability of certain mathematical problems, such as factoring large numbers. Quantum computers might be able to solve these problems exponentially faster. Quantum information science is a fast-developing field at the intersection of

*I am grateful to Ben Garfinkel, David Meyer, and several anonymous reviewers for comments on the technical portions of this paper. Any mistakes are my responsibility.

quantum physics and computer science. It uses counterintuitive concepts from quantum physics that make it possible to perform calculations that are impossible for even the fastest classical supercomputers. In principle, a large-scale, fully functional, universal quantum computer could factor very large numbers in a matter of hours.

The maturation of quantum computing would thus pose a categorical threat to the confidentiality, integrity, and availability of the entire cyber domain.[1] An intelligence adversary with the right kind of machine could potentially break RSA, decrypt classified data, and forge digital signatures. All networks and applications on those networks, public and private, using vulnerable cryptography would be put at risk. Because military operations in all physical environments—land, sea, air, space—rely on many of the same information technologies and networks that power the global economy, a systematic vulnerability in the cyber domain would become a systematic vulnerability in all domains. Classified information could be collected, altered, or deleted. Personal, financial, legal, logistic, and operational data could be manipulated to influence tactical and strategic operations. Malware could be installed at will to enable espionage or disrupt critical infrastructure. Disinformation could be disseminated from the secure accounts of senior officials, heightening the credibility of foreign deception efforts. The authentication codes protecting sensitive equipment and weapons stockpiles could be falsified, facilitating illicit proliferation. Given the ubiquitous importance of cyberspace, the systematic compromise of cybersecurity would be a strategic problem of the first order.

The threat of a spooky quantum vulnerability is easy to exaggerate, which makes it tempting to downplay the threat.[2] Indeed, history is littered with expectations of technological transformation that never came to pass.[3] Threats in theory are often limited by challenges in practice, so the realization of the quantum threat will likely depend on institutional capacity as much as scientific potential.[4] Nevertheless, the quantum threat cannot be dismissed out of hand since the scientific state of the art is advancing rapidly.[5] Recent breakthroughs in the lab have demonstrated that it is possible for experimental quantum machines to perform some calculations faster than classical supercomputers, even as the ability to break RSA is still a long way off. The window of vulnerability to quantum computing has not yet opened, but it is increasingly plausible that it could open in the future. Indeed, it is precisely because scientific progress in quantum computing has made the threat so credible that the cryptographic community has redoubled efforts to field countermeasures.

Prophesies that are both believable and undesirable tend to become self-denying. The more that progress in quantum computing portends a "cryptocalypse," the more likely that scientists and policy makers will take steps to keep this from happening.[6] Cryptographers have already identified alternatives to RSA that rely on different mathematical problems believed to be intractable for both classical and quantum computers. The US National Institute of Standards and Technology (NIST) is currently evaluating, and will soon certify, new standards that can be incorporated into cyber systems. Furthermore, quantum mechanics can also be leveraged to create totally new types of secure data networks. Operational prototypes exist in China, Europe, and North America. Chinese scientific progress in quantum information science has been especially motivating for the US government, and both China and the US have dramatically increased their investment in this area in recent years. One implication of this investment is the liklihood that "quantum safe" offsets will be available and implemented long before anyone is able to field a threatening quantum computer.

In this article I explain why the quantum threat may be a self-denying prophesy. First, I provide a quick overview of the quantum threat to public encryption. Next, I discuss the potential impact of quantum computing on the balance between cyber offense and defense. Third, I review progress in the development of countermeasures to the quantum threat, then offer three scenarios based on different assumptions about engineering progress in quantum technology. Finally, I conclude with some cautious optimism about the prospects for quantum defense over offense.

The Quantum Threat to Public Encryption

The quantum threat emerges at the nexus of cybersecurity, cryptology, and quantum computing. The security of cyberspace depends on the computational difficulty of certain mathematical functions, which turn out to be vulnerable to certain quantum algorithms. The threat of quantum cryptanalysis (code breaking) has also inspired the development of various forms of quantum-safe cryptography (code making) such as classical post-quantum cryptography (PQC) and quantum key distribution (QKD).[7] Table 1 parses out these different technologies. This section focuses on the offensive (cryptanalytic) threat posed by quantum computing, while the defensive (cryptographic) remedies of PQC and QKD are discussed in a later section.

Table 1. Classical and quantum information technologies compared

Cryptologic applications	Classical information technology	Quantum information technology
General applications that rely on cryptography for security	Intelligence, communication, administration, command and control, automation, governance, diplomacy, law enforcement, science, engineering, manufacturing, finance, commerce, advertising, entertainment	Scientific modeling and simulation, quantum sensing and measurement, data storage and search, machine learning and artificial intelligence
Classical cryptography vulnerable to quantum cryptanalysis	Rivest-Shamir-Adleman (RSA) Diffie-Helman (DH) Elliptic Curve Cryptography (ECC) Advanced Encryption Standard (AES) Secure Hash Algorithm (SHA)	Shor's algorithm provides an exponential speedup vs. RSA, DH, and ECC. Grover's algorithm provides a polynomial speedup vs. AES and SHA.
Quantum-safe cryptography	Post-Quantum Cryptography (PQC)	Quantum Key Distribution (QKD)

Pundits often assert that quantum computing is "equivalent to opening a combination lock by trying every possible number and sequence simultaneously" or that it can easily solve hard problems like "the traveling salesman problem."[8] Such descriptions are either wrong or extremely misleading. Quantum computing leverages the counterintuitive phenomena of quantum physics to solve mathematical problems. Whereas a digital bit must be one *or* zero, a quantum bit (qubit) can be a "superposition" of one *and* zero. Multiple qubits can be "entangled" to represent more information than can be represented with separate qubits. It is important to appreciate that quantum computers offer performance improvements only for mathematical problems for which a suitable quantum algorithm has been discovered. Furthermore, physical implementations of quantum computers must be able to run quantum algorithms at scale (i.e., with thousands or millions of qubits) while detecting and correcting errors. Difficult outstanding engineering challenges abound. The online appendix summarizes a few key technical concepts to explain how quantum computing works in principle and why it is difficult to implement in practice.[9]

In principle, quantum computing imperils the security of popular cryptographic protocols like RSA. RSA is an example of an asymmetric protocol, which uses different keys for encryption and decryption.[10] Asymmetric encryption, invented independently by British intelligence and American academics in the 1970s, is invaluable for secure internet communication.[11] It is distinguished from symmetric encryption, which uses the same key for both operations; prominent examples include the famous Enigma machine and modern block ciphers like Advanced Encryption Standard (AES). Distributing the same key throughout a large dispersed organization has always presented a serious security challenge; for example, the Allies were able to break into Enigma networks when they captured German ships carrying common key material.[12] In asymmetric encryption, by contrast, the so-called public key can be openly revealed to allow other people to send encrypted messages that only the recipient can decrypt by using a secret private key. The private key can also be used to create digital signatures that anyone can verify with the public key.

A critical requirement of asymmetric encryption is that it must be extremely difficult to guess the private key from the public key. Modern RSA works because the public key is based on a very large number (i.e., two to the power of 2048) while the private key is based on its prime factors. With ordinary classical computers, it is easy to multiply two large prime numbers together, but it is exponentially harder to factor the result. A typical desktop computer would need more than six quadrillion years to crack 2048-bit RSA.[13] However, in 1994 Peter Shor discovered a quantum algorithm that can theoretically factor prime numbers (and calculate discrete logarithms) exponentially faster than the fastest known classical methods.[14] If one assumes the existence of a powerful quantum computer, therefore, Shor's algorithm could in principle enable successful cryptanalytic attacks in a matter of hours, an astounding improvement compared to the countless lifetimes required by the fastest classical supercomputers today.[15]

RSA is widely used in implementing public key infrastructure (PKI), which links real-world individuals and organizations to cryptographic keys to facilitate secure communication and digital authentication.[16] Military PKI systems, for example, employ a common access card (CAC) with an embedded chip that stores the keys enabling an authorized user to log on to classified and unclassified networks. PKI underwrites the security of military communications, financial transactions, and intellectual property and the privacy of civil society around the world. Digital signatures produced with RSA certify the authenticity of digital messages and facilitate the installation of software from trusted vendors. Breaking RSA would make it possible to decrypt secure data and install arbitrary code on protected networks.

RSA is not the only protocol that matters in modern cryptosystems. Quantum computing provides only a modest advantage against symmetric ciphers like AES or Secure Hash Algorithms (SHA) using other methods such as Grover's algorithm. Unfortunately, PKI necessarily relies on asymmetric ciphers like RSA, Diffie-Helman (DH), and Elliptic Curve Cryptography (ECC), all of which can be defeated with Shor's algorithm.[17] RSA is the linchpin of most modern implementations of PKI, and there are no quick fixes short of replacing vulnerable asymmetric protocols with something else. The development of a functional quantum computer able to break RSA, and thereby compromise PKI, would imperil the privacy and authenticity of the entire cyber domain.

Shor's algorithm has been known since 1994, but for many years it seemed like little more than a theoretical curiosity. For all practical purposes, it appeared infeasible to build an actual quantum machine powerful enough to run Shor's algorithm with reliable error correction. Completely eliminating all PKI dependence on vulnerable protocols, moreover, would have required a massive update of government and private sector cryptosystems, or the construction of an entirely new quantum communications infrastructure based on immature technology. These would have been major undertakings, to say the least. The theoretical threat posed by Shor's algorithm thus did not seem like a practical urgency.

This perception changed in the 2010s as academic and corporate labs demonstrated working prototypes. A solid-state machine in 2012 was able to "run a three-qubit compiled version of Shor's algorithm to factor the number 15, and successfully find the prime factors 48% of the time."[18] Since then, quantum computers have factored numbers much larger than 15, but still nothing as large as a 2048-bit RSA key. The most dramatic experimental breakthrough to date occurred in September 2019, when a 53-qubit machine known as Sycamore achieved a milestone known as "quantum supremacy." Sycamore, built by Google and physicists at the University of California, Santa Barbara, ran a quantum algorithm faster than could be simulated by the world's fastest classical supercomputer (the IBM Summit at the Oak Ridge National Laboratory).[19]

To crack RSA with the most efficient known method, a quantum computer must be able to keep 20 million qubits in coherence (i.e., maintaining superposition and entanglement without losing quantum information) for several hours, which is what is required.[20] There is still a long way to go before this will be possible. Prototype machines have been able to maintain fewer than 100 qubits in coherence for short amounts of time. In 2017, IBM maintained 50 qubits in coherence for 90 microseconds.[21] In 2019, Google's Sycamore maintained 53 qubits in coherence for three minutes, a dramatic improvement to be sure but a long way from cracking RSA. Sycamore might be likened to the Wright Flyer: a gross contraption compared to what might come later, yet nonetheless a harbinger of a new technological era.[22] The many unknowns and major engineering challenges ahead make it difficult to hazard a guess about whether a large-scale quantum computer remains 10 or 100 years away, but anything less seems overly optimistic.

The Offense-Defense Balance in Cyberspace

The ability to break RSA would in principle provide a capable intelligence adversary with a formidable offensive advantage. Yet quantum information science (in particular PQC or QKD) also has the potential to restore the advantage to defense, again in principle. If defensive offsets are not developed in time, however, a dangerous window of vulnerability to quantum attack could open. Windows are important in international relations because political actors are tempted to jump through them.[23] An actor with an uncontested capability to perform quantum cryptanalysis would be tempted to use it to gain intelligence advantages, which might then be parlayed into military or economic advantages.

The race between offensive measures and defensive countermeasures is as old as war itself. Offensive advantage, moreover, is never just an immutable characteristic of weapon systems. The offense- defense balance in any era depends on organizational and geostrategic context, not simply technology.[24] Yet scientific principles and engineering feasibility constrain the strategic and operational art of the possible.[25] Technical trends establish the boundary conditions for any potential window in which offense has the advantage. This window can and does change as actors take the initiative to build new weapons and find new ways to use them.

For example, between the world wars technological trends shaped the offensive potential of bombers and the defensive potential of radar. The Royal Air Force (RAF) worked out an air defense scheme after World War I that relied on acoustic mirrors along the Channel Coast able to detect an aircraft 10 or more miles away.[26] Yet as aircraft speeds increased, acoustic mirrors could no longer provide sufficient warning of incoming bombers in time to launch fighters to intercept them. Technological innovation made the "Channel gap" a pressing strategic problem for the RAF, which was not resolved until the emergence of radar a few years before World War II. Importantly, the exploitation of the technological potential for both strategic bombing and air defense required complementary organizational innovation, an area in which Britain performed well while Germany did not.[27] While offensive advantage can be fleeting, it can still be a very real and consequential factor for strategic competition in the window of time before defensive innovation prevails. The question is how long it takes for any given threat, or countermeasures to it, to become practically feasible.

Quantum computing has the potential to alter the offense-defense balance in cyberspace, but this is not a simple proposition. The cyber domain is often described as intrinsically offense dominant, but in fact the balance is mutable.[28] The hacker does not always get through, in part because cybersecurity has appreciably improved in recent years.[29] There are many reasons for this development, to include the emergence of a multibillion-dollar information security industry, the increased use of active network monitoring and counterintelligence methods such as threat hunting, and the rise of specialized government agencies focused on cybersecurity and military units such as US Cyber Command. These improvements do not imply that we can simply ignore serious cyber threats, however, as recent episodes like the 2016 Russian influence campaign and 2017 NotPetya attacks make clear. On the contrary, it is precisely because we *do* have to worry about serious cyber threats that we have become better at detecting and defending against them. If cyberspace is a contested domain, it is also contestable.[30] Offense does not categorically hold the advantage.[31]

The contest between offense and defense in cyberspace is dynamic and conducted at many levels. Hidden vulnerabilities and clandestine exploits are the coin of the realm for offensive cyber operations. Attackers have incentives to keep their exploits secret because revelation can prompt the defender to patch or reconfigure systems. Many vulnerabilities in software systems tend to be transitory because they can be quickly patched or mitigated once revealed, yet vulnerabilities at the hardware or protocol layers can take longer to remediate. It can take a while to develop and acquire viable substitutes, and even once available, network dependencies can raise the costs of testing and switching to the new components.[32]

Unlike with many cyber vulnerabilities, unfortunately, mere knowledge of the quantum threat to RSA is not enough to close it. Shor's algorithm has been known for a quarter century, as noted, but not yet mitigated. There is no simple patch available because entirely new cryptosystems are needed. The quantum threat is a striking instance of what cybersecurity professionals call a "class break," a vulnerability that categorically affects an entire class of technology versus just particular targets.[33] Shor's algorithm is about the biggest class break imaginable.

According to one prominent physicist, "If a quantum computer is ever built, much of conventional cryptography will fall apart."[34] As the general council of the National Security Agency (NSA) explains, "The strategic advantage here would be for one country to surreptitiously acquire such a capability and maintain it for perhaps several years or more. Other countries would not realize that everything from their weapons systems to financial transactions would be vulnerable during that period; and that would include not only current activity but also the historic, encrypted communications collected and retained by the winner in anticipation of this very capability."[35] The former president of a major research university argues that Chinese progress in quantum technology "presents the United States with its new 'Sputnik moment.'. . . Whoever gets this technology first will also be able to cripple traditional defenses and power grids and manipulate the global economy."[36]

Chinese developments thus provide a sense of urgency in these matters. China has named quantum informatics a key plank in its "13th Five-Year Plan" for technology and innovation, and it is building the world's largest quantum laboratory.[37] Even though China has historically struggled to catch up in science, in quantum information technology it has been the first to achieve several important milestones.[38] China launched the first satellite for quantum science, demonstrating the ability to leverage the entanglement of particles—described by Einstein as "spooky action at a distance"—from orbit, an unprecedented distance. China has also built a large-scale experimental quantum network between Beijing and Shanghai. China hopes not only to improve its general economic competitiveness by investing in quantum technology but also to shore up its perceived vulnerability to US cyber operations—highlighted by the Snowden leaks—by developing more secure quantum networks. Chinese strategists have started writing about "quantum hegemony," and the United States is taking note.[39]

It is important to appreciate that quantum networking is a related but distinct category of technology from quantum computing. Both technologies draw on quantum mechanics, but the similarities end there. China's recent achievements in satellite-enabled quantum experiments and its Beijing-Shanghai link are all in the realm of quantum communications rather than computation. Chinese progress in quantum computing has been less impressive, and here North America remains the leader. Quantum computing offers advantages to the offense (cryptanalysis) while quantum communications offers advantages to the defense (cryptography). However, these cryptologic advantages do not map directly onto military advantages. Cryptographic security (defense) is needed to cover plans and preparations for a military offensive, and cryptanalytic achievements (offense) can provide intelligence that helps to strengthen military defenses against surprise attack. Furthermore, both types of quantum technologies are systemic variables, whereas the offense-defense balance in any given case usually depends more on dyadic factors such as the organizational capacity of rivals.[40]

It is far from clear how well either China or the United States will be able to operationalize quantum technology, even as there are reasons to suspect that the US military and intelligence community may have important relative advantages in this respect.[41] What is clearer is that geopolitical competition has become a major catalyst for both countries to invest in quantum information science. Active political rivalry on the scientific frontier makes the cyber offense-defense balance more important, even as it tends to make it more ambiguous.

Defending against the Quantum Threat

Scientific breakthroughs can give rise to new threats to national security, and scientific research can also produce countermeasures to them.[42] Yet this counteraction does not happen by itself. To realize any effective countermeasure, actors must invest resources and political will. Actors may show little interest in preventative action when a threat is diffuse, far away, or hard to understand. Yet as time horizons shorten and threats begin to seem more palpable, the imperative for preventative action becomes more urgent.[43] The incentives to invest in applied scientific research will also tend to increase when a geopolitical rival invests in the same threatening technology. The quantum threat has long seemed diffuse and uncertain. Yet real achievements by a real competitor like China are helping to dramatize the urgency of the problem. Balancing in politics and balancing in science can become one and the same.[44]

Quantum-safe cryptography, as I use the term here, includes both PQC and QKD. These innovations are inspired, in part, by the threat posed by Shor's algorithm and experimental progress in quantum computers. If offsets can be fielded soon, the quantum threat window may not ever open in the first place.

PQC works by using mathematical problems difficult for both classical and quantum computers to solve (i.e., PQC is not vulnerable to Shor's algorithm). Candidate problems include finding the shortest vector in a lattice, decoding error-correction codes, and solving systems of multivariate equations over finite fields.[45] PQC runs on classical computers, providing security against classical and quantum attacks. Because quantum computers have very specialized applications, classical computers will almost certainly remain the best choice for many applications. Even quantum systems will still incorporate some classical components. Therefore, PQC will be needed to ensure the security of classical computers in the future.

In the United States, the NIST "has initiated a process to develop and standardize one or more additional public-key cryptographic algorithms . . . that are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers."[46] The NIST has received, and is evaluating, nearly 70 submissions from two dozen countries.[47] The NSA, meanwhile, has signaled that it "will initiate a transition to quantum resistant algorithms in the not too distant future," cautioning against adopting strong protocols like ECC and instead waiting for PQC.[48] While the NIST should approve PQC alternatives within the next few years, the full transition could still take a decade more. Previous transitions (e.g., to AES) took much longer than anticipated due to economic and organizational constraints. In the ideal case, new PQC protocols would simply be swapped in for current cryptographic primitives to minimize the need to reengineer all the other systems that depend on them. More likely, however, "PQC standardization . . . will need a new wineskin to hold the new wine."[49] So long as classical computing power continues to increase, the additional computational overhead of PQC will probably not pose a general barrier to implementation. However, the greater resource-intensiveness of PQC could pose a problem for more constrained and bandwidth-limited military applications (such as ship-to-shore networks). This problem might be mitigated by judiciously limiting the use of computationally intensive primitives within the overall cryptographic system, just as slower RSA is used to open a session conducted with faster AES today.

The alternative to PQC is QKD. Quantum mechanics can be leveraged to create new kinds of communication networks that use a totally different approach to cryptography. QKD exploits the Heisenberg Uncertainty Principle to detect the presence of an eavesdropper. Since the act of measuring quantum data can change them, an eavesdropper in the channel would increase detectable error rates. QKD thus makes it possible to securely distribute unique keys between geographically separated parties (which was the original justification for inventing asymmetric encryption like RSA).[50] The practical feasibility of QKD over large distances, including between satellites in orbit and ground stations, has been demonstrated in numerous experiments.[51] Research is underway to develop quantum routers and networks that can preserve entangled states while scaling up to greater numbers of users, higher bandwidths, and longer distances, along with reliable quantum repeater and memory devices that do not destroy quantum state.[52] These challenges are perhaps less formidable than those associated with general-purpose quantum computing, but they are still difficult. Yet there are also promising signs of progress.[53]

QKD is hardly a silver bullet. The same mechanism that prevents the eavesdropper from copying the data (i.e., the act of tapping the quantum circuit causes an increase in random errors) also enables the adversary to impose a service denial attack on the quantum channel. An attempt to copy data every time it is transmitted has the potential to force every connection to reset. QKD also does not protect data integrity against side channel attacks on the engineering implementation of the system or social engineering attacks on the gullibility of human operators. Elaborations such as "measurement-device-independent QKD" can close some loopholes, but they still assume that the preparation of photons for transmission will be unobserved and that communicators will also have an authenticated classical channel.[54] This does not preclude some types of man-in-the-middle attacks.

Any transition to quantum communication networks (with QKD) will also be difficult. Quantum networks rely on very different principles than does the installed base of classical digital networks around the world. If switching to PQC will be hard, QKD could be even harder. Adoption of PQC, insofar as security motivates consideration of quantum networking, will probably be more feasible for most organizations and states. As cryptographer Tom Berson wryly notes, QKD is a "new, difficult, expensive way to achieve an outcome which we have, for decades, been achieving easily and cheaply."[55] For most practical network applications, PQC to shore up classical networks will be available more quickly, feasibly, and reliably without attempting to transition to a wholly new quantum network architecture protected by QKD. Quantum networking may yet become attractive for novel applications other than cryptography that have no classical equivalent, such as certifying deletion or sharing out quantum computational resources.[56]

Assessing the Quantum Window of Vulnerability

It is difficult, even irresponsible, to make specific predictions about progress at the scientific frontier, but it is possible to gain some clarity about the relative bounds of the problem. In particular, it is possible to say something about the size of the technological window of vulnerability based on relative estimates about the maturation of offensive and defensive innovation. Nontechnical considerations also affect the size of the window. Foremost among these is the length of time that secrets need to be kept.

The latent value of secrecy will vary depending on the encrypted data's content and policy priorities. Some secrets are extremely perishable, such as the current location of mobile military assets in war or a negotiating position in a deal that will be concluded in the next few days. By contrast, weapon designs and other capabilities that require significant investment may need longer protection if revelation would enable an adversary to develop countermeasures. Politically sensitive covert action might be kept secret for a long time if revelation would be embarrassing to the government or allies or concerns activities of exceptionally long duration.[57] Intelligence sources and methods are particularly sensitive. Historical data can enable the adversary to better understand an adversary's doctrine or even identify long-running operations. For example, the US Army intercepted a batch of KGB communications about agent operations in the West in the 1940s and was able to decrypt some of them due to improper reuse of one-time pads by KGB agents.[58] The Army decrypted only a small fraction of these messages (known as the Venona files) before the Soviets discovered the compromise and switched to a different system. Nonetheless, the ongoing decryption and analysis of the Venona trove enabled the Allies to uncover the Cambridge Five spy ring (including Guy Burgess and Kim Philby) as well as operations against the Manhattan Project (including Julius and Ethel Rosenberg). Venona continued to illuminate KGB methods and facilitate Western counterintelligence throughout the Cold War.[59]

Figure 1 summarizes three different scenarios based on three successively longer estimates of the time it will take for an attacker to field a fully functional, large-scale quantum computer that can crack RSA.[60] The threat window is bounded on the attacker's side by the rapid development, slightly delayed development, or extremely delayed development of quantum computers, denoted by $t_{\text{qc-rapid}}$, $t_{\text{qc-delayed}}$, and $t_{\text{qc-extreme-delay}}$. These might be considered as 5, 20, or 50 years from now, respectively, but any specific estimates would be misleading. My focus here rather is on the relative size of the window. The window is bounded on the defender's side by the amount of time it will take the defense to transition to quantum-safe cryptosystems secured by PQC or QKD (denoted $t_{\text{q-safe}}$) and the amount of time that organizations want to keep their secrets from an adversary (up to t_{secret}). The point $t_{\text{q-safe}}$ is the earliest possible point that quantum-safe encryption is technically feasible, even as any organizational implementation will take some additional time. Whether or not a target can implement PQC or QKD properly is a critical factor in any given case, but my focus here is on technological boundary conditions.

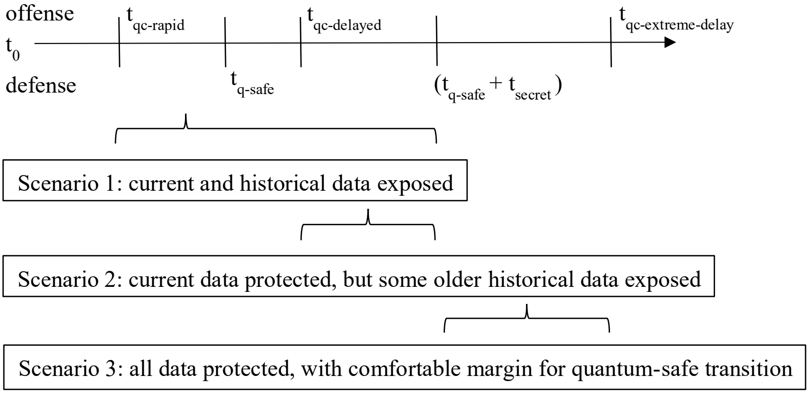
offense
t_0
defense
$t_{\text{qc-rapid}}$
$t_{\text{qc-delayed}}$
$t_{\text{qc-extreme-delay}}$
$t_{\text{q-safe}}$
$(t_{\text{q-safe}} + t_{\text{secret}})$
Scenario 1: current and historical data exposed
Scenario 2: current data protected, but some older historical data exposed
Scenario 3: all data protected, with comfortable margin for quantum-safe transition

Figure 1. Windows of vulnerability to quantum decryption

Scenario 1 ($t_{\text{qc-rapid}}$) is the best case for offense; scenario 3 ($t_{\text{qc-extreme-delay}}$) is the best case for defense; and scenario 2 ($t_{\text{qc-delayed}}$) is a mixed case. The first scenario assumes a breakthrough in quantum computing in the next few years, occurring either in public or in secret, that enables an intelligence agency to begin bulk decryption of data secured with contemporary PKI. No quantum-safe offsets are available at the time of this breakthrough (i.e., $t_{\text{q-rapid}} < t_{\text{q-safe}}$ for whatever reason). At that point, most financial transactions, military communications, private personal information, and other data will be exposed. It would still be necessary for the attacker to be able to access, assess, analyze, and disseminate sensitive data, which are all nontrivial organizational performances. If these (difficult) conditions are met, however, then the quantum-enabled attacker could read confidential data, forge digital signatures, and install arbitrary code. Even perishable, time-sensitive, current data would be exposed in the time between a quantum computing breakthrough and the introduction and adoption of viable quantum-safe cryptosystems (i.e., the interval from $t_{\text{q-rapid}}$ to $t_{\text{q-safe}}$). Access to time-sensitive data might even enable an adversary to manipulate markets or disrupt operations. Such an ability could provide intelligence and influence in the short term and erode trust in the global economy in the long term.

Scenario 1 is the worst case for the defender because the quantum computing breakthrough occurs prior to the implementation of quantum-safe cryptography. Even after quantum-safe cryptography is deployed at $t_{\text{q-safe}}$, any data encrypted and stored prior to that date, using old encryption protocols, will still be vulnerable. Any data encrypted prior to $t_{\text{q-safe}}$ in an unsafe protocol may retain some strategic or tactical value for as long as t_{secret} and will thus remain vulnerable to quantum decryption up until $t_{\text{q-safe}}$

+ t_{secret}. After that point, all historical secrets will have lost their intelligence value for understanding military operations or political policy.

In the other two scenarios, defensive innovators are first past the post, allowing current data to be protected from quantum decryption. These cases differ depending on whether any historical data is also exposed. The second-best (or second-worse) case for the defender is scenario 2, where a quantum computing breakthrough is delayed until just after quantum safe implementation (i.e., $t_{q\text{-}safe} < t_{qc\text{-}delayed)}$. Scenario 2 is problematic because some old data that were encrypted in the old format will become exposed after the quantum breakthrough, and these will still have some intelligence value to the adversary. All historical data encrypted and stored prior to $t_{q\text{-}safe}$ will become readable to the adversary in the interval from $t_{qc\text{-}delayed}$ to $t_{q\text{-}safe}$ + t_{secret}. A proactive intelligence adversary might even begin harvesting encrypted data before the quantum computing breakthrough in anticipation of decrypting them afterwards.

The best case for the defender is scenario 3, where a breakthrough is delayed until long after the quantum-safe transition. In this case, there is nothing valuable left to decrypt after $t_{qc\text{-}extreme\text{-}delay}$. If progress in quantum computing is so delayed, or quantum-safe offsets are available so soon, then no valuable data are exposed. Perhaps the engineering obstacles of entangling millions of fully functional coherent qubits will prove too formidable. For whatever reason, quantum-safe offsets are in place far in advance of the emergence of a powerful quantum computer. When that day finally comes, all data that retain any political or economic utility have long since been encrypted in quantum-safe formats. Any ancient data remaining on servers, still encrypted in unsafe formats, will have long since gone stale (i.e., $t_{q\text{-}safe} + t_{secret} < t_{qc\text{-}extreme\text{-}delay}$). The adversary will thus find no value even in decrypting the old data that it has stockpiled in anticipation of acquiring a quantum computer.

Scenario 3 provides a cushion for the transition to PQC or QKD that is missing in the other two scenarios. This margin (i.e., the interval between $t_{q\text{-}safe}$ + t_{secret} and $t_{qc\text{-}extreme\text{-}delay}$) is important because rolling out the PQC standards that are eventually certified by the NIST is sure to be a long and difficult process. The longer a quantum breakthrough is delayed, or the sooner the quantum-safe offset is available, the more time organizations will have to upgrade their cryptosystems. Those organizations that highly prioritize cybersecurity may be able to upgrade to PQC relatively quickly, once it is available. Many others will delay because of the difficulty of ensuring backward compatibility with their legacy installed base of software. If a quantum computer becomes available during the period of incomplete transition to PQC, then systems that do not use PQC, or data exchanged with systems that do not use it, will remain vulnerable. In effect this would amount to a localized reversion to scenarios 1 or 2 for some organizations, despite the global availability of PQC per scenario 3. Rather than a discrete point in time, $t_{q\text{-safe}}$ should really be thought of as a fuzzy band that will vary by organization and industry.

In the final analysis, I assess scenario 1 (early quantum computing breakthrough) to be *least* likely while scenario 3 (the triumph of quantum-safe defense) is far *more* likely. Scenario 2 (some historical data exposed to quantum cryptanalysis) deserves to be taken seriously, both because there might be a surprising breakthrough in the midrange and because the quantum-safe transition will be uneven.

How to Stop Worrying and Love the Cryptocalypse

The prospect of a devastating quantum threat to cybersecurity is an example of a self-denying prophesy. The magnitude and credibility of the threat inspires the search for countermeasures to mitigate it. The more convincing the doomsayer's prophesy, the harder its potential victims work to postpone catastrophe.[61] Quantum computing has the potential to create a dramatic "class break" in the computational infrastructure of modern military and economic power. This threat should be taken seriously thanks to recent engineering progress in quantum computing. Indeed, scientists and states are taking it *so* seriously that the most dangerous eventuality is unlikely to come to pass. The US government is taking the quantum threat—and opportunity—particularly seriously because China is betting big on quantum technology.

Self-denying prophesies are common in military history. British prime minister Stanley Baldwin famously said in 1932 that "the bomber will always get through." In 1940, of course, German bombers did not always get through. British fears of strategic bombing, heightened by the RAF's own rhetoric, encouraged the RAF in the interwar years to build the astonishingly successful air defense system that won the Battle of Britain. Likewise, in the eternal race between code makers and code breakers, the looming threat of quantum decryption is already encouraging innovation in quantum-safe encryption. This does not mean that future systems will provide perfect operational security, any more than the RAF's integrated air defense system could intercept every bomber. Baldwin would have been considerably less motivating, however, had he cautioned that the bomber only sometimes gets through, depending on a complex interaction of social and technical factors.

Predicting the interaction of scientific progress, international politics, and secret intelligence is especially difficult. Resolution of the many uncertainties and empirical speculations mentioned in this article will take further assessment of technical progress; and indeed, further technical progress. How much confidence can we have that the quantum threat window will not open? My estimates are informed by current trends, but a future breakthrough is always possible. A well-resourced intelligence agency like the NSA might develop a working quantum computer in secret before the completion of PQC implementation. Documents leaked by Edward Snowden suggest that the NSA has included funding for research into "a cryptologically useful quantum computer" as part of an $80 million research program on "Penetrating Hard Targets."[62] If the NSA were to succeed, is it realistic to believe that its quantum coup could be kept secret? In the 1940s, Bletchley Park secretly developed its Bombe and Colossus machines to break the Enigma and Lorenz cryptosystems, respectively. Britain kept its triumphs secret for decades in order to keep on exploiting Warsaw Pact countries using similar cryptosystems.[63] However, this feat is unlikely to be replicated in the age of quantum computing. The conditions of absolute operational security at Bletchley Park differ starkly from today's world of pervasive leaks and penetrating intelligence. Bletchley Park had a virtual monopoly on the computer scientists of its day (including the brilliant Alan Turing), but the locus of innovation in computer science has long since passed out of government hands. Major firms like Google and IBM are racing to be the first to develop quantum computers for lucrative commercial and scientific applications beyond the national security domain (such as drug discovery and scientific modeling), and there is a cottage industry of reporting on quantum progress in the technical trade press. There is so much investment pouring into commercial and academic quantum science that cryptographers will have plenty of warning well before the quantum threat becomes imminent, an eventuality that remains many years if not many decades away. According to quantum computing expert Scott Aaronson, "It seems improbable that the NSA could be that far ahead of the open world without anybody knowing it."[64]

The PQC transition, by contrast, is already underway and should be well advanced within the next decade. One might reasonably expect PQC to mature sooner and ultimately be more widely implemented than QKD, if only because PQC protocols are designed to be analogous with current cryptographic protocols. Quantum networking technology is perhaps more mature than quantum computing, but, nevertheless, the implementation problems in large-scale quantum communications are legion. It will likely be PQC rather than QKD—classical rather than quantum protocols—that will provide widespread protection against the threat of quantum cryptanalysis. The widespread implementation of PQC is going to be especially difficult for military systems with widespread dependencies on legacy cryptosystems (and RSA). A thorough survey of military systems will be crucial to ensuring that critical functions and data are prioritized for protection. This transition will inevitably have to be phased, with local upgrades installed and tested in less critical areas to gain confidence in the fixes. This process is sure to be long and complicated, but progress may be expedited if senior leadership gives cybersecurity the priority it deserves.

Quantum cryptanalysis may still be decades away, but some secrets might retain their value for many decades. There are likely things of interest about the early Cold War that remain hidden in the secret archives of intelligence agencies. Given the longevity of some secrets, there is no room for complacency about the quantum threat. Indeed, the entire argument here relies on practitioners *not* being complacent. It is the very plausibility and danger of the threat that mobilize scientific and institutional action. The prospect of quantum decryption sometime in the next few decades is sufficiently likely, and the risks of relying on vulnerable protocols like RSA for cryptographic security are sufficiently great, that effort to develop and implement quantum-safe networks should be a high priority.

Current US government interest in quantum information science is encouraging in this regard. As of this writing, the Trump administration's fiscal year 2021 budget request features generous funding for "industries of the future" like "artificial intelligence (AI), quantum information sciences (QIS), 5G/advanced communications, biotechnology, and advanced manufacturing." Even as the administration slights scientific research in other areas, including biosecurity, the budget includes "$210 million for the National Science Foundation (NSF) for QIS research, doubling the FY 2020 Budget for QIS," and "$237 million for DOE's [Department of Energy's] Office of Science to support QIS research. This will bolster quantum information efforts at the national laboratories and in academia and industry."[65] Nearly half a billion is earmarked for quantum technology, including $25 million to build a quantum internet connecting 17 national labs.[66] While Congress is unlikely to pass the 2021 budget intact, it is suggestive of the administration's priorities. Moreover, funding for quantum science is likely to be spared the squabbles that embroil more controversial budget items. Despite the extreme polarization in contemporary American politics, there is bipartisan support for increasing investment in quantum science. As the DOE under secretary for science points out, "The dollars we have put into quantum information science have increased by about fivefold over the last three years."[67] This funding is motivated in no small part by the concern that China could leapfrog ahead of the United States. Investment in quantum information technology has thus become an important component of what the 2018 National Defense Strategy describes as "the re-emergence of long-term, strategic competition between nations."[68]

If the prospect of quantum-safe security via QKD is not enough of a motivation for investing in quantum networking, there are other positive reasons to invest. Quantum networks may enable some applications that are simply infeasible with classical networks. These include encryption schemes allowing users to certify the deletion or retention of data, detect tampering, and create unique time windows for decryption.[69] Quantum computing also holds great promise for scientific modeling and drug discovery.

This article has only explored the technical bounds of the possible, but many other social factors affect the window of vulnerability. Organizational institutions, human behavior, industrial policy, and strategic interaction can squander technological advantages. They can also compensate for technological weaknesses. Even if quantum-safe networks are not available before quantum computers (scenario 1), protecting some secrets will still be possible. Target organizations will still find ways to hide their most valuable secrets by using physically isolated networks or abstaining from digital encoding altogether. Conversely, even in a world of secure quantum-safe networks (scenario 3), it will be still possible to collect secrets by attacking the insecure human endpoints of the network. Strong cryptography, classical or quantum, does not automatically translate into strong information security. Gullible humans, flawed security policy, and sociotechnical complexity can inadvertently expose data protected by quantum-safe systems.[70]

Endemic friction in the sociotechnical implementation of cryptology is something of an insurance policy for *both* offense and defense in any of the three scenarios. The actual performance of either quantum decryption or quantum-safe encryption is unlikely to live up to its full potential. Even if I am too pessimistic about the scientific prospects of quantum computing relative to quantum-safe alternatives, quantum computers will still have to operate in human organizations that offer little reason for optimism. The practical implication is clear. Organizations cannot rely solely upon technology for cryptologic advantage. Information assurance begins and ends with a workforce that understands and cares about the confidentiality, integrity, and availability of relevant data. More complex information technologies require an even higher level of technical acumen and awareness from personnel, and an even stronger commitment on the part of leadership to maintaining a robust cybersecurity posture. Offensive cyber advantage, conversely, depends on knowing how to exploit the behavior of organizations that fail to maintain their guard.

No technical advantage can be sustained forever, if indeed it can be realized in the first place. In the case of quantum computing, the credible fear that a geopolitical adversary might realize a major intelligence advantage has already mobilized considerable effort for prevention. It is important to sustain this effort. Quantum computing may yet have other important military applications, but we should make sure that an exponential improvement in cryptanalysis will not be one of them. The 2^n horsemen of the cryptocalypse should be just believable enough to make themselves irrelevant.

Jon R. Lindsay

Jon R. Lindsay is an assistant professor at the Munk School of Global Affairs and Public Policy and Department of Political Science at the University of Toronto. He served in the US Navy in the aviation, intelligence, and special warfare communities. He is the author of *Information Technology and Military Power* (Cornell, 2020) and volumes on deterrence (Oxford, 2019) and cybersecurity (Oxford, 2015).

Notes

[1] John Mulholland, Michele Mosca, and Johannes Braun, "The Day the Cryptography Dies," *IEEE Security & Privacy* 15, no. 4 (July/August 2017): 14–21, DOI: 10.1109/MSP.2017.3151325.

[2] Frank L. Smith, "Quantum Technology Hype and National Security," *Security Dialogue*, April 2020, https://doi.org/10.1177/0967010620904922.

[3] Lawrence Freedman, *The Future of War: A History* (New York: PublicAffairs, 2017).

[4] Jon R. Lindsay, "Demystifying the Quantum Threat: Infrastructure, Implementation, and Intelligence Advantage," *Security Studies* 29, no. 2 (2020): 335–61, DOI: 10.1080/09636412.2020.1722853.

[5] For a thorough technical assessment, see National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects* (Washington, DC: The National Academies Press, 2019), https://doi.org/10.17226/25196.

[6] Victoria Craw, "Quantum Computing Set to Revolutionise Everything from National Security to Drug Design and Financial Investments," *News.Com.Au*, 29 January 2018, http://www.news.com.au/technology/. See also "Risk Analysis of Quantum Computer Attacks on Digital Signatures," accessed 21 April 2020, https://www.quantumcryptopocalypse.com/.

[7] There are other interesting applications of quantum information science that are beyond the scope of this article, ranging from new types of remote sensing to improvements in scientific modeling and machine learning. For a survey of potential applications, see Michael J. Biercuk and Richard Fontaine, "The Leap into Quantum Technology: A

Primer for National Security Professionals," *War on the Rocks* (blog), 17 November 2017, https://warontherocks.com/; and National Academies of Sciences, Engineering, and Medicine, *Quantum Computing*.

8. Vivek Wadhwa, "Quantum Computers May Be More of an Imminent Threat than AI," *Washington Post*, 5 February 2018, https://www.washingtonpost.com/.

9. The appendix for this article is available online at https://www.airuniversity.af.edu/.

10. R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications ACM* 21, no. 2 (February 1978): 120–26, https://dl.acm.org/doi/10.1145/359340.359342.

11. Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (New York: Random House, 1999), 243–92.

12. David Kahn, *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1933–1945*, rev. ed. (Annapolis, MD: Naval Institute Press, 2012), 149–60, 255–66.

13. DigiCert, "Check Our Numbers: The Math behind Estimations to Break a 2048-bit Certificate," accessed 17 May 2019, https://web.archive.org/.

14. Peter W. Shor, "Algorithms for Quantum Computation: Discrete Logarithims and Factoring," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (Los Alamitos, CA: IEEE Computer Society, 1994), 124–34, http://citeseerx.ist.psu.edu/.

15. Craig Gidney and Martin Ekera, "How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits," arXiv, 6 December 2019, https://arxiv.org/.

16. See Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, *Cryptography Engineering: Design Principles and Practical Applications* (Indianapolis, IN: John Wiley & Sons, 2010).

17. M. Roetteler and K. M. Svore, "Quantum Computing: Codebreaking and Beyond," *IEEE Security and Privacy* 16, no. 5 (September 2018): 22–36, DOI: 10.1109/MSP.2018.3761710.

18. Erik Lucero et al., "Computing Prime Factors with a Josephson Phase Qubit Quantum Processor," *Nature Physics* 8, no. 10 (October 2012): 719–23, https://www.nature.com/.

19. Frank Arute et al., "Quantum Supremacy Using a Programmable Superconducting Processor," *Nature* 574, no. 7779 (October 2019): 505–10, https://doi.org/10.1038/nphys2385.

20. Gidney and Ekera, "How to Factor 2048 Bit RSA Integers."

21. Samuel K. Moore, "IBM Edges Closer to Quantum Supremacy with 50-Qubit Processor," *IEEE Spectrum: Technology, Engineering, and Science News*, 15 November 2017, https://spectrum.ieee.org/tech-talk/; and Martin Giles and Will Knight, "Google Thinks It's Close to 'Quantum Supremacy.' Here's What That Really Means," MIT *Technology Review*, 9 March 2018, https://www.technologyreview.com/.

22. Scott Aaronson, "Why Google's Quantum Supremacy Milestone Matters," *New York Times*, 30 October 2019, https://www.nytimes.com/.

23. Marc Trachtenberg, "A 'Wasting Asset': American Strategy and the Shifting Nuclear Balance, 1949–1954," *International Security* 13, no. 3 (1988): 5–49, DOI: 10.2307/2538735; and Stephen Van Evera, *Causes of War: Power and the Roots of Conflict* (Ithaca: Cornell University Press, 1999), chap. 4.

24. Charles L. Glaser and Chaim Kaufmann, "What Is the Offense-Defense Balance and Can We Measure It?," *International Security* 22, no. 4 (Spring 1998): 44–82, https://

web.stanford.edu/; and Stephen Biddle, "Rebuilding the Foundations of Offense-Defense Theory," *The Journal of Politics* 63, no. 3 (2001): 741–74, https://www.jstor.org/.

25. For example, orbital physics constrains the employment of antisatellite weapons today as much as in the Cold War despite tremendous advances in spacecraft. Thus, a technical primer over three decades old remains relevant: Ashton B. Carter, "Satellites and Anti-Satellites: The Limits of the Possible," *International Security* 10, no. 4 (Spring 1986): 46–98, https://www.jstor.org/.

26. John Ferris, "Fighter Defence before Fighter Command: The Rise of Strategic Air Defence in Great Britain, 1917–1934," *Journal of Military History* 63, no. 4 (1999): 845–84, https://www.jstor.org/.

27. David Zimmerman, *Britain's Shield: Radar and the Defeat of the Luftwaffe* (Stroud, UK: Sutton Publishing, 2001).

28. Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316–48, http://dx.doi.org/10.1080/09636412.2015.1038188; and Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41, no. 3 (2017): 72–109.

29. Richard A. Clarke and Robert K. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats* (New York: Penguin, 2019).

30. According to the 2018 *Command Vision for US Cyber Command*, "Cyberspace is an active and contested operational space in which superiority is always at risk." United States Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command* (Ft. Meade, MD: USCYBERCOM, June 2018), 6, https://www.cybercom.mil/.

31. Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly* 13, no. 3 (2019): 122–45; and Max Smeets, "The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly* 12, no. 3 (2018): 90–113, https://www.airuniversity.af.edu/.

32. Max Smeets, "A Matter of Time: On the Transitory Nature of Cyberweapons," *Journal of Strategic Studies* 41, no. 1–2 (2017): 6–32, https://doi.org/10.1080/01402390.2017.1288107.

33. Bruce Schneier, "Class Breaks," *Schneier on Security* (blog), 3 January 2017, https://www.schneier.com/.

34. Gilles Brassard quoted in Hoi-Kwong Lo and Norbert Lütkenhaus, "Quantum Cryptography: From Theory to Practice," *Physics in Canada* 63, no. 4 (2007): 191–96, https://arxiv.org/.

35. Glenn S. Gerstell, "I Work for N.S.A. We Cannot Afford to Lose the Digital Revolution," Opinion, *New York Times*, 10 September 2019, https://www.nytimes.com/.

36. C. L. Max Nikias, "This Is the Most Important Tech Contest since the Space Race, and America Is Losing," *Washington Post*, 11 May 2018, https://www.washingtonpost.com/.

37. Central Committee of the Communist Party of China, "The 13th Five-Year Plan for Economic and Social Development of the People's Republic of China (2016–2020)," December 2016, https://en.ndrc.gov.cn/; and Eamon Barrett, "Google and NASA Have Claimed Quantum Supremacy, but China Is Not Far Behind the U.S.," *Fortune*, 30 October 2019, https://fortune.com/2019/.

[38] Dan Breznitz and Michael Murphree, *Run of the Red Queen: Government, Innovation, Globalization, and Economic Growth in China* (New Haven, CT: Yale University Press, 2011).

[39] Elsa B. Kania and John Costello, *Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership* (Washington, DC: Center for a New American Security, 2018), https://www.cnas.org/; and Taylor Owen and Robert Gorwa, "Quantum Leap: China's Satellite and the New Arms Race," *Foreign Affairs*, 7 September 2016, https://www.foreignaffairs.com/.

[40] Biddle, "Rebuilding the Foundations of Offense-Defense Theory."

[41] Greg Austin, *Cybersecurity in China: The Next Wave* (Zurich: Springer, 2018).

[42] Robert L. Paarlberg, "Knowledge as Power: Science, Military Dominance, and U.S. Security," *International Security* 29, no. 1 (2004): 122–51, https://www.jstor.org/.

[43] David M. Edelstein, *Over the Horizon: Time, Uncertainty, and the Rise of Great Powers* (Ithaca, NY: Cornell University Press, 2017).

[44] Scholars in the realist tradition of international relations generally expect political actors to balance against threats. A classic statement is found in Kenneth N. Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley, 1979). Another version of balancing theory argues that threatening intentions must be present to provoke balancing, not just threatening capability; see Stephen M. Walt, *The Origins of Alliance* (Ithaca, NY: Cornell University Press, 1990). Some counter that intentions are so fickle that states tend to balance primarily against military power; see John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: Norton, 2001). Others highlight historical anomalies, for example, Paul Schroeder, "Historical Reality vs. Neo-Realist Theory," *International Security* 19, no. 1 (1994): 108–48, https://doi.org/10.2307/2539150. My goal is not to adjudicate this debate but simply to suggest that the intuitive concept of political balancing can be extended to the realm of scientific threats. Indeed, geopolitics is often the catalyst for the emergence of a scientific threat in the first place. While the nature of military and scientific threats may differ, the political dynamics of balancing responses—worrying about uncertainty, dithering under long-time horizons, free riding on others, mobilizing action against manifest threats, for example—have a familiar rhyme and reason.

[45] Lily Chen et al., *Report on Post-Quantum Cryptography*, NISTIR 8105 (Gaithersburg, MD: National Institute of Standards and Technology, April 2016), http://dx.doi.org/10.6028/NIST.IR.8105; K. Lauter, "Postquantum Opportunities: Lattices, Homomorphic Encryption, and Supersingular Isogeny Graphs," *IEEE Security Privacy* 15, no. 4 (2017): 22–27, DOI: 10.1109/MSP.2017.3151338; and Daniel J. Bernstein et al., "Post-Quantum RSA," Cryptology ePrint Archive, 19 April 2017, https://eprint.iacr.org/.

[46] Computer Security Resource Center, "Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms," National Institute of Standards and Technology, 20 December 2016, https://csrc.nist.gov/.

[47] Dustin Moody, "Let's Get Ready to Rumble: The NIST PQC 'Competition,'" paper presented at PQCrypto 2018, Fort Lauderdale, FL, 11 April 2018, https://csrc.nist.gov/.

[48] Bruce Schneier, "NSA Plans for a Post-Quantum World," *Lawfare* (blog), 21 August 2015, https://www.lawfareblog.com/. The NSA notes that "for those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition." Quoted in Schneier.

49. L. Chen, "Cryptography Standards in Quantum Time: New Wine in an Old Wineskin?," *IEEE Security and Privacy* 15, no. 4 (2017): 51–57, https://doi.org/10.1109/MSP.2017.3151339.

50. According to Eleni Diamanti et al., "Encryption keys generated by QKD can be used in a symmetric cipher scheme, such as Advanced Encryption Standard, which is quantum resistant, for enhanced security, or they can be combined with the one-time-pad encryption scheme for unconditional security." See Eleni Diamanti et al., "Practical Challenges in Quantum Key Distribution," *Npj | Quantum Information* 2 (8 November 2016): 3, https://doi.org/10.1038/npjqi.2016.25.

51. P. D. Townsend, "Secure Key Distribution System Based on Quantum Cryptography," *Electronics Letters* 30, no. 10 (May 1994): 809–11, https://ieeexplore.ieee.org/.

52. Diamanti et al., "Practical Challenges in Quantum Key Distribution"; Christoph Simon, "Towards a Global Quantum Network," *Nature Photonics* 11, no. 11 (November 2017): 678–80, https://doi.org/10.1038/s41566-017-0032-0; Stephanie Wehner, David Elkouss, and Ronald Hanson, "Quantum Internet: A Vision for the Road Ahead," *Science* 362, no. 6412 (19 October 2018), https://doi.org/10.1126/science.aam9288; and Acín et al., "Quantum Technologies Roadmap."

53. According to Diamanti et al., "In China, the deployment of a 2,000 km QKD network between Shanghai and Beijing is underway; in Europe, after the [Secure Communication based on Quantum Cryptography] network demonstration in 2008, the UK is now creating a quantum network facilitating device and system trials, and the integration of quantum and conventional communications; in Japan, QKD technologies will be tested to secure transmission of sensitive genome data; and the US has also started installing its own QKD network." See Diamanti et al., "Practical Challenges in Quantum Key Distribution," 1–2.

54. Diamanti et al.

55. Tom Berson (@nd2t), "Quantum Key Distribution," Twitter, 23 July 2019, 4:30 p.m., https://twitter.com/.

56. Simon, "Towards a Global Quantum Network"; and Wehner, Elkouss, and Hanson, "Quantum Internet."

57. Information Security Oversight Office, "The President: Executive Order 13526; Classified National Security Information," 29 December 2009, National Archives, https://www.archives.gov/.

58. Michael Warner and Robert Louis Benson, "Venona and Beyond: Thoughts on Work Undone," *Intelligence and National Security* 12, no. 3 (July 1997): 1–13; and Richard Aldrich, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (London: HarperCollins, 2010), 72–88.

59. Michael Warner, *The Rise and Fall of Intelligence: An International Security History* (Washington, DC: Georgetown University Press, 2014), 153.

60. This framework draws on Michele Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?," paper presented at the 5th Conference on Quantum Cryptography, Tokyo, 2015, Cryptology ePrint Archive, Report 2015/1075, https://eprint.iacr.org/.

61. Jean-Pierre Dupuy, *A Short Treatise on the Metaphysics of Tsunamis*, trans. Malcolm B. DeBevoise (East Lansing: Michigan State University Press, 2015). Dupuy points out that such disasters are usually represented as being beyond control—acts of god—yet are actually made more or less likely by the behavior of their victims.

62. Steven Rich and Barton Gellman, "NSA Seeks to Build Quantum Computer That Could Crack Most Types of Encryption," *Washington Post*, 2 January 2014, https://www.washingtonpost.com/.

63. Stephen Budiansky, "Colossus, Codebreaking, and the Digital Age," in *Colossus: The Secrets of Bletchley Park's Codebreaking Computers*, ed. B. Jack Copeland (New York: Oxford University Press, 2006), 52–63.

64. Rich and Gellman, "NSA Seeks to Build Quantum Computer."

65. White House, "Advancing United States Leadership in the Industries of the Future," FY 21 fact sheet, 2 February 2020, https://www.whitehouse.gov/.

66. Cade Metz, "White House Earmarks New Money for A.I. and Quantum Computing," *New York Times*, 10 February 2020, https://www.nytimes.com/.

67. Metz.

68. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018), 2, https://dod.defense.gov/.

69. Anne Broadbent and Christian Schaffner, "Quantum Cryptography beyond Quantum Key Distribution," *Designs, Codes and Cryptography* 78, no. 1 (January 2016): 351–82, https://doi.org/10.1007/s10623-015-0157-4.

70. For further discussion of the social context of quantum cryptology, see Lindsay, "Demystifying the Quantum Threat."

Disclaimer and Copyright

The views and opinions in *SSQ* are those of the authors and are not officially sanctioned by any agency or department of the US government. This document and trademarks(s) contained herein are protected by law and provided for noncommercial use only. Any reproduction is subject to the Copyright Act of 1976 and applicable treaties of the United States. The authors retain all rights granted under 17 U.S.C. §106. Any reproduction requires author permission and a standard source credit line. Contact the *SSQ* editor for assistance: strategicstudiesquarterly@us.af.mil.