The Quantum Decryption Offset—Defend, Deny, Discover

A Strategic Framework for Offsetting Enabling Technologies in an Era of Integrated Deterrence

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
25-02-2022	FINAL	N/A

4. TITLE AND SUBTITLE

The Quantum Decryption Offset—Defend, Deny, Discover: A Strategic Framework for Offsetting Enabling Technologies in an Era of Integrated Deterrence

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

LCDR Schrodt, Kevin

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Writing & Teaching Excellence Center
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the curriculum. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Integrated Deterrence includes offsetting adversary enabling-technology development. The rules-based world order faces a revisionist adversary in China and the emergence of dual-use enabling technologies—suitable for civilian use and military advantage. Examples include artificial intelligence, 5G, nanotechnology, and quantum computing. The latter can theoretically break the encryption that secures the internet, critical infrastructure, and financial systems. The U.S.-China relationship is also dual-use—a country with whom the U.S. wants to trade and invest, but a competitor militarily and economically. The technological progress of quantum computing is inevitable, and through it, quantum decryption poses an existential threat to the rules-based world order if weaponized by China. Fortunately, protection is possible. Post-quantum cryptography (PQC) defends classical information systems from quantum decryption. PQC is in development, as is the quantum computer. Thus, the United States requires a technology offset strategy in the Indo-Pacific to protect classical information systems and deny China their desired outcomes from quantum decryption. To achieve this end, the author proposes a system of three interdependent strategic pillars to defend allies and the U.S., deny China access to technology solutions, and discover international and bilateral collaboration opportunities. Defend—Deny—Discover transcends offsetting quantum decryption; it serves as an exemplar to address enabling technologies within a greater Integrated Deterrence framework.

15. SUBJECT TERMS (Key words)
Quantum, emerging technology, decryption, integrated deterrence, China, Indo-Pacific

16. SECURITY CLASSIFICATION OF:	**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
			Director, Writing Center

a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	N/A	15	401-841-6499

Standard Form 298 (Rev. 8-98)

Introduction

The rules-based world order faces a revisionist adversary in China and the emergence of dual-use enabling technologies—suitable for civilian use and military advantage. Examples include artificial intelligence, 5G, nanotechnology, and quantum computing. The latter theoretically can break the encryption that secures the internet, critical infrastructure, and financial systems. Advancing quantum computing is a resource-intensive endeavor, achievable only through national-level laboratories, large corporations, or well-funded research institutions. Its technological progress is inevitable. Quantum decryption poses an existential threat to the rules-based world order if weaponized by China. Fortunately, protection is possible. Post-quantum cryptography (PQC) defends classical information systems from quantum decryption.[1] PQC is in development, as is the quantum computer. The U.S.-China relationship is also dual-use—a country with whom the U.S. wants to trade and invest, but a competitor militarily and economically.

The United States requires a technology offset strategy in the Indo-Pacific to protect classical information systems and deny China their desired outcomes from quantum decryption. To achieve this end, the author proposes a system of three interdependent strategic pillars designed to defend allies and the U.S., deny China access to technology solutions, and discover international and bilateral collaboration opportunities. This is Integrated Deterrence in reality. [2]

Background

---

[1] Bernstein, D. J. and T. Lange. "Post-Quantum Cryptography." *Nature (London); Nature* 549, no. 7671 (2017): 88-194. doi:10.1038/nature23461. https://usnwc.primo.exlibrisgroup.com/permalink/01USNWC_INST/ouaji3/cdi_proquest_miscellaneous_1938850072. 188.

[2] Lloyd Austin, "Global Emerging Technology Summit," National Security Commission on Artificial Intelligence (public remarks, online video, July 13, 2021). https://youtu.be/MkJs-eRPABg?t=30210. The link will take the reader directly to Secretary Austin's remarks at 8:23::30 where he defines Integrated Deterrence as the proper synchronization of technology, operational concepts, and capabilities alongside partners and allies to prevent conflict.

Quantum computing is part of a larger multidisciplinary field known as Quantum Information Science (QIS). Other areas of study include sensors, communication, and simulation. The quantum aspect leverages sub-atomic particles (e.g., photons) and associated quantum mechanical properties like entanglement, superposition, and coherence.[3] QIS, especially quantum computing, has experienced a global boom in research and development due to the dual-use economic and national security opportunities.

A quantum computer's capacity for rapidly factoring large numbers is an application of significant interest to national security. Classical computing systems operate through a binary framework (bits)—0s and 1s. However, a quantum computer relies on superposition to use 0s and 1s simultaneously (qubits), exponentially increasing processing power as the number of qubits increases.[4] Quantum computers will not replace classical computers; everyday tasks do not require such a purported level of computing power. That said, quantum computing can optimize some tasks currently accomplished by classical computers. For example, an area of economic interest is the capacity to search massive databases rapidly (e.g., optimizing the global supply chain).[5] For national security, though, the most urgent threat is decryption via a quantum computer.

Quantum computers will make decryption a reality due to the inevitability of technological advancement.[6] A computer's inability to solve a math problem in an acceptable

---

[3] Moloney Figliola, Patricia. *Quantum Information Science: Applications, Global Research and Development, and Policy Considerations*. Washington, D.C.: Congressional Research Service, 2019. https://crsreports.congress.gov/product/pdf/R/R45409. 1.

[4] *Ibid.*

[5] Nielsen, Michael A. and Isaac L. Chuang. *Quantum Computation and Quantum Information*. 10th anniversary ed. Cambridge ;New York: Cambridge University Press, 2010. 7.

[6] Grobman, Steve. "Quantum Computing's Cyber-Threat to National Security." *Prism (Washington, D.C.)* 9, no. 1 (2020): 52-67. https://usnwc.primo.exlibrisgroup.com/permalink/01USNWC_INST/ouaji3/cdi_proquest_journals_2455929484 . 57.

timeframe is the underlying principle for encryption in the public domain, especially the internet (e.g., https://). It could take a classical system 10,000 years to solve the math problem that 'unlocks' the data, whereas quantum computers theoretically perform the calculation in minutes.[7] 'Theoretically' is the keyword. The limiting factor is scaling the number of qubits; a quantum computer requires tens of thousands, if not millions, of qubits to decrypt data successfully.[8] The most capable quantum computer to date implements 256 qubits.[9] Quantum decryption will be a reality, but it is unclear when.

PQC can protect classical systems against quantum decryption threats. PQC comprises security protocols for classical systems designed to resist quantum decryption. The U.S. National Institute of Standards and Technology (NIST) leads a global competition to identify the strongest PQC candidate.[10] Once selected, the intent is to proliferate this quantum protection openly. The urgency? Historically, it has taken upwards of two decades to deploy public-domain encryption infrastructure.[11]

The race is technical between PQC proliferation and developing a quantum computer capable of decryption. If China achieves quantum decryption before the PQC security protocols are ubiquitous across all systems, they will "tighten their grip to better determine their own

---

[7] *Ibid.,* 59

[8] Li, Kai, Pei-Gen Yan, and Qing-Yu Cai. "Quantum Computing and the Security of Public Key Cryptography." *Fundamental Research* 1, no. 1 (2021): 85-87. doi:10.1016/j.fmre.2020.12.001. https://usnwc.primo.exlibrisgroup.com/permalink/01USNWC_INST/ouaji3/cdi_crossref_primary_10_1016_j_fmre_2020_12_001. 85.

[9] This article from *The Harvard Gazette* describes the accomplishment and is followed by the peer-reviewed publication confirming the work: Siliezar, Juan. "Harvard-Led Physicists Take Big Step in Race to Quantum Computing." *The Harvard Gazette,* July 7, 2021, Science and Technology. https://news.harvard.edu/gazette/story/2021/07/harvard-led-physicists-create-256-qubit-programmable-quantum-simulator/. Ebadi, S., Wang, T.T., Levine, H. *et al.* Quantum phases of matter on a 256-atom programmable quantum simulator. *Nature* 595**,** 227–232 (2021). doi:10.1038/s41586-021-03582-4.

[10] "NIST Advances Post-Quantum Cryptography." *Signal* 73, no. 7 (2019): 7. https://usnwc.primo.exlibrisgroup.com/permalink/01USNWC_INST/ouaji3/cdi_proquest_reports_2197774530.

[11] "Post-quantum cryptograpy," Computer Security Resource Center, Accessed October 9, 2021, https://csrc.nist.gov/projects/post-quantum-cryptography.

geopolitical destiny" by exploiting the information environment through a protracted campaign of manipulation and influence.[12] The strategic framework contained herein is push-pull. The push—get PQC protocols on every classical system. The pull—slow China's progress in advancing quantum computing.

Defend, Deny, Discover

The objective of the quantum decryption offset is to make PQC security protocols ubiquitous across all classical systems globally, including China. The U.S. and China enjoy interleaved economic interests. Both see value and benefit in continued trade and investment. Nevertheless, one cannot deny the competitive relationship between the two most significant economies in the world. The offset specifically targets China because they present the greatest threat to the rules-based world order through increasingly aggressive behavior.

The quantum decryption offset is a system—a group of interdependent elements[13]—designed to holistically address the global proliferation of PQC before quantum computing becomes viable. The pillars do not stand alone, as the outcomes from one mitigate the risks of another. First, Defense through Partnership seeks to assist partners in the Indo-Pacific through technology policy advice and to facilitate security cooperation activities for implementing PQC across critical infrastructure. Second, Denial of Technology Artifacts prevents China from acquiring quantum computing platforms that advance quantum decryption. Finally, Discovery

---

[12] Grobman, Steve. "Quantum Computing's Cyber-Threat to National Security." *Prism: A Journal of the Center for Complex Operations* 9, no. 1 (2020): 52-66. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fquantum-computings-cyber-threat-national-security%2Fdocview%2F2455929484%2Fse-2%3Faccountid%3D322. 64.

[13] Merriam-Webster Online, s.v. "System," Accessed October 12, 2021, https://www.merriam-webster.com/dictionary/system.

through Collaboration advocates for strengthened U.S.-China ties and international collaboration that seeks a global PQC implementation plan.

Defense through Partnership

The first pillar of the strategic framework is Defense through Partnership. The United States must undertake quantum security cooperation and build capabilities alongside allies in the Indo-Pacific, where quantum research permeates the region. Offsetting quantum decryption through defense succeeds when the U.S. and partners present an equally defensive cybersecurity front-line replete with PQC security protocols. In 2019, China, Japan, South Korea, and India were among the top ten quantum research and development countries.[14] Other countries in the region have active quantum science programs.[15] The cyber domain provides quantum decryption's target—encryption and the protected data, where all countries in the Indo-Pacific are vulnerable to China cyberattacks. A 2019 Rand Report identified that "even wealthy and technologically advanced countries…such as Japan and South Korea, have major [cybersecurity] gaps to fill."[16] During the President's address to the United Nations in September 2021, President Biden stated that the U.S. will pursue relentless diplomacy "to shape rules of the world on vital issues like…cyber and emerging technologies."[17] Defense through Partnership takes a top-down/bottom-up approach to account for the varying levels of quantum expertise in the Indo-

---

[14] Srivastava, Smriti. "Top 10 Countries Leading in Quantum Computing Technology," *Asia Europe Latest News North America.* December 14th, 2019. https://www.analyticsinsight.net/top-10-countries-leading-quantum-computing-technology/.

[15] For instance, Singapore: https://quantumsg.org/. And Australia: https://ia.acs.org.au/article/2021/demystifying-australia-s-quantum-potential.html.

[16] Harold, Scott W., Derek Grossman, Brian Harding, Jeffrey W. Hornung, Gregory Poling, Jeffrey Smith, and Meagan L. Smith, *The Thickening Web of Asian Security Cooperation: Deepening Defense Ties Among U.S. Allies and Partners in the Indo-Pacific*. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR3125.html. 350.

[17] Joseph Biden, Jr., *Remarks by President Biden Before the 76th Session of the United Nations General Assembly.* The White House Briefing Room. September 21, 2021. https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/09/21/remarks-by-president-biden-before-the-76th-session-of-the-united-nations-general-assembly/.

Pacific. It seeks to inform partners at the policy level and integrate PQC protocols and quantum expertise into the cybersecurity infrastructure. At the policy level, the Embassy Science Fellows Program, administered through the DOS Office of Science and Technology Cooperation, could establish a persistent position for an American QIS expert to be posted at U.S. Embassies in the Indo-Pacific. This Fellow would come from a U.S. government science agency to advance quantum policy and scientific priorities. Japan or Australia offers an immediate opportunity because the U.S. shares formal quantum cooperation agreements with each country.[18] Of utmost importance would be to facilitate the development of country-specific PQC implementation plans, presenting future avenues for U.S. cyber-security cooperation.

The U.S. could leverage Title 10 DOD security cooperation funding and resources alongside the Embassy Fellow's efforts. DOD has a vast quantum research base through service-oriented research labs, university partnerships, and defense support agencies.[19] However, DOD must identify and align personnel with quantum skillsets to augment assigned forces during security cooperation engagements to provide quantum expertise. DOD should explore integrating QIS experts from these research labs with security cooperation forces to accelerate the proliferation of PQC protocols. Cybersecurity is a recognized weakness throughout the Indo-Pacific.

Furthermore, the roll-out of a PQC architecture is coming, and cyber-security cooperation with foreign partners is a nascent initiative in the DOD. In August of 2021, General Nakasone—

---

[18] On December 19, 2020, the U.S. and Japan issued a joint statement of cooperation "to advance innovative and emerging quantum information science and technology." https://www.state.gov/tokyo-statement-on-quantum-cooperation/. On September 15, 2021, Australia, the UK, and the U.S. announced a trilateral partnership that includes cooperation in the field of quantum technologies. https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/15/joint-leaders-statement-on-aukus/.

[19] Service research laboratories include Air Force- https://afresearchlab.com/. Navy- https://www.nrl.navy.mil/. Army- https://www.arl.army.mil/. DOD-wide S&T efforts are administrated through the OUSD for Research and Engineering- https://www.cto.mil/.

Commander of USCYBERCOM—signed a memorandum of understanding with Singapore "designed to expand cooperation...in cyberspace."[20] It behooves DOD to formalize a requirement that integrates quantum experts with cybersecurity operational forces to assist allies with PQC implementation, subsequently offsetting quantum decryption against critical infrastructure throughout the Indo-Pacific. Sharing knowledge through a top-down, bottom-up approach facilitates understanding when the U.S. needs international consensus for the next strategic pillar—Denial through Technology Artifact Controls.

Denial through Technology Artifact Controls

The U.S. should internally enact export controls and externally petition international organizations to limit the dissemination of technology artifacts that advance quantum decryption. Offsetting quantum decryption through denial succeeds when China cannot reap the benefits from the U.S. and other quantum-productive countries.

Countries in favor of the current rules-based world order are building the platforms that a revisionist, rising power will use. China leads in patenting quantum computing applications—they are patenting ideas that do not yet have an artifact from which to execute the application.[21] Not to be confused with artifacts, an application is to WhatsApp as an artifact is to the smartphone. In 2017, a Patinformatics, LLC report identified "approximately 76% of the academic patent families published in the field of quantum applications since 2012 have been from Chinese Universities."[22] In contrast, the U.S. and Japan historically outpace China in

[20] https://www.cybercom.mil/Media/Images/igphoto/2002840336/.
[21] Grobman, Steve. "Quantum Computing's Cyber-Threat to National Security." *Prism: A Journal of the Center for Complex Operations* 9, no. 1 (2020): 52-66. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fquantum-computings-cyber-threat-national-security%2Fdocview%2F2455929484%2Fse-2%3Faccountid%3D322. 59.
[22] U.S. universities are a distant second at 14%. Statistics found in the following report: Scanlon, Bryan and Anthony Trippe. *Quantum Computing Applications: A Patent Landscape Report*. Patinformatics, LLC, 2017.

discovering, designing, and engineering quantum computing platforms.[23] When confronted by controlling an emerging, dual-use, enabling technology, a consideration arises: how to determine what needs to be controlled?

The U.S. needs to establish a national security review process to analyze China's patents and academic publications that advance quantum computing applications. A potential contributor to this effort is the Department of Energy (DOE), which possesses resources and an adequate QIS knowledge base to perform the requisite analysis. As a principal member of the National Quantum Initiative Act (NQIA)[24], DOE has established five National QIS Research Centers across various national laboratories, including universities and private corporations.[25] If an application from China advances quantum decryption, then an appropriate control mechanism—under the Export Control Reform Act of 2018 (ECRA)[26]—should be identified. This action would prevent China from acquiring an existing, capable technology artifact from the U.S. Also, the U.S. should work to influence the international community through the Wassenaar

---

https://assets.website-files.com/6124f9f348fc634f20bb900c/612d4345603b5e31b0e84347_Quantum-Applications-Patent-Landscape-Report.pdf. Slide 7.

[23] Scanlon, Bryan and Anthony Trippe. *Quantum Computing Highlights: A Patent Landscape Report*. Patinformatics, LLC, 2017. https://assets.website-files.com/6124f9f348fc634f20bb900c/612d35bb9f499955ffa6eaf4_Quantum_Computing_Highlights_Final_opt.pdf . Slide 3.

[24] National Quantum Initiative Act of 2018, Public Law 115-368, 115th Cong., (December 21, 2018). https://www.congress.gov/115/plaws/publ368/PLAW-115publ368.pdf. The NQIA was signed into law on December 21, 2018 to provide for a coordinated Federal program to accelerate quantum research and development for the economic and national security of the United States.

[25] "National QIS Research Centers," Office of Science, U.S. DOE, Accessed October 9, 2021, https://science.osti.gov/Initiatives/QIS/QIS-Centers.

[26] Export Control Act of 2018, Public Law 115-232, 115th Cong., (August 13, 2021). https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf. 132 STAT. 2198.

Arrangement (WA)[27] to control like-artifacts from their own countries.[28] Both the ECRA and WA include allowances for controlling QIS technologies.

Despite the evident need for them, such controls could come at a cost. First, if the U.S. controls its technology base, it could be creating a global need that China would potentially fill.[29] Furthermore, some might argue that controlling the proliferation of nascent and emerging technologies unnecessarily hinders much-needed civilian use-cases; thus, export controls are detrimental to economic prosperity.[30] In reply to both concerns, the controls would have a shelf-life. Remember—the rules-based world order is racing to implement PQC security protocols across classical systems before possible quantum decryption. Therefore, denying technology-artifact solutions offsets China's progress towards that end. The controls will lift once PQC is ubiquitous. The concerns are valid; building trust throughout the international community will be necessary, making the third strategic pillar all the more critical—Discovery through Collaboration.

Discovery through Collaboration

The U.S. should collaborate with the international community to accelerate PQC implementation and pursue academic quantum science collaboration with China. In his first public address as Secretary of State, Antony Blinken posits, "Our relationship with China…will

---

[27] "List of Dual-Use Goods and Technologies and Munitions List," *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, Public Documents, Volume II, December 2019, https://www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-PUB-002-Public-Docs-Vol-II-2019-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-19.pdf.

[28] Of note, the U.S. and five countries from the Indo-Pacific—Australia, Japan, India, New Zealand, Republic of Korea—are participating members in the WA. https://www.nti.org/learn/treaties-and-regimes/wassenaar-arrangement/.

[29] Kathleen A. Walsh, email message to author, October 11, 2021.

[30] Jones, Scott A. "Trading Emerging Technologies: Export Controls Meet Reality." *Security and Human Rights* (2021): 1-13. doi:10.1163/18750230-31010004. https://usnwc.primo.exlibrisgroup.com/permalink/01USNWC_INST/ouaji3/cdi_crossref_primary_10_1163_18750230_31010004. 11.

be collaborative when it can be."[31] Foremost, collaboration is about the human element. People-to-people engagements help grow cultural awareness and mutual trust while broadening perspectives. This paper presents two options for collaboration.

First, the U.S. should lead the formation of a U.N. organization that accelerates PQC implementation. Making PQC security protocols ubiquitous throughout classical systems depends on international support because the cyber domain is without national borders. Quantum decryption is a threat facing the international community where China is not the sole aggressor, but they are the primary threat due to their stated aim to revise the world order. Achieving quantum decryption would give China an advantage to that end. The Charter of the U.N. seeks to "unite our strength to maintain international peace and security."[32] Securing cyberspace is in perfect alignment with international stability.

The U.N. has proven adept in the physical domain through treaty organizations. For example, the U.N. administers the Comprehensive Nuclear Test Ban Treaty Organization to monitor, attribute, and hold accountable signatory countries for nuclear test explosions.[33] A critical difference between a treaty organization and what this author is proposing is that the cyber domain is not suitable for treaties due to an inability to verify compliance.[34] An additional consideration is that China could refuse to be a signatory to such an agreement. Exploring these issues is beyond this paper's scope but is worth highlighting to express the complexity of a

---

[31] Antony Blinken. "A Foreign Policy for the American People." News release, March 3, 2021. The Department of State. Accessed September 24, 2021. https://www.state.gov/a-foreign-policy-for-the-american-people/.

[32] "United Nations Charter (full text)," Preamble, Accessed October 13, 2021, https://www.un.org/en/about-us/un-charter/full-text.

[33] "About," Comprehensive Nuclear Test Ban Treaty Organization, Accessed October 13, 2021, https://www.ctbto.org/specials/who-we-are/.

[34] Nye, Joseph S. "From Bombs to Bytes: Can our Nuclear History Inform our Cyber Future?" Bulletin of the Atomic Scientists 69, no. 5 (2013): 8-14. doi:10.1177/0096340213501338. https://journals-sagepub-com.usnwc.idm.oclc.org/doi/pdf/10.1177/0096340213501338. 12.

seemingly necessary multilateral solution. On the contrary, a bilateral agreement between the two global leaders in quantum computing might prove more influential for PQC implementation.

Therefore, another option for collaboration is establishing a graduate-level quantum science exchange program at leading U.S. and China universities. A quantum science exchange program could provide the U.S. with valuable intelligence if PQC is not ubiquitous before China realizes quantum decryption. This effort should include a confluence of U.S. intelligence activities to provide early warning and inform response plans regarding quantum decryption. Daniel Golden writes in *Spy Schools* that "U.S. universities have become a favored arena for the secret jousting of spy versus spy."[35] Quantum computing technology development is still in a nascent stage. Recruiting agents for espionage now could reap future insights. However, this initiative—exploiting quantum science academia for espionage—could require a restructuring of intelligence resources.

There is momentum within the intelligence community (IC) to understand China's progress in disruptive, enabling technologies. Due to U.S. national priorities and an "increasingly adversarial [China] government," the Central Intelligence Agency recently established a China Mission Center, which "will bring together case officers who recruit spies, intelligence analysts, technology experts and other specialists in a single unit."[36] Strategic priorities from the Office of the Director of National Intelligence (ODNI) align subordinate organization activities and influence intelligence resources allocation. ODNI is the administrator of the National Intelligence Priorities Framework (NIPF) and a member of the NQIA-established Subcommittee

---

[35] Golden, Daniel. *Spy Schools : How the CIA, FBI, and Foreign Intelligence Secretly Exploit America's Universities*. New York, New York: Henry Holt and Company, 2017. xvii.

[36] Warren P. Strobel, "CIA Chief Burns Forms China-Focused Group in Pivot Toward Asian Rival," *Wall Street Journal,* October 7, 2021. https://www.proquest.com/docview/2579572452/808DC65331F4586PQ/2?accountid=322.

on QIS.[37] Thus, the ODNI has the access and authority to prioritize quantum decryption. Although there is a compelling case for quantum, one can always look to the federal budget to understand what a national priority is—and is not.

Competing Interests

Some would argue that the strategic pillars are too much for one enabling technology. The U.S. government faces a multitude of threats to economic and national security. Follow the money—the government has not prioritized QIS, despite a law directing the President to ensure the U.S. stays at the forefront of this technology race. The federal funding for QIS is estimated to cost $1.1 billion over five years ($220 million/year).[38] The allotment is $80 million for NIST, leading the international effort to identify adequate PQC security protocols. Those numbers pale in comparison to historical context. From 1940-1945, the Manhattan Project cost $20 billion ($5 billion/year) in constant fiscal 1996 dollars.[39] Why should the federal government prioritize quantum decryption over *other* enabling technology threats? To which the author replies: Exactly.

The U.S. must establish a governing body that holistically applies the Defend, Deny, Discover-strategic framework against enabling technologies. This model transcends quantum decryption. A holistic application would create resource efficiencies and eliminate redundant processes. For example, DOD recognizes other dual-use, enabling technology threats to include

---

[37] U.S. Office of the Director of National Intelligence, *National Intelligence Priorities Framework,* ICD-204, January 7, 2021. https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf.

[38] CBO issues cost estimate for national quantum initiative act. (2018, Aug 20). *Targeted News Service* Retrieved from https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fwire-feeds%2Fcbo-issues-cost-estimate-national-quantum%2Fdocview%2F2091231435%2Fse-2%3Faccountid%3D322.

[39] Schwartz, Stephen I. *Atomic Audit : The Costs and Consequences of U.S. Nuclear Weapons since 1940*. Washington, D.C: Brookings Institution Press, 1998. xvii.

artificial intelligence, 5G, biotechnology, and autonomous systems.[40] Every technology area is unique in its readiness level, threat priority, and operational application. The framework is a system of levers through which an enabling technology can be advanced on behalf of the U.S. and allies while simultaneously denying an adversary their desired outcomes from weaponizing said technologies. There is precedent for the establishment of a single government body chartered to direct science and technology development. In 1941, President Roosevelt approved—"without fuss"—a proposal for an executive body responsible for coordinating and prioritizing scientific discovery supporting the war effort.[41] This organization initially started as the National Defense Research Committee and eventually became the Office of Scientific Research and Development (OSRD) with an expanded charter (to include medical sciences) and authority (congressional funding).[42] After the war, OSRD dissolved—defense research authorities liquidated throughout the services.[43] As the U.S. pivots from two decades of the Global War on Terror to the more ethereal Great Power Competition, the time is right to establish a governing body that holistically confronts enabling technology implications.

Conclusion

Enabling technologies require an offset strategy intended to include partners and competitors alike. There is no one solution in a global ecosystem rife with social and policy problems where trust is the underpinning factor.[44] One of the greatest threats—and opportunities—is quantum computing. Through the Defend-Deny-Discover framework, granular

---

[40] "Modernization Priorities," OUSD for Research and Engineering. Accessed October 12, 2021. https://www.cto.mil/modernization-priorities/.
[41] Aspray, W. (1998). "An architect of science." *Science*, 279(5350), 500-501. Retrieved from https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Farchitect-science%2Fdocview%2F213577049%2Fse-2%3Faccountid%3D322. 500.
[42] *Ibid.*
[43] "227.1 Administrative History," *Records of the office of Scientific Research and Development,* Accessed October 11, 2021. https://www.archives.gov/research/guide-fed-records/groups/227.html.
[44] Frank L. Smith, III, interview by author, Newport, RI, September 20, 2021.

quantum decryption recommendations percolate to the surface, like DOS Fellows, DOD Title 10 security cooperation, intelligence priorities, and the U.S. leading the establishment of a U.N. organization. The interconnected, globalized world needs to build plans to implement PQC security protocols on classical systems. Future research can explore this concept in more depth. What, technically, does implementation look like? What mechanisms are available to compel countries, industries, and private companies to harden their systems with PQC? Finally, across the instruments of national power, the U.S. must seek ways to understand better how those that "do not do" quantum mechanics can help those that "do"—to collectively advance the technology and its subsequent countermeasures, especially in the name of national security.