SECURITY STUDIES
2020, VOL. 29, NO. 2, 335–361
https://doi.org/10.1080/09636412.2020.1722853

Routledge
Taylor & Francis Group

Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage

Jon R. Lindsay

ABSTRACT

In theory, a fully functional quantum computer could break the cryptographic protocols that underwrite cybersecurity everywhere, which would be disastrous for national security, global trade, and civil society. Quantum cryptography, conversely, promises an unprecedented level of security, yet this benefit comes with some danger: revisionist actors with impenetrable communications might be able to conduct surprise attacks and covert conspiracies. In reality, neither of these threat scenarios are likely. Intelligence advantage in political competition depends on the interaction of technological infrastructure with organizational institutions. Robust cryptosystems can be undermined by poor organizational coordination, and careful security policy can compensate for technical vulnerabilities. Scientific innovation in quantum technology only affects one of these dimensions while potentially complicating the other. Even if the formidable engineering challenges of quantum computing can be overcome, signals intelligence collectors will still have to analyze a vast number of decrypts and deliver timely and relevant judgments to interested decision makers. The quantum networks of tomorrow, similarly, will provide little protection for complex organizations that have weak operations security practices. In the practice of intelligence, we should expect classical politics to dominate quantum computing.

"Quantum supremacy," the inflection point where a quantum computer outperforms the fastest digital supercomputer, may have already been achieved.[1] Academic labs and major firms like Google, IBM, and Microsoft are experimenting with working prototypes.[2] Governments in Europe, Asia,

Jon R. Lindsay is an assistant professor at the Munk School of Global Affairs and Public Policy and the Department of Political Science, University of Toronto. He is the author of *Information Technology and Military Power* (Cornell University Press 2020) and co-editor of *Cross-Domain Deterrence: Strategy in an Era of Complexity* (Oxford University Press 2019) and *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (Oxford University Press 2015).

[1] Aram W. Harrow and Ashley Montanaro, "Quantum Computational Supremacy," *Nature* 549, no. 7671 (13 September 2017): 203–9; Frank Arute et al. "Quantum Supremacy Using a Programmable Superconducting Processor," *Nature* 574, no. 7779 (23 October 2019): 505–10.

[2] See, for example, T. D. Ladd et al., "Quantum Computers," *Nature* 464, no. 7285 (4 March 2010): 45–53; Stephen D. Bartlett, "Atomic Physics: A Milestone in Quantum Computing," *Nature* 536, no. 7614 (4 August 2016): 35–36; T. F. Watson et al., "A Programmable Two-Qubit Quantum Processor in Silicon," *Nature* 555, no. 7698 (March 2018): 633–37.

and North America have produced serious investment plans.[3] These developments may have important consequences for international relations (IR), even as "the full promise of quantum technology is unknown, in national security or any other field."[4] As a congressman from Texas writes, "The impact of quantum on our national defense will be tremendous… . The consequences of mastering quantum computing, while not as visual or visceral as a mushroom cloud, are no less significant than those faced by the scientists who lit up the New Mexico sky with the detonation at the Trinity test site 72 years ago."[5]

The cryptographic applications of quantum computing appear particularly dramatic. In principle, a fully functional quantum computer would be able to break the mathematical protocols that underwrite cybersecurity everywhere. The categorical compromise of core cryptographic functions would have deleterious consequences for global finance, governance, justice, and national defense. According to one prominent physicist, "if a quantum computer is ever built, much of conventional cryptography will fall apart."[6] Even more breathlessly, the "cryptocalypse" would unravel trust online and end privacy as we know it.[7] While quantum computing threatens to undermine current classical protocols, a related but distinct quantum technology promises an unprecedented level of communications security.[8] Some worry that a revisionist actor with unbreakable communications could deprive Western intelligence agencies of indications and warning of surprise attack or other dangerous conspiracies. China's early progress in quantum communications has thus prompted speculation that "quantum hegemony" will provide a decisive military advantage.[9]

There are reasons to be skeptical. Concerns about an emerging Chinese quantum advantage echo earlier, and exaggerated, concerns about Chinese

[3] Antonio Acín et al., "The Quantum Technologies Roadmap: A European Community View," *New Journal of Physics* 20, no. 8 (2018): 080201; National Science and Technology Council, "National Strategic Overview for Quantum Information Science" (Washington, DC: Office of Science and Technology Policy, September 2018); 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, 12 September 2018).

[4] 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/2017/11/leap-quantum-technology-primer-national-security-professionals/.

[5] Will Hurd, "Quantum Computing Is the Next Big Security Risk," *Wired*, 7 December 2017.

[6] Gilles Brassard quoted in Hoi-Kwong Lo and Norbert Lütkenhaus, "Quantum Cryptography: From Theory to Practice," *Physics in Canada* 63, no. 4 (21 February 2007): 191–96.

[7] 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/innovation/inventions/quantum-computing-set-to-revolutionise-everything-from-national-security-to-drug-design-and-financial-investments/news-story/2b495e494f47ee43b3975f5e884f11af.

[8] Gilles Brassard, "Cryptography in a Quantum World," in *SOFSEM 2016: Theory and Practice of Computer Science* (Berlin: Springer, 2016), 3–16.

[9] Taylor Owen and Robert Gorwa, "Quantum Leap: China's Satellite and the New Arms Race," *Foreign Affairs*, 7 September 2016; Kania and Costello, "Quantum Hegemony?"; Glenn S. Gerstell, "I Work for N.S.A. We Cannot Afford to Lose the Digital Revolution," *New York Times*, 10 September 2019.

advantages in digital technology.[10] More generally, quantum threat narratives about the end of protection and the end of collection rely on questionable assumptions about the social context of technology and the practice of intelligence. There are serious engineering hurdles to clear before anyone will possess a quantum computer powerful enough to crack public encryption. Moreover, alternative cryptographic protocols that are believed to be safe from both classical and quantum attack are already under review by technical standards–setting bodies. Even in the worst-case scenario where a quantum computer emerges before quantum-safe offsets are in place, it is unlikely quantum computing will transform intelligence or politics. The best cryptanalysis is useless if analysts cannot identify valuable intelligence, or if customers cannot or will not use it. The best cryptography, likewise, offers little defense against flawed organizational implementations or the gullibility or negligence of human users. If the quantum information revolution comes to pass, therefore, it will still be possible to protect and collect secrets.

This article explains how technological infrastructure and organizational institutions interact to shape intelligence advantage—the ability to collect or protect secret information that is useful for political competition. I draw on scholarship on military innovation to highlight the social factors that shape any kind of technological advantage. Then I model intelligence advantage as the interaction of technical infrastructure and organizational institutions in strategic context. Next, I use these concepts to explore the limits of quantum cryptanalysis and quantum-safe cryptography. I find that the macroscale realities of classical politics are likely to overwhelm the microscale possibilities of quantum computing.[11]

Infrastructure and Institutions

From the stirrup to cyberwarfare, narratives of technological revolution reappear regularly in strategic thought. By and large, scholars of military innovation view them with a jaundiced eye.[12] Different strands of this literature focus on the causes of major doctrinal changes,[13] the diffusion of

[10] Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security* 39, no. 3 (Winter 2014/15): 7–47; Greg Austin, *Cybersecurity in China: The Next Wave* (Zurich: Springer, 2018).

[11] I want to make it clear that I am not arguing that political reality has a quantum nature or that quantum mechanics should be used to rethink political theory. Cf. Alexander Wendt, *Quantum Mind and Social Science: Unifying Physical and Social Ontology* (New York: Cambridge University Press, 2015). On the contrary, my argument moves in the opposite direction, using familiar institutional and strategic concepts to bound the political implications of quantum mechanics.

[12] Reviews include Adam Grissom, "The Future of Military Innovation Studies," *Journal of Strategic Studies* 29, no. 5 (October 2006): 905–34; Stuart Griffin, "Military Innovation Studies: Multidisciplinary or Lacking Discipline?" *Journal of Strategic Studies* 40, no. 1–2 (January 2017): 196–224.

[13] Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars* (Ithaca, NY: Cornell University Press, 1984); Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca, NY: Cornell University Press, 1991); Owen Reid Cote Jr., "The Politics of Innovative Military

capabilities,[14] the military-industrial complex,[15] and battlefield effectiveness.[16] Yet a common refrain is that technological possibilities do not determine strategic outcomes. Politics shapes technology, more often than not, precisely because political actors anticipate that technology will shape the pursuit of power.[17] Social practices coordinate the invention and operation of material systems while organizational behavior is constrained and enabled by technological structures.[18]

Technology is both pervasive and vital in international security, but it does not determine strategic outcomes for at least two reasons. First, the implementation of technological infrastructure requires actors to negotiate many problems. Engineering at the scientific frontier is inherently difficult, and systems integration is intrinsically complex.[19] Not every state has the financial resources and organizational capacity to innovate advanced weaponry.[20] The

Doctrine: The U.S. Navy and Fleet Ballistic Missiles" (PhD diss., Massachusetts Institute of Technology, 1996); Elizabeth Kier, *Imagining War: French and British Military Doctrine between the Wars* (Princeton, NJ: Princeton University Press, 1997); Grissom, "The Future of Military Innovation Studies."

[14] Stephanie G. Neuman, "International Stratification and Third World Military Industries," *International Organization* 38, no. 1 (Winter 1984): 167–97; Emily O. Goldman and Leslie C. Eliason, eds., *The Diffusion of Military Technology and Ideas* (Stanford, CA: Stanford University Press, 2003); Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (Princeton, N.J: Princeton University Press, 2010); Andrea Gilli and Mauro Gilli, "The Spread of Military Innovations: Adoption Capacity Theory, Tactical Incentives, and the Case of Suicide Terrorism," *Security Studies* 23, no. 3 (July–September 2014): 513–47; Andrea Gilli and Mauro Gilli, "Why China Hasn't Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber-Espionage," *International Security* 43, no. 3 (Winter 2018/19): 141–89.

[15] Eugene Gholz, "Globalization, Systems Integration, and the Future of Great Power War," *Security Studies* 16, no. 4 (October–December 2007): 615–36; Jonathan D. Caverley, "United States Hegemony and the New Economics of Defense," *Security Studies* 16, no. 4 (October–December 2007): 598–614; Peter Dombrowski and Eugene Gholz, *Buying Military Transformation: Technological Innovation and the Defense Industry* (New York: Columbia University Press, 2006).

[16] Risa A. Brooks and Elizabeth A. Stanley, eds., *Creating Military Power: The Sources of Military Effectiveness* (Stanford, CA: Stanford University Press, 2007); Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, NJ: Princeton University Press, 2004); Ryan Grauer, *Commanding Military Power: Organizing for Victory and Defeat on the Battlefield* (New York: Cambridge University Press, 2016).

[17] William H. McNeill, *The Pursuit of Power: Technology, Armed Force, and Society since A.D. 1000* (Chicago: University of Chicago Press, 1982). The interdisciplinary field of science, technology, and society (STS) offers a rich alternative to technological determinism; inter alia, Langdon Winner, *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought* (Cambridge, MA: MIT Press, 1977); Wiebe E. Bijker, Thomas P. Hughes, and Trevor Pinch, eds., *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (Cambridge, MA: MIT Press, 1987); David E. Nye, *Technology Matters: Questions to Live With* (Cambridge, MA: MIT Press, 2006). For a counterargument to the STS consensus, cf. Allan Dafoe, "On Technological Determinism: A Typology, Scope Conditions, and a Mechanism," *Science, Technology, & Human Values* 40, no. 6 (November 2015): 1047–76.

[18] On the reciprocal interaction of social and technical factors, see: Bruno Latour, "Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts," in *Shaping Technology/Building Society: Studies in Sociotechnical Change*, ed. Wiebe E. Bijker and John Law (Cambridge, MA: MIT Press, 1992), 225–58; Geoffrey C. Bowker and Susan Leigh Star, *Sorting Things Out: Classification and Its Consequences* (Cambridge, MA: The MIT Press, 1999); Wanda J. Orlikowski, "Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations," *Organization Science* 11, no. 4 (July–August 2000): 404–28; Greg Downey, "Virtual Webs, Physical Technologies, and Hidden Workers: The Spaces of Labor in Information Internetworks," *Technology and Culture* 42, no. 2 (April 2001): 209–35.

[19] Thomas P. Hughes, *Rescuing Prometheus: Four Monumental Projects That Changed the Modern World* (New York: Random House, 1998); Andrea Prencipe, Andrew Davies, and Michael Hobday, eds., *The Business of Systems Integration* (New York: Oxford University Press, 2003); Gholz, "Globalization, Systems Integration, and the Future of Great Power War."

[20] Horowitz, *The Diffusion of Military Power*.

costs to acquire a military capability include not only the price of building and operating the weapons themselves but also the supporting infrastructure needed to do so—bases, airfields, satellites, networks, etc.[21] As a result, there tends to be significant variation in the international diffusion of military capabilities. This empirical finding is at odds with the claims of some structural realists that potent technologies should diffuse quickly through the international system.[22] Instead, high-end capability appears to be getting more concentrated rather than less.[23]

Second, the actual use of technology in war must confront a different set of doctrinal and administrative complexities. Political and military organizations must develop doctrine for new capabilities and coordinate their use in operational circumstances full of friction and uncertainty.[24] Various platforms, branches, services, and government agencies, each with their own material cultures and bureaucratic interests, have to be integrated into a coherent politico-military force.[25] While infrastructural challenges raise the barriers to acquiring any given operational capability, institutional factors condition its effectiveness in strategic competition.

Both types of challenges are as relevant for intelligence as they are for military power. Indeed, the military innovation literature emerged partly in reaction to exuberant claims about a "revolution in military affairs" created by novel intelligence capabilities.[26] Modern warfare depends on accurate surveillance, analysis, and targeting, which in turn rely on enabling intelligence systems.[27] For example, the American advantage in antisubmarine warfare throughout the Cold War required not just quiet attack submarines and long-range patrol aircraft but also a distributed network of operational intelligence organizations that could integrate data from undersea hydrophones and other sources.[28]

[21] Gilli and Gilli, "The Spread of Military Innovations"; Gilli and Gilli, "Why China Hasn't Caught Up Yet."

[22] Kenneth N. Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley, 1979).

[23] Caverley, "United States Hegemony and the New Economics of Defense"; Stephen G. Brooks and William C. Wohlforth, "The Rise and Fall of the Great Powers in the Twenty-First Century: China's Rise and the Fate of America's Global Position," *International Security* 40, no. 3 (Winter 2015/16): 7–53; Michael Beckley, "The Power of Nations: Measuring What Matters," *International Security* 43, no. 2 (Fall 2018): 7–44.

[24] Rosen, *Winning the Next War*; Biddle, *Military Power*; Thomas G. Mahnken, *Technology and the American Way of War since 1945* (New York: Columbia University Press, 2010).

[25] C. Kenneth Allard, *Command, Control, and the Common Defense* (New Haven, CT: Yale University Press, 1990); Harvey M. Sapolsky, Eugene Gholz, and Caitlin Talmadge, *US Defense Politics: The Origins of Security Policy*, 3rd ed. (New York: Routledge, 2017).

[26] Technocentric accounts include Andrew F. Krepinevich, ed., *The Military-Technical Revolution: A Preliminary Assessment* (Washington, DC: Center for Strategic and Budgetary Assessments, 2002); William A. Owens and Edward Offley, *Lifting the Fog of War* (New York: Farrar, Straus and Giroux, 2000). For an extended review, see Tim Benbow, *The Magic Bullet? Understanding the Revolution in Military Affairs* (London: Brassey's, 2004).

[27] Barry D. Watts, "The Evolution of Precision Strike" (Washington, DC: Center for Strategic and Budgetary Assessments, 2013); Emily O. Goldman, ed., *Information and Revolutions in Military Affairs* (New York: Routledge, 2005).

[28] Owen R. Cote Jr., "The Third Battle: Innovation in the U.S. Navy's Silent Cold War Struggle with Soviet Submarines," *Newport Papers* 16 (Newport, RI: Naval War College, 2003); Christopher Ford and David Rosenberg, *The Admirals' Advantage: U.S. Navy Operational Intelligence in World War II and the Cold War* (Annapolis, MD: Naval Institute Press, 2005).

The technological dimension of intelligence is especially prominent in cybersecurity.[29] One strand of the cyber debate in IR argues that networked information technologies are inherently dangerous and disruptive.[30] From this perspective, the quantum information revolution represents a fundamental change in the material implementation of cyberspace and should thus be particularly consequential. Another strand of debate echoes themes from the military innovation literature. Cyber skeptics stress the operational challenges of remote-control warfare,[31] the strategic disincentives for large-scale attacks,[32] the political tendency to exaggerate threats,[33] and the empirical pattern of low-intensity cyber conflict.[34] From this perspective, quantum information technologies can be expected to run afoul of familiar infrastructural and institutional problems.

Intelligence Advantage

Intelligence advantage is shaped by the interaction of technological infrastructure and organizational institutions in some strategic context. Quantum information technology can only directly affect the former, and then only in part. By "intelligence" here I mean the collection and protection of politically valuable secrets rather than covert action.[35] In this article,

[29] Jon R. Lindsay, "Cyber Espionage," in *The Oxford Handbook of Cybersecurity*, ed. Paul Cornish (New York: Oxford University Press, forthcoming).

[30] Inter alia, John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (April 1993): 141–65; Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001); Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Ecco, 2010); Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (Fall 2013): 7–40; Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations* (New York: Oxford University Press, 2016); Jacquelyn Schneider, "The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War," *Journal of Strategic Studies* 42, no. 6 (September 2019): 841–63.

[31] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (April–June 2013): 365–404; Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37; Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41, no. 3 (Winter 2016/17): 72–109.

[32] Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (2012): 401–28; Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (Fall 2013): 41–73; Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyber Attack," *Journal of Cybersecurity* 1, no. 1 (September 2015): 53–67; Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (July–September 2017): 452–81.

[33] Myriam Dunn Cavelty, "Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate," *Journal of Information Technology & Politics* 4, no. 1 (2008): 19–36; Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats," *Journal of Information Technology & Politics* 10, no. 1 (2013): 86–103.

[34] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–32; Brandon Valeriano and Ryan C. Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–2011," *Journal of Peace Research* 51, no. 3 (May 2014): 347–60; Sarah Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics," *Journal of Cybersecurity* 5, no. 1 (January 2019 [online]).

[35] Intelligence scholars debate whether covert action, secrecy, or government agency are necessary for a definition of intelligence. I follow Michael Warner in considering secrecy to be constitutive: Michael Warner, "Wanted: A Definition of 'Intelligence,'" *Studies in Intelligence* 46, no. 3 (2002 [online]); Michael Warner, "Fragile and Provocative: Notes on Secrecy and Intelligence," *Intelligence and National Security* 27, no. 2 (April 2012):

I focus narrowly on the signals intelligence (SIGINT) exploitation of digital data and the operations security (OPSEC) measures employed against it, for the simple reason that these are the areas where quantum computing is expected to have a major impact.[36] Quantum technology may also enable stealth-defeating radar, subatomic lithography for expanded data storage, algorithmic enhancements for artificial intelligence (AI), and advanced scientific modeling and simulation.[37] These are important applications, and there are doubtlessly others not yet imagined, but they are beyond the scope of this article.

Quantum-threat narratives tend to ignore sociotechnical context and extrapolate directly to radical intelligence advantage. If, for instance, a quantum computer could break public encryption protocols, then this would provide a major collection advantage. An attacker could gain access to all manner of sensitive military, diplomatic, and commercial secrets. Insight into a competitor's secret plans and capabilities could, in turn, be used to enhance warfighting, bargaining performance, and market power. If, conversely, quantum communications could provide unbreakable security, then this would provide a major secrecy advantage. In the wrong hands, perfect OPSEC could be used to protect preparations for a surprise attack or a criminal conspiracy. Extreme versions of these threat narratives can be described, respectively, as the end of privacy or "cryptocalypse," and the end of intelligence or "going dark."

It is important to appreciate that quantum computing and quantum communications are very different technologies. The details will be discussed later, but at this juncture the important difference is that they have applications on opposite sides of the intelligence contest between collectors

223–40. While intelligence shares many features with data science, journalism, and scholarship, it is distinguished by reliance on secret sources and methods and/or the use of open-source information for secret ends. Warner also considers covert action (disinformation, subversion, sabotage) an essential dimension of intelligence statecraft; while I generally agree with him on this point, I set aside covert action in this article to focus on the espionage implications of quantum technology. I also relax Warner's focus on state intelligence given that quantum technologies are likely be used, or used predominantly, by nonstate actors such as commercial firms. By politically valuable secrets I mean any private information useful for political, military, or economic competition.

[36] Collection disciplines other than SIGINT include human intelligence (HUMINT), geospatial or imagery intelligence (GEOINT, IMINT), and measurement and signature intelligence (MASINT); see Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 6th ed. (Los Angeles: CQ Press, 2015), chap. 5. SIGINT can be further divided into the exploitation of electronic emissions (ELINT) and human communications (COMINT). Cyber (computer network) exploitation is a functional amalgam of ELINT and COMINT, but it is methodologically distinct from either, with some overlap with HUMINT. Cryptanalysis (code-breaking), moreover, is just one component of COMINT, which also includes radio direction finding and traffic analysis. The cryptanalytic application of quantum computing is thus quite specialized within the broader SIGINT enterprise. In this article I use "SIGINT" as a general umbrella term referring to the collection of digital secrets. I also use the term "OPSEC" here in a very general sense to refer to passive defenses such as data classification and compartmentalization as well as active counterintelligence measures.

[37] National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects* (Washington, DC: National Academies Press, 2019).

and protectors.[38] Specifically, they have complementary applications in the cryptologic contest between code-breakers (cryptanalysis) and code-makers (cryptography). Quantum computing has the potential to dramatically improve SIGINT by enabling timely cryptanalysis of popular security protocols. Quantum computing might also enable minor improvements for data analysis and search optimization, which could be useful for making sense of the vast amount of information produced through bulk decryption via quantum algorithms, or for the analytical fusion of SIGINT with other sources of intelligence. Quantum communications, by contrast, might improve OPSEC by enabling alternative approaches to encryption that are safe from attack by both quantum and classical methods. Furthermore, there exist mathematical protocols described as "quantum safe" or "quantum resistant" that do not depend on any quantum hardware whatsoever (which is precisely what makes them attractive).

It is also important to appreciate that intelligence advantage in both narratives can only ever provide an indirect political advantage. A SIGINT advantage can be invaluable in war if it provides timely warning of an enemy attack or helps to locate enemy targets. SIGINT advantage can also be invaluable in peace if it reveals the negotiating position or intellectual property of a competitor. OPSEC, similarly, can be invaluable in war and peace by denying these advantages to a competitor. Yet SIGINT must be put to work in the context of warfighting or political-economic bargaining to make a difference. Leaders who ignore timely and relevant SIGINT, or circumstances that change before they can act on it, will undermine the value of intelligence. Knowledge is power, but only if exercised at the right time and place. Likewise, OPSEC only becomes a threat if used to cover offensive operational moves or conceal valuable assets. Actors who have nothing important to hide gain little additional benefit through perfect OPSEC. Offensive or defensive advantage in an intelligence contest, finally, provides at best an indirect or relative improvement in an actor's power position. The political use of intelligence advantage is a separate problem.[39]

The social context of intelligence technology conditions its effectiveness. Cryptographic protocols are just mathematical functions. They must be implemented in software and hardware to encrypt and decrypt data. A cryptosystem is the suite of cryptologic protocols and computing infrastructure an organization uses to protect confidential data from unauthorized access (and

[38] On the notion of an intelligence contest applied to cyber operations, see Joshua Rovner, "Cyber War as an Intelligence Contest," *War on the Rocks* (blog), 16 September 2019, https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

[39] On intelligence–policy relations see Michael I. Handel, *War, Strategy and Intelligence* (London: Frank Cass, 1989); Michael Herman, *Intelligence Power in Peace and War* (New York: Cambridge University Press, 1996); Joshua Rovner, *Fixing the Facts: National Security and the Politics of Intelligence* (Ithaca, NY: Cornell University Press, 2011); Keren Yarhi-Milo, *Knowing the Adversary: Leaders, Intelligence, and Assessment of Intentions in International Relations* (Princeton, NJ: Princeton University Press, 2014).

ensure its availability to authorized users). The best case, from an OPSEC perspective, is a rigorous implementation of strong protocols. This increases the chances that an organization will be able to reliably encrypt and authenticate data. The worst case, conversely, is a flawed implementation of weak protocols. In between the extremes of secure and insecure cryptosystems, a rigorous implementation of weak protocols will result in weakened security that is, nonetheless, mitigated by emissions control (EMCON) procedures, physical access control ("air gaps"), information compartmentalization, active counterintelligence, and other OPSEC policy measures that reduce the exposure of valuable data to a SIGINT attacker. Conversely, an organization with a flawed implementation of strong protocols will create self-inflicted vulnerabilities, fumbling away the mathematical potential for security.

Successful OPSEC thus depends not only on strong cryptographic technology but also bureaucratic policy and the conscientiousness of operational personnel. It follows that organizational institutions can either compensate for technological vulnerabilities or undermine technological strengths. On the other side of the intelligence contest, likewise, a SIGINT organization must be able to recognize and exploit the target's technological and organizational weaknesses. Sophisticated cryptanalytic technology will provide little advantage if an attacker lacks the technical and organizational skill to engineer an intrusion, ensure the security of the operation, analyze the take, and deliver useful products to intelligence consumers. The best case, again from an OPSEC perspective, is a coordinated security posture in which the target organization has the capacity to guard against every possible move from a collector that lacks the organizational capacity to conduct sophisticated attacks. The worst case is an uncoordinated posture in which a low-capacity protector is outmaneuvered by a high-capacity collector. In the middle, once again, there are mixed cases. High-capacity protectors and collectors may engage in complicated intelligence–counterintelligence interactions with ambiguous results, exemplified by the intelligence contest between the KGB and CIA in Cold War Berlin.[40] Conversely, the outcome of a contest between protectors and collectors who are both organizationally inept will turn more on hope and luck than competence. Lucky security is sadly still widespread in major corporate and government organizations today, a world full of targets with poor OPSEC together with attackers who make a lot of mistakes.

Table 1 describes a simplified theory of intelligence advantage as a function of cryptographic infrastructure and organizational institutions.[41]

[40] David E. Murphy, Sergei A. Kondrashev, and George Bailey, *Battleground Berlin: CIA Vs. KGB in the Cold War* (New Haven, CT: Yale University Press, 1997).

[41] This is an extension of the theory of information practice presented in Jon R. Lindsay, *Information Technology and Military Power* (Ithaca, NY: Cornell University Press, 2020), chap. 2. Cryptographic infrastructure here is a

Table 1. Intelligence advantage as a function of the target organization's cryptographic infrastructure and institutional coordination relative to the attacking organization.

	Strong Cryptosystem	Weak Cryptosystem
Coordinated Target	OPSEC advantage	SIGINT failure
Uncoordinated Target	OPSEC failure	SIGINT advantage

Strong cryptosystems (robust protocol and implementation) and a coordinated security posture (target institutions relatively more capable than attacking institutions) result in an OPSEC advantage. At the extreme, this corresponds to the quantum-threat narrative about the end of intelligence. Conversely, weak systems (poor implementations of insecure protocols) and an uncoordinated posture (offense relatively more capable than defense) are a boon for SIGINT, which at the extreme corresponds to the end-of-secrecy narrative. The off-axis categories describe organizational failures by the competitors that squander technological potential. An OPSEC failure occurs when strong cryptography is available, but lax security policy or complacent behavior undermines it. In this case, a relatively more capable SIGINT attacker can exploit the sociotechnical implementation of the defender's cryptosystem. In the remaining case, a SIGINT failure occurs when exploitable technical vulnerabilities and potent cryptanalytic methods exist, but the target organization compensates with protective countermeasures and/or the complexity of the intelligence process overwhelms the attacker.

These are ideal types. As suggested above, actual cryptosystems usually fall somewhere in between the strong and weak extremes. Relative organizational capacity, likewise, is usually neither completely coordinated nor uncoordinated. Organizations with contested or lucky security postures usually muddle through with vulnerable or degraded technologies. These variables tend to change endogenously over time, furthermore, as intelligence competitors adjust their tradecraft and posture in response to threats and opportunities that they discover. Technological innovation in cryptanalysis may undermine the OPSEC advantage of a coordinated protector. Yet the collector may still suffer SIGINT failures until it improves its organizational capacity to exploit the new cryptanalytic potential. The threat or reality of SIGINT advantage may spur protectors to innovate in cryptography. Yet protectors may still suffer OPSEC failures until they improve their organizational capacity to take advantage of the new cryptographic potential. The dynamic interaction of technologies and organizations continues haltingly and indefinitely. This interaction tends to ratchet up the complexity of the intelligence problem over time without, however, delivering either side a lasting intelligence advantage. The evolution of intelligence practice is an ongoing, complex, and ambiguous process.

component of what the book describes as "the external problem," which includes the technological potential of any given era, while institutional coordination here corresponds to "the internal solution."

Code-Breaking with Quantum Computing

How should we expect quantum information technology to fare in an intelligence contest? This section examines intelligence advantage from the attacker's perspective. The next section will examine the target's perspective. Quantum computing creates the scientific possibility of weakening existing cryptographic infrastructure, which potentially improves SIGINT. Realizing this possibility, however, requires the construction of a universal quantum computer powerful and reliable enough to run quantum algorithms at scale against public encryption protocols. If the engineering obstacles are not overcome, then OPSEC will maintain the advantages it has today (conditioned on the target's OPSEC policy and organizational behavior). Even if a quantum computer is built, furthermore, the SIGINT attacker might still fail to leverage it properly to create an advantage against an organized and determined defender.

The End of Secrecy?

A digital bit is a scalar quantity that must be exactly zero or one. By contrast, a quantum bit (qubit) is a vector of complex numbers known as "probability amplitudes" that represent a "superposition" of zero and one. Multiple qubits can be "entangled" such that the whole system represents more information than a collection of separable qubits. The abstraction of quantum computing is essentially a generalization of probability theory and information theory that enables new mathematical solutions to some previously intractable problems.[42] It is important to understand that a quantum computer is not some sort of general-purpose parallel computing machine that can speed up any algorithm whatsoever, as is so often misrepresented in popular accounts.[43] Quantum computers can, in principle, compute more efficient solutions for some specific problems, if and only if a suitable quantum algorithm has been discovered. There are no known quantum speedups for many of the algorithms used in everyday computing. There are also few known practical applications for many quantum algorithms that have been invented, aside from benchmarking the performance of quantum computers.[44]

It so happens that a quantum algorithm does exist that can attack the mathematical protocols widely used today for public key infrastructure (PKI), which enables secure internet connections and digital signatures.

[42] Scott Aaronson, *Quantum Computing since Democritus* (New York: Cambridge University Press, 2013); Mark M. Wilde, *Quantum Information Theory*, 2nd ed. (New York: Cambridge University Press, 2017).

[43] For example, Vivek Wadhwa, "Quantum Computers May Be More of an Imminent Threat than AI," *Washington Post*, 5 February 2018.

[44] For a thorough review of technical concepts, see National Academies of Sciences, Engineering, and Medicine, *Quantum Computing*.

PKI depends on so-called asymmetric protocols like Rivest-Shamir-Adleman (RSA) and Diffie-Helman (DH) that rely on distinct keys for encryption and decryption (contrasted with symmetric protocols that use the same key for each operation). A critical requirement of asymmetric encryption is that it must be extremely difficult to guess the private key (used to decrypt messages or produce digital signatures) from the public key (used to encrypt messages or authenticate signatures). RSA relies on the mathematical fact that it is easy to multiply two large prime numbers together but exponentially harder to factor the result with classical methods. A typical desktop computer would need over six quadrillion years to crack a 2048-bit RSA key.[45] However, a quantum algorithm described by Peter W. Shor can factor prime numbers exponentially faster than the fastest known classical algorithm.[46] Assuming major engineering progress in quantum computing, it may someday be possible to recover a private key from a public key in a matter of hours.[47] Another quantum algorithm discovered by Lov Grover poses a minor threat to symmetric protocols like Advanced Encryption Standard (AES) and Secure Hash Algorithms (SHA), but Grover's speedup can be offset by doubling the size of the key.[48] Unfortunately, AES and SHA cannot be used alone to implement PKI systems. Current implementations of PKI depend on asymmetric protocols like RSA and DH that are vulnerable, in principle, to quantum cryptanalysis.

The importance of PKI cannot be overemphasized.[49] PKI enables online banking, software updates, electronic medical records, virtual private networks (VPN) and intranets, remote maintenance on industrial machinery, and the monitoring and control of industrial operations. Military and government agencies use PKI to authenticate access to secure facilities, secure networks, and compartmented information on those networks. PKI and VPN technology enable secret and top-secret traffic to tunnel through the public internet. Nuclear weapons inspectors rely on PKI to verify that controlled equipment at remote sites has not been tampered with. The systematic compromise of PKI would put all these things at risk. Threat actors might be able to bypass access controls, exploit web services protected by

[45] DigiCert, "Check our Numbers: The Math Behind Estimations to Break a 2048-bit Certificate," https://web.archive.org/web/20181004033325/https://www.digicert.com/TimeTravel/math.htm.

[46] Peter W. Shor, "Algorithms for Quantum Computation: Discrete Logarithims and Factoring," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (Santa Fe, NM: IEEE Computer Society, 1994), 124–34.

[47] Craig Gidney and Martin Ekerå, "How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits," *arXiv*, 6 December 2019, https://arxiv.org/pdf/1905.09749.pdf.

[48] Daniel J. Bernstein, "Grover vs. McEliece," in *Post-Quantum Cryptography*, ed. Nicolas Sendrier (Berlin: Springer, 2010), 73–80; Stephen P. Jordan and Yi-Kai Liu, "Quantum Cryptanalysis: Shor, Grover, and Beyond," *IEEE Security Privacy* 16, no. 5 (September/October 2018): 14–21.

[49] Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, *Cryptography Engineering: Design Principles and Practical Applications* (Indianapolis, IN: Wiley, 2010), 275–300; John Mulholland, Michele Mosca, and Johannes Braun, "The Day the Cryptography Dies," *IEEE Security Privacy* 15, no. 4 (2017): 14–21.

TLS/SSL,[50] forge digital certificates, and install arbitrary code. Insider threats would become more dangerous because moles would be able to access and decrypt data stored on intranets and within the protected compartments of classified systems. External threats would be harder to detect since they could copy data in transit without having to intrude into a network to gather data at rest. Threat actors could also forge credentials to upload malware into critical infrastructure or inject bogus data into trusted systems. Any data encrypted with AES would still be safe; however, if the master keys to a cryptosystem were placed on or transmitted through a network protected with PKI, then data protected by AES would become exposed too. Shor's algorithm is an extreme example of what computer security professionals call a "class break" because it affects an entire class of functionality rather than just a single application.[51] One physicist thus warns that when PKI "breaks down, our way of life breaks down."[52]

Engineering Challenges in Quantum Computing

Superposition and entanglement are counterintuitive concepts that do not correspond with everyday experience. Quantum technologies are exciting precisely because they amplify weird microscale phenomena into useful macroscale effects. In the process, however, they encounter thermodynamic noise, electromagnetic effects, infrastructural friction, and messy human organizations.

The implementation of a fully functional quantum computer must overcome several hurdles. Engineers must be able to physically realize a very large number of logical qubits capable of superposition and entanglement. They must be able to set the initial value of qubits as an input, maintain the coherence of the quantum state of the qubits while systematically manipulating superposition and entanglement, accurately measure the results of the computation, and control for errors throughout the entire process. Errors occur in classical digital computers, of course, but they tend to be random rather than correlated, and it is easy to check and repair errors using backup data and checksum bits. Yet an entangled quantum state is shared across many qubits, which means that local errors can have systemic consequences, and quantum data cannot simply be copied for backups (due to the "no-cloning theorem"). Specialized quantum error correction algorithms do exist, but they require significant computational overhead and many additional (ancilla) qubits. To take just one example, a

[50] Transport Layer Security (TLS), and its deprecated predecessor Secure Sockets Layer (SSL), enables secure internet communications. TLS is commonly used for secure web browsing via HyperText Transfer Protocol Secure (HTTPS).

[51] Bruce Schneier, "Class Breaks," *Schneier on Security* (blog), 3 January 2017, https://www.schneier.com/blog/archives/2017/01/class_breaks.html.

[52] Stephen Ornes, "Code Wars," *Proceedings of the National Academy of Sciences of the United States of America* 114, no. 11 (14 March 2017): 2784–87.

quantum algorithm for simulating one particular problem in physical chemistry requires only 111 logical qubits but 180 million physical qubits to allow for error correction.[53]

The theoretical promise of quantum cryptanalysis is moot if a SIGINT agency is unable to maintain the coherence of a huge number of qubits. Experimental prototypes have been able to maintain dozens of qubits in coherence for brief periods of time in extremely cold conditions (that is, 15 millikelvin, colder than outer space) within carefully shielded laboratories that minimize random thermodynamic and electromagnetic perturbations. In November 2017 IBM announced that it had built working 20- and 50-qubit machines that were able to maintain a coherence time of 90 microseconds, the time available to perform calculations on entangled qubits before losing quantum state information.[54] Google announced a 72-qubit machine in March 2018 but provided little performance data.[55] A Google machine known as Sycamore reportedly achieved "quantum supremacy" in September 2019 by entangling 53 qubits to run a quantum algorithm in just over three minutes that would take a classical computers ten thousand years to simulate.[56] The Canadian firm D-Wave boasts thousands of qubits, but most scientists would argue that they are not fully functional qubits.[57] Some nominally quantum machines can solve only a particular subset of quantum information problems due to limitations in their qubit implementations or because they are unable to maintain coherence long enough to complete useful calculations.

Cracking a 2048-bit RSA key requires over four thousand logical qubits, which is already orders of magnitude more than prototype systems can manage today.[58] To maintain thousands of logical qubits in a coherent state with quantum error correction would require at least twenty million physical qubits using the most efficient design known today.[59] The state of the

[53] National Academies of Sciences, Engineering, and Medicine, *Quantum Computing*, 3–15.

[54] Samuel K. Moore, "IBM Edges Closer to Quantum Supremacy with 50-Qubit Processor," *IEEE Spectrum*, 15 November 2017.

[55] Martin Giles and Will Knight, "Google Thinks It's Close to 'Quantum Supremacy.' Here's What That Really Means," *Technology Review*, 9 March 2018.

[56] Arute et al., "Quantum Supremacy Using a Programmable Superconducting Processor." Scientists at IBM counter that "an ideal simulation of the same task can be performed on a classical system in 2.5 days and with far greater fidelity," as quoted in Edwin Pednault et al., "On 'Quantum Supremacy,'" *IBM Research Blog*, 21 October 2019, https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy. However, even this significant IBM optimization, running on the largest supercomputer in the world (Oak Ridge Summit) and consuming 250 petabytes of memory, would still take considerably longer than the 200 seconds required by Sycamore, while quantum algorithms using more than 53 qubits would quickly exceed Summit's capacity; see Scott Aaronson, "Why Google's Quantum Supremacy Milestone Matters," *New York Times*, 30 October 2019.

[57] Troels F. Rønnow et al., "Defining and Detecting Quantum Speedup," *Science* 345, no. 6195 (25 July 2014): 420–24; Philip Ball, "The Era of Quantum Computing Is Here. Outlook: Cloudy," *Quanta Magazine*, 24 January 2018.

[58] Jordan and Liu, "Quantum Cryptanalysis: Shor, Grover, and Beyond."

[59] Gidney and Ekerå, "How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits," proposes a significant improvement over previous schemes that required as many as a billion qubits. Even this achievement, however, remains many orders of magnitude beyond what can be realized presently.

art in quantum engineering today is nowhere close. An operational universal quantum computer able to break RSA remains decades away, if it is possible at all. As a US Air Force study on the military utility of quantum technology concludes, "the path from theory to practical systems is formidable, and … despite claims heralding imminent breakthroughs, as of now, no compelling evidence exists that quantum computers can be usefully applied to computing problems of interest to the Air Force."[60] Google's impressive milestone notwithstanding, it is premature to conclude that the quantum information revolution is already here, or even just around the corner.

The Institutional Challenges of SIGINT

Nevertheless, let us assume for the sake of argument that all the formidable engineering obstacles can be overcome. Even if a quantum computer can break RSA in the lab, intelligence advantage in political competition would still depend on many additional choices by many actors. Intelligence is not a static product, but a process, often described as an ongoing cycle.[61] Leadership articulates intelligence requirements and constraints. Organizations collect and process information while protecting sensitive sources and methods. Analysts try to make sense of the take and place it in context for intelligence consumers. Policymakers or commanders must then understand, care about, and act on intelligence. Their perceived successes and failures encourage them to revise information requirements or undertake intelligence reforms. Everyone involved must take counterintelligence precautions. There are many transaction costs and frictions throughout the intelligence cycle that can undermine the advantages created by quantum decryption.[62]

To steal valuable secrets, the target must possess some valuable secrets in the first place. The target must be reliant on secrecy to protect a bargaining advantage, an operational capability, or intellectual property, or there will be nothing of value to discover in all the data collected. Relevant secrets, furthermore, must be encoded in a medium that is exposed to collection and vulnerable in principle to decryption, not committed to memory or recorded on paper that does not circulate. Put simply, the target must make some OPSEC mistakes. A formidable target might also run counterintelligence operations to deceive the SIGINT collector by planting fake

[60] USAF Scientific Advisory Board, "Utility of Quantum Systems for the Air Force," 19 August 2016, http://www.scientificadvisoryboard.af.mil/Portals/73/documents/AFD-151214-041.pdf?ver=2016-08-19-101445-230.

[61] Lowenthal, *Intelligence: From Secrets to Policy*, chap. 4.

[62] Jon R. Lindsay and Tai Ming Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015); Gilli and Gilli, "Why China Hasn't Caught Up Yet."

data. While quantum computing might support bulk decryption of intercepted data, it does little to improve the agency's access and placement for intercepting valuable data in the first place, especially if the target has relatively strong OPSEC and an active counterintelligence posture.

Then the intelligence agency must be able to identify and make sense of the secrets it has collected. After cryptanalysts break the target's cryptosystem, they must process and decrypt the relevant secrets out of a huge volume of traffic they have collected. Advanced SIGINT agencies like the NSA already can only process a small percentage of what they collect. Bulk quantum decryption of the totality of digital communication would create even bigger haystacks to sift through without necessarily revealing more needles. Automation and machine learning can help with the processing and analysis of SIGINT to some extent; indeed, "big data" techniques are essential given the growing volume of open-source and classified data that intelligence agencies must process. To the degree that quantum methods like Grover's algorithm provide a modest (polynomial) speed up for searches, quantum computers can marginally improve search and machine-learning functions. Yet the availability of more information and improved computational throughput also has the potential to create new analytical burdens and confusion.[63] Quantum optimizations will do little to fix, and may even exacerbate, the longstanding challenges of AI, which generally have more to do with the complexity of human judgment and situated interaction than technical implementation.[64] Making sense of secrets will still depend on human analysts who are intuitively familiar with the subject matter and able to discriminate wheat from chaff, detect enemy deception, corroborate SIGINT with other sources of intelligence, and assess the veracity and relevance of the overall intelligence picture.[65] Intelligence success is rarely the result of a single great operation or a lucrative single source. It is almost always the result of a lot of hard work, prior investment, and mundane organizational processes. The intelligence cycle grinds on by virtue of the administrative labor of numerous people over a long period of time.

[63] Kristin M. Lord, *The Perils and Promise of Global Transparency: Why the Information Revolution May Not Lead to Security, Democracy, or Peace* (Albany, NY: State University of New York Press, 2007); Robert Mandel, *Global Data Shock: Strategic Ambiguity, Deception, and Surprise in an Age of Information Overload* (Stanford, CA: Stanford University Press, 2019).

[64] Meredith Broussard, *Artificial Unintelligence: How Computers Misunderstand the World* (Cambridge, MA: MIT Press, 2018); Brian Cantwell Smith, *The Promise of Artificial Intelligence: Reckoning and Judgment* (Cambridge, MA: MIT Press, 2019).

[65] Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca, NY: Cornell University Press, 2011).

The Uncertain Political Impact of SIGINT

Cryptanalysis has indeed helped to change the course of history in a few dramatic cases like the Zimmermann Telegram (which brought the United States into World War I), the Battle of Midway (which devastated the Japanese carrier navy in World War II), and the Battle of the Atlantic (which hastened the defeat of Germany). SIGINT has often been invaluable for warning and targeting in war, especially against targets with poor OPSEC practices such as the Wehrmacht (or the US Army in Vietnam).[66] SIGINT also helped the West to maintain its intelligence advantage over the Soviets throughout the Cold War.[67]

Many other times, by contrast, SIGINT successes have not translated into politico-military advantage. American SIGINT broke Japanese codes before Pearl Harbor, but dysfunctional intelligence–policy arrangements prevented any useful signal from getting through the noise.[68] Edward J. Drea finds that General Douglas MacArthur "consistently dismissed ULTRA evidence that failed to accord with his preconceived vision … . he was willing to ignore intelligence that contradicted that strategic appreciation to which he was committed."[69] Likewise for MacArthur's lieutenants, "when ULTRA challenged [air commander General George] Kenney's cherished belief that air power alone could force the enemy to desert the Admiralties, he simply disregarded the evidence."[70] On the other hand, "MacArthur used ULTRA most effectively when its revelations were in harmony with his fixed ideas of strategy," and "its impact on the air and sea dimensions of the war profoundly affected the conduct of operations."[71] Moreover, "ULTRA guided Kenney's air operations with a higher degree of consistency than it did the ground campaigns."[72] SIGINT thus can be more useful against some types of targets than others, and some decision makers can be more or less likely to pay attention to it.

If the impact of cryptology on war is indeterminate, then the realm of diplomacy is even more ambiguous. According to David Alvarez, "signals intelligence would have little appreciable impact on American diplomacy in the period 1930–1945."[73] American SIGINT agencies understood their success as "a function of the number of cryptosystems broken and messages

[66] R. A. Ratcliff, *Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers* (New York: Cambridge University Press, 2006).

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

[68] Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962).

[69] Edward J. Drea, *MacArthur's ULTRA: Codebreaking and the War against Japan, 1942–1945* (Lawrence: University Press of Kansas, 1992), 230. ULTRA was the code name for the most sensitive Allied SIGINT.

[70] Ibid.

[71] Ibid., 231.

[72] Ibid., 232.

[73] David Alvarez, *Secret Messages: Codebreaking and American Diplomacy, 1930–1945* (Lawrence: University Press of Kansas, 2000).

read. Codebreakers were usually indifferent to the content of the messages."[74] President Franklin D. Roosevelt, meanwhile, was often not interested in decrypts: "Arlington Hall's successes against dozens of foreign codes remained largely invisible to the White House."[75] Roosevelt's curious indifference toward SIGINT stands in stark contrast to Winston Churchill's voracious appetite for ULTRA.[76] Policymaker personality and strategic context are important conditions on the political impact of intelligence.

These historical vignettes highlight features of the intelligence process that are unlikely to change just because the technology of cryptology changes. Once a SIGINT organization has produced valuable and vetted intelligence, the product must be delivered to a cleared, interested, and available customer. Intelligence consumers—military commanders or civilian policymakers—must be open to receiving new information that can inform a decision, and they have to trust the intelligence professionals providing the data. Bias or disinterest will reduce the policy relevance of the intelligence signal. Politicization may suppress or redirect it altogether.[77] A myriad of intelligence–policy pathologies arise from bureaucratic and political incentives to undermine or distort a SIGINT coup. Even in the best of circumstances, customers face cognitive challenges of their own in making sense of intelligence amidst all the other forms of information flooding in.

In the case of time-sensitive current intelligence, customers need to receive and make sense of it before it goes stale (or is "overcome by events"). Other historical data can still be useful for problems in which the target is unlikely to alter its behavior in such a way as to invalidate the intelligence between the moment of collection and the moment of application. According to intelligence historian Michael Warner, the Venona trove of KGB documents "acted as a sort of Rosetta Stone for Western counterintelligence for decades to come."[78] Any data that is protected by a vulnerable protocol like RSA and harvested by an adversary before the target's transition to post-quantum cryptology (PQC) or quantum key distribution (QKD) will thus still be able to be decrypted after the emergence of a large-scale quantum computer.[79] As this interval shrinks and the data exposed becomes stale, it is reasonable to assume that the political danger of revelation will diminish. Almost everything about intelligence advantage is indirect and contextual.

[74] Ibid., 233.

[75] Ibid., 240.

[76] F. H. Hinsley, "British Intelligence in the Second World War: An Overview," *Cryptologia* 14, no. 1 (January 1990): 1–10.

[77] Rovner, *Fixing the Facts*.

[78] Warner, *The Rise and Fall of Intelligence*, 153.

[79] Michele Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" *IEEE Security & Privacy* 16, no. 5 (September/October 2018): 38–41.

The political impact of intelligence ultimately depends on strategic interaction between organizations. If action based on sensitive sources creates suspicion for the target that its communications have been compromised, then the target is likely to alter OPSEC behavior to preclude future exploitation. Fearing the loss of future information, intelligence producers and consumers might decide that the operational gains from acting on intelligence do not outweigh the potential losses to future intelligence. A cryptanalytic advantage that remains unrealized or latent cannot impact current interactions and must be discounted for the future, which is inherently uncertain. If intelligence does influence a decision, it will be difficult to determine whether it has actually made a difference in any given case. Complexity and nonlinear feedback complicate even the most reasonable decisions.[80] Although there are important applications of quantum computing in the early stages of the intelligence cycle—technical decryption prior to all-source analysis—it is unlikely to offer any additional advantage for the dissemination and application of intelligence. In sum, the marginal advantages of quantum computing for the SIGINT attacker are conditional on a nontrivial amount of organizational effort.

Code-Making with Quantum-Safe Cryptography

I now turn to the defender's perspective. If quantum computing offers a cryptanalytic advantage against current asymmetric protocols (RSA, DH), then the obvious defensive response is to switch to quantum-safe substitutes. There are two basic alternatives. First is to look to quantum mechanics itself for a defense against quantum computing. Quantum communications is a different class of technology with lower implementational hurdles compared to quantum computing. Nevertheless, building a quantum network at scale presents many of its own formidable challenges. Second is to adopt different mathematical protocols for PKI that are invulnerable to both quantum and classical attack. Such "post-quantum cryptography" is already available, but the implementation of new protocols across all of cyberspace is, again, a nontrivial problem. The upgrade of critical cryptosystems inevitably presents a host of organizational, economic, and regulatory problems in excess of any scientific uncertainty about the robustness of the protocols. If the implementation problems associated with quantum communications and PQC are not overcome, and if the attacker acquires a working quantum computer, then the SIGINT attacker might indeed gain an advantage, conditioned on its organizational practice as discussed above. Yet even if the defensive implementation and adoption

[80] Robert Jervis, *System Effects: Complexity in Political and Social Life* (Princeton, NJ: Princeton University Press, 1997); Richard K. Betts, "Is Strategy an Illusion?" *International Security* 25, no. 2 (Fall 2000): 5–50.

problems are solved, the target is still not out of the woods. If the members of the target organization fail to properly implement the new protocols against a creative and determined attacker, then OPSEC will still fail. As information security experts are fond of pointing out, there is no patch for human stupidity.

The End of Intelligence?

If quantum mechanics threatens classical cryptographic security, it can also be leveraged to create new quantum protocols that are, so to speak, secure by the laws of physics. QKD exploits the fact that perfect copying of arbitrary quantum data is not possible by the "no-cloning theorem."[81] QKD thus makes it possible to detect the presence of an eavesdropper through an increase in error rates. QKD can be used to securely distribute unique symmetric keys between geographically separated parties, which has always been a major practical challenge for security organizations (and an important historical motivation for developing asymmetric cryptography). The practical feasibility of QKD over large distances has been demonstrated in numerous experiments since the first proof of concept in 1994, the same year Shor presented his famous algorithm.[82]

However, quantum computing does not pose a categorical threat to all classical cryptography. As mentioned above, quantum computing only provides speedups for problems that can be solved with quantum algorithms. If different mathematical problems can be found that do not admit an easy quantum solution, then the security motivation for using quantum networks is much reduced (even as there may be other communication benefits).[83] The US National Institute of Standards and Technology (NIST) is currently evaluating PQC alternatives to core cryptographic primitives. PQC protocols use different mathematical constructs to generate digital keys that are extremely hard to discover using either classical or quantum cryptanalysis, yet easy to verify with classical methods.[84] More generally, quantum computing has spurred theorists to innovate in classical algorithms, with efficiency gains catching up to quantum methods in some cases.[85] Fears of offensive

[81] Charles H. Bennett and Gilles Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (Bangalore, India 1984), 175–79.

[82] P. D. Townsend, "Secure Key Distribution System Based on Quantum Cryptography," *Electronics Letters* 30, no. 10 (May 1994): 809–11.

[83] Cryptographer Tom Berson quips that QKD is "a new, difficult, expensive way to achieve an outcome which we have, for decades, been achieving easily and cheaply." Tom Berson, @nd2t, Twitter, 23 July 2019, 4:30 pm, https://twitter.com/nd2t/status/1153779489639239681.

[84] Lily Chen et al., "Report on Post-Quantum Cryptography" (Gaithersburg, MD: National Institute of Standards and Technology, April 2016).

[85] Edwin Pednault et al., "Breaking the 49-Qubit Barrier in the Simulation of Quantum Circuits," *arXiv* 1710.05867 [quant-ph], 16 October 2017, http://arxiv.org/abs/1710.05867; Alex Neville et al., "No Imminent Quantum Supremacy by Boson Sampling," *Nature Physics* 13, no. 12 (December 2017): 1153–57.

advantage often catalyze defensive innovation, just as the belief that the bomber would always get through in the 1930s encouraged the Royal Air Force to build the air defense system that won the Battle of Britain.[86] Quantum cryptanalysis is something of a self-denying prophesy in this regard because it encourages scientists and states to develop quantum-safe alternatives like PQC and QKD.

Engineering Challenges in Quantum Communications

The engineering challenges of quantum communication are perhaps less formidable than those associated with general-purpose quantum computing, but they are still significant. 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. Large-scale quantum networks will require the further innovation of reliable quantum repeater and memory devices that do not destroy quantum state.[87]

QKD protocols provide absolute theoretical security for only one part of a communication link. An attacker might still monitor side channels in physical implementations of QKD that leak information. Penetration experiments have successfully targeted both the photon sources and detectors of commercial QKD systems.[88] A promising alternative protocol known as measurement-device-independent QKD is claimed to be "inherently immune to all side-channel attacks targeting the measurement device, usually the most vulnerable part in a QKD system."[89] The more sophisticated protocols are slow, however, and, importantly, they still assume that eavesdroppers do not have access to the preparation of photons. Large-scale quantum networks, moreover, still must rely on trusted intermediate repeaters and other nodes that, currently, still depend on classical components.[90] This is a familiar story: the endpoints are often the weak links in any secure communication system. A further assumption is that QKD communicators have an authenticated classical channel they use in generating the private key. QKD is thus not immune to so-called man-in-the-middle attacks. The attacker can also jam the QKD link by simply

[86] David Zimmerman, *Britain's Shield: Radar and the Defeat of the Luftwaffe* (Stroud, UK: Amberley Publishing, 2001).

[87] Eleni Diamanti et al., "Practical Challenges in Quantum Key Distribution," *Npj | Quantum Information* 2 (8 November 2016): 16025; Christoph Simon, "Towards a Global Quantum Network," *Nature Photonics* 11, no. 11 (November 2017): 678–80; Stephanie Wehner, David Elkouss, and Ronald Hanson, "Quantum Internet: A Vision for the Road Ahead," *Science* 362, no. 6412 (19 October 2018): eaam9288; Acín et al., "The Quantum Technologies Roadmap."

[88] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki, "Secure Quantum Key Distribution," *Nature Photonics* 8, no. 8 (August 2014): 595–604.

[89] Diamanti et al., "Practical Challenges in Quantum Key Distribution," 6.

[90] Wehner, Elkouss, and Hanson, "Quantum Internet."

monitoring it, since its intervention effectively creates random results for the receiver. QKD as such provides no protection against service denial attacks; indeed, QKD even enables new forms of it (insofar as tapping a quantum link effectively jams it).

QKD provides absolute security for only one link in a cryptosystem, which on the whole can only be relatively secure. A quantum network must be able to scale up if it is to be useful for large distributed organizations in the modern economy or for military operations across large geographical domains. Quantum networks need quantum repeaters and quantum memory devices that preserve coherent quantum state. These devices must deal with the error-correction problems discussed above. Alternately, quantum communications networks can be broken down into shorter links connected by nodes operating on classical principles, which is what China has done with its Beijing–Shanghai network. Yet the connective nodes rely on additional nonquantum means that remain vulnerable to a sophisticated attacker. More complex protocols often create opportunities for more devious attacks. The whole system can never be perfectly secure because any communication network is a sociotechnical assemblage of humans and machines, let alone of classical and quantum components.

Chinese achievements to date have been concentrated in quantum communications rather than quantum computing, which by contrast is more advanced in North America and Europe.[91] These two categories of technology must not be conflated. Chinese progress in quantum encryption does not imply that Chinese intelligence agencies are on the verge of a SIGINT revolution. China's interest in quantum communication is a function of its technonationalist aspirations to achieve scientific breakthroughs, amplified by paranoia about the insecurity of Chinese networks encouraged by the Snowden leak and Stuxnet attack, which both highlighted American SIGINT prowess. Quantum informatics is accordingly listed as one of the key breakthrough projects in China's 13th Five Year Plan of National Technology and Innovation released in March 2016, and China intends its National Laboratory for Quantum Information Science to be the world's largest quantum research facility.[92] In summer 2017 the Chinese Quantum Experiments at Space Scale satellite, also known as Micius, demonstrated the ability to maintain particles in an entangled state via satellite link, followed by an intercontinental satellite transmission test in January 2018.[93] Like Sputnik in an earlier era, the "Micius moment" has been a wake-up

[91] For a thorough review of Chinese aspirations and progress in quantum technology, see Kania and Costello, "Quantum Hegemony?"

[92] Stephen Chen, "China Building World's Biggest Quantum Research Facility," *South China Morning Post*, 11 September 2017.

[93] Davide Castelvecchi, "China's Quantum Satellite Clears Major Hurdle on Way to Ultrasecure Communications," *Nature News*, 15 June 2017.

call for those who believe US scientific and military advantage is in jeopardy.[94] It is notable, however, that eleven of the twelve recipients of the first annual Micius Prize, created by a Chinese foundation to recognize excellence in quantum science, hailed from North America or Europe rather than China.[95] It is far from obvious that China is destined to lead in quantum communications. Whoever the leader turns out to be, moreover, will still not be able to close all vulnerabilities.

Engineering Challenges in Post-Quantum Cryptography

The prognosis for classical PQC is perhaps more optimistic. In the United States, 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."[96] NIST reported in 2018 that it had received sixty-nine "complete and proper" submissions from 25 countries for its PQC competition, and evaluations continue as of this writing, with the goal of certifying new public standards within the next few years.[97] It is also notable that the National Security Agency (NSA) has announced that it "will initiate a transition to quantum resistant algorithms in the not too distant future."[98] One indication of NSA's confidence in the near-term viability of PQC is that it has recommended not adopting strong elliptic curve cryptography but rather waiting for PQC.[99]

The PQC transition will be complicated, to be sure. Widely implemented PQC may be a decade away as of this writing. It will take NIST several years to issue PQC standards. Big firms and government agencies may be able to swap in new protocols relatively quickly for some applications where they deem security a high priority. Others will require more time and effort to avoid configuration conflicts and preserve backward compatibility. Some organizations and software developers will simply neglect upgrading protocols for the sake of convenience (or due to negligence). Yet compared to a potential transition to the radically different architecture of large-scale QKD, the transition of legacy PKI to asymmetric PQC appears

[94] For instance, C. L. Max Nikias, "This Is the Most Important Tech Contest since the Space Race, and America Is Losing," *Washington Post*, 11 May 2018.

[95] David Cyranoski, "Chinese Quantum Prize Rewards International Stars of the Field," *Nature*, 29 April 2019.

[96] 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/news/2016/public-key-post-quantum-cryptographic-algorithms.

[97] Dustin Moody, "Let's Get Ready to Rumble: The NIST PQC 'Competition,'" 9 April 2018, https://csrc.nist.gov/Presentations/2018/Let-s-Get-Ready-to-Rumble-The-NIST-PQC-Competiti.

[98] Bruce Schneier, "NSA Plans for a Post-Quantum World," *Lawfare* (blog), 21 August 2015, https://www.lawfareblog.com/nsa-plans-post-quantum-world.

[99] "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," as quoted in Ibid.

to be much more feasible. PQC will likely mature and become widely available well before reliable quantum networks. Nevertheless, if historical experience with the rollout of standards such as AES is suggestive, many systems that remain online will continue to rely on older outdated protocols for years after NIST and the global cryptographic community endorses new ones. Cryptographic security will thus improve in principle but not necessarily in practice.

The Institutional Challenges of OPSEC

We do not have to wait for QKD or PQC to probe the impact of perfect cryptography on IR. The advent of asymmetric PKI in the 1970s and its widespread adoption in the 1990s represented a triumph of cryptographic defense over cryptanalytic offense. SIGINT agencies appeared to be locked out of protocols that they could not break, even with all the resources of the US government. This seemed like a major boon for anyone who wanted to build trusted digital systems for peace or war.

Yet while SIGINT agencies lost some ability to attack cryptography directly, they were still able to mount indirect attacks on cryptosystem implementation. The goal of a SIGINT agency is to gather intelligence, after all, and breaking codes is only instrumental toward that end. Former NSA contractor Edward Snowden observed in 2013 that while PKI was still safe from the NSA, most data were not: "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it."[100] Documents leaked by Snowden also suggest the NSA attempted to influence (weaken) the definition of public cryptographic standards. The NSA also found ways to undermine the cryptosystems of popular technology platforms produced by firms like Google, Facebook, and Microsoft, both with and without their consent.[101] Perfect cryptography does not translate into perfect security so long as SIGINT attackers can find a way to copy data before it gets encrypted, steal cryptographic keys that are stored insecurely, exploit hardware characteristics that betray software operations, or trick gullible users into providing credentials. As one textbook points out, "cryptography is fiendishly difficult … [but] it is still one of the easy parts of a security system."[102] If complexity is the enemy of information security, then the tremendous complexity of global information infrastructure creates many new opportunities for

[100] Edward Snowden, "NSA Whistleblower Answers Reader Questions," *Guardian*, 17 June 2013.
[101] Nicole Perlroth, Jeff Larson, and Scott Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web," *New York Times*, 5 September 2013.
[102] Ferguson, Schneier, and Kohno, *Cryptography Engineering*, 13.

deception.[103] More sophisticated forms of trust only enable more creative ways to abuse it.

Even worse, the very possibility of perfect cryptography encourages organizations and individuals to trust their valuable financial and administrative data to digital networks. This, in turn, provides more targets for the NSA and other agencies to exploit. The availability of strong cryptography can easily provide a false sense of security. Robust PKI has been ubiquitous for the past three decades, and yet organizations and individuals have been hemorrhaging confidential data through the internet. Indeed, SIGINT agencies like the NSA have been enjoying a renaissance in technical collection, in large part because most organizations fail to use strong encryption properly and have poor OPSEC practices. The mathematical strength of an encryption protocol effectively shifts a SIGINT agency's incentives for exploitation to other vulnerabilities in the software, hardware, and organizational implementation of a cryptosystem. Even in a world of strong cryptography, therefore, SIGINT still thrives if OPSEC is weak. It is an unappreciated irony of history that the advent of strong cryptographic security has helped to unleash the current epidemic of cyber insecurity.

On one hand, the advent of QKD and PQC will largely cancel out the cryptanalytic threat that quantum computing creates. On the other hand, quantum and classical systems will still depend on complex implementations by, with, and for human users. Despite all the media attention to major breaches and corporate training in cyber hygiene in recent years, many people are still ignorant, complacent, or unconcerned about cybersecurity. Attackers can still use "social engineering" tricks such as phishing, waterholing, and blackmailing to persuade targets to expose credentials that enable attackers to forge authentication. Sociotechnical complexity and gullible humans can thus be expected to undermine QKD and PQC just as they do strong cryptography today. Undoubtedly, quantum networks will create new complications for foreign intelligence collection and require new kinds of technical expertise at SIGINT agencies. However, it is highly unlikely sophisticated collectors will be locked out of quantum protected systems altogether. More perversely, large-scale quantum networks might further improve public trust in cryptosystems, encouraging actors to trust even more valuable data to computing systems, which would then simply become more attractive targets for SIGINT agencies with the means and moxie to exploit side channels and human weaknesses. Today we are experiencing something of a golden age of cyber espionage, despite, if not because of, the availability of strong cryptosystems. Future defenses based

[103] On the fundamental role of deception in cybersecurity, see Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (April–June 2015): 316–48.

on quantum-safe cryptosystems will, likewise, only be only as good as the people who maintain and employ them.

Quantum of Solace

If technology alone determined intelligence advantage, then a fundamentally different type of information technology—qubit rather than bit—might create radically different strategic outcomes. Yet technology rarely determines anything directly. Quantum computing is an exciting scientific development, to be sure, but it is likely to have little net effect on the political dynamics of intelligence and cybersecurity. Indeed, threat narratives about the end of secrecy and the end of intelligence are wildly exaggerated. The good news is that secrecy will still be possible after the second quantum revolution. The bad news is that intelligence agencies will still be able to penetrate that secrecy. The simple theory presented in this article suggests the challenges of implementing cryptosystems and coordinating organizations tend to make intelligence advantage difficult to realize and extremely difficult to sustain. In the worst-case scenario of a technical breakthrough in quantum computing prior to the adoption of quantum-safe offsets, the idiosyncrasies of social organization and strategic interaction can still be expected to prevent quantum cryptology from reaching its full potential. Human organizations will still find ways to fumble the technical potential for improved SIGINT and OPSEC.

Intelligence contests in the future will probably become even more complex than they already are, and not simply because of quantum computing. Advanced information technologies of any sort will be introduced and employed within a complex, global, ambiguous, and evolving sociotechnical system. China will continue to play catch-up to the leaders in quantum technology in North America and Europe. Powerful countries will maintain advantages in cyberspace through their capable SIGINT agencies and leading information technology firms. Many classical information technologies will continue to be used in the ostensibly quantum future because of widespread legacy dependency on them. New patches will be layered over old architecture to compensate for flaws as they are discovered. Whatever advantages are to be gained through quantum technologies will be blunted by the maturation of competing offensive and defensive quantum capabilities, the anticipatory action by industry and government to counteract or compensate quantum advantages, and all the inevitable frictions in the infrastructure of quantum computing.

For the same reasons, network defenders and cyber warriors will have to contend with quantum technologies as an inevitably complicating feature of their operational domain. The future of cyberspace, with all its heterogeneous infrastructures and overlapping institutions, will keep providing more ways and means for more types of actors to pursue deceptive ends. Tactics of espionage, disinformation, covert action, subversion, and sabotage will continue to be attractive for many actors in a world of complex interdependence, even as the results will continue to be ambiguous. Quantum technology can be expected to inject more friction into an already complex web of dynamic intelligence contests. For SIGINT practitioners and their targets who must cope with all that friction, this is cold comfort.

It is perhaps fitting that a speculative study should end on a speculative note. The concepts of information and technology have an intimate relationship to one other and to the broader political world. Computing technology and cryptology have become indispensable in the conduct of war and the management of peace. These technologies owe a major debt to information theory, the basic principles of which were first described in a wartime study of cryptography by Claude E. Shannon.[104] War shaped modern cryptology historically, even as cryptology shapes modern conflict today. Information theory has also informed the game-theoretical models at the heart of modern IR theory, which highlight uncertainty as an important cause of war. Political scientists are thus coming to appreciate the fundamental importance of information in politics at the same time as physicists and computer scientists are beginning to rethink the fundamental concepts of information and computation. As quantum computing prompts a reimagining of information theory, is it possible that cryptology could once again become a generative source of political theory? Might the logic of intelligence help illuminate the nature of security competition in a world of complex interdependence? If so, then quantum computing may ultimately prove more interesting for IR in theory than practice.

Acknowledgements

The author is grateful for helpful discussion and comments on previous drafts from Jonathan Caverley, Allan Dafoe, Brendan Green, Austin Long, David Meyer, Dustin Moody, Neil Narang, Jacquelyn G. Schneider, Michael Warner, participants of the Emerging Technologies and Strategic Stability workshop at Stanford University, the Q Symposium on Quantum Computing, Communication, Control, and Intelligence at the University of Sydney, the State of the Art of Cybersecurity and Cyberconflict Research Conference at ETH Zurich, and several anonymous reviewers, as well as for research assistance from Jinhui Jiao, Ryder McKeown, and Nicola Plummer.

[104] Claude E. Shannon, “A Mathematical Theory of Cryptography,” technical report (Bell Labs, 1 September 1945).