Post-Quantum Cryptography: The Quantum Arms Race and Its Threat to Strategic Stability

Christian Custodio[1]
[1]United States Military Academy, Department of Physics and Nuclear Engineering, West Point, New York, United States
https://doi.org/10.38126/JSPG280102
Corresponding author: christian.f.custodio.mil@army.mil
Keywords: Post-Quantum Cryptography; Quantum Computing; Harvest Now, Decrypt Later; Strategic Stability; Cybersecurity Policy; National Security; RSA Encryption

Executive Summary: The landscape of quantum technology is evolving with computing at the forefront of nations' policies and budgets. Post-Quantum Cryptography (PQC) promises a new era of secure information with the threat that quantum-capable computers pose to classical encryption methods. In response, the federal government has issued national security memoranda which aim to secure government and corporate systems. However, current policy does not address the issue of "harvest now, decrypt later" attacks, where adversaries collect classically encrypted information today to decrypt once a quantum-capable computer is developed. This inevitable mass decryption event would expose large amounts of classified information and could potentially undermine strategic stability. Countries like Russia and China have already invested heavily to develop quantum computers and outpace our capabilities. To counter this risk, federal agencies—including NIST, NSA, DHS, and the State Department—must accelerate the quantum-resistance timeline, expand access to new encryption standards, and create organizations that support diplomatic engagement. These efforts will reduce our vulnerability and strengthen bilateral relations in this new era of information security.

I. Introduction and background

The encryption standards that protect government institutions, civilian infrastructure, and private corporations are at risk of becoming obsolete. Advances in quantum computing jeopardize the mathematical foundations of modern cryptography, creating a vulnerability window that adversaries are already beginning to exploit. By intercepting network traffic, exploiting data leaks, and stealing from servers, adversaries can harvest sensitive data today and store it undetected, waiting until quantum computers are capable of decryption. This threat, known as "harvest now, decrypt later," must be addressed urgently to prevent a mass decryption event that could expose sensitive information and destabilize relations between the United States and its adversaries (Palo Alto Networks 2025; Barenkamp 2022).

Traditional computers process information using bits, the smallest unit of data represented as either a zero or one, whose computational capacity scales linearly with their number. Every operation within a classical computer is built from combinations of these binary states. As more bits and processing resources are added, classical computers can handle increasingly complex calculations. Quantum computers instead use quantum bits, or qubits, which exploit the principles of quantum mechanics. Qubits are unique in their ability to exist in multiple states simultaneously, rather than just zero or one, through a phenomenon known as superposition. This allows certain computations that would normally be performed sequentially by a classical computer to be explored far more efficiently, enabling computational power for some problems to scale exponentially (Figure 1).

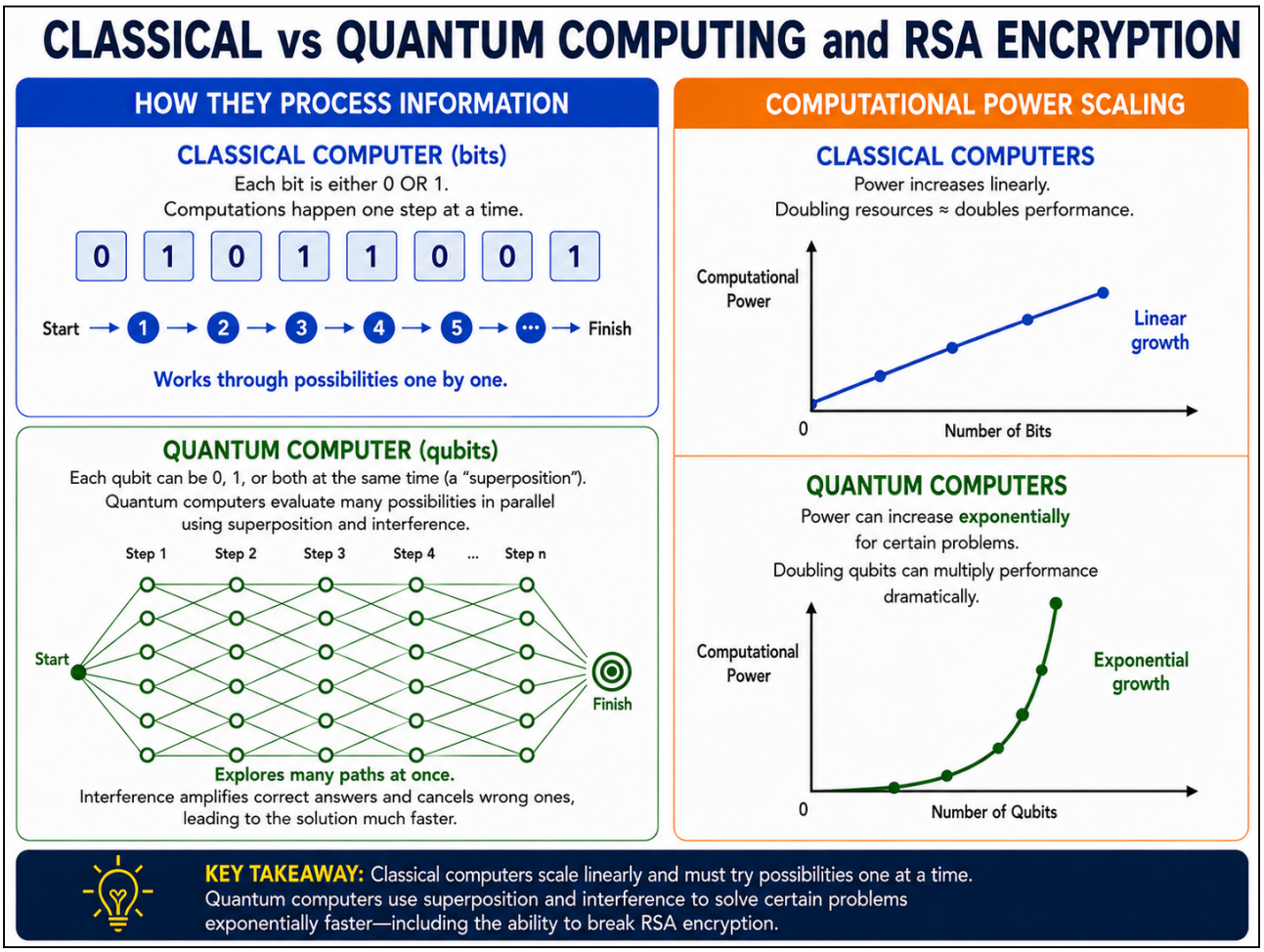

Figure 1: Algorithmic and computational scaling differences between classical (bits) and quantum (qubits) systems, highlighting why quantum superposition and interference threaten traditional RSA encryption protocols.

Traditional computers can be thought of as working through an enormous building filled with locked rooms. A classical computer may test doors one at a time, and even clever classical algorithms can only narrow the search by using patterns or clues. As the number of possible doors grows, the time required to find the right one can become astronomically large. Quantum computers do not literally open every door at once, but they can use quantum mechanical behavior to evaluate possible pathways far more efficiently.

This distinction is especially important in cryptography because systems such as RSA rely on the practical limits of classical computation. RSA is not impossible for a classical computer to break in theory. Rather, it is considered secure because factoring the extremely large numbers behind RSA would take an impractical amount of time, potentially billions of years with current classical methods. Peter W. Shor first formalized this threat by demonstrating that quantum mechanics could be used to factor large numbers far faster than classical computers, challenging the basic assumption that makes RSA secure (Shor 1997).

This capability poses a direct threat to existing encryption standards. Rivest-Shamir-Adleman (RSA), one of the most widely used encryption methods, relies on prime factorization—a mathematical operation so computationally infeasible for classical machines that it forms the basis of modern secure communication. Quantum computers, however, enable algorithms that can efficiently break RSA encryption, rendering this security measure obsolete (Mailloux, Lewis II, and

Grimaila 2016). RSA's importance cannot be overstated; it underpins the encryption used by governments, banks, corporations, and individuals daily. An adversary capable of breaking it could compromise sensitive systems on a national scale.

This vulnerability has not gone unnoticed by adversaries. Russia has already responded by acting aggressively through its National Technology Initiative, which identifies quantum technologies as "strategically important cross-cutting directions" and established dedicated research centers such as the Quantum Technology Center at Lomonosov Moscow State University and the Center for Quantum Communications at the National University of Science and Technology (Ivezic 2024).

In response to the threat of growing vulnerabilities, the federal government has begun prioritizing post-quantum cryptography (PQC), encryption standards designed to withstand quantum-enabled attacks. In May 2022, the White House issued a national security memorandum to promote U.S. leadership in quantum computing and directed the National Institute of Standards and Technology (NIST) to create standards for quantum-resistant cryptography, which is designed to withstand attacks from a future cryptanalytically relevant quantum computer (CRQC) capable of breaking classical encryption (White House 2022). In June 2025, the White House reinforced federal directives on cybersecurity through Executive Order 14144, "Strengthening and Promoting Innovation in the Nation's Cybersecurity," highlighting the urgency of transitioning to newly standardized quantum-resistant systems (White House 2025b). It mandates that all federal systems must transition to PQC compliant by January 2, 2030 (White House 2025b). The National Security Agency (NSA) has recommended that National Security System (NSS) standards incorporate additional protective measures including lattice-based cryptography, hash-based signatures, and quantum key distribution. However, the NSA acknowledges that feasibility constraints may affect the speed of implementation. Given the urgency of the quantum threat and the typical timelines required for technological development and testing of these additional measures, it is imperative that complementary, non-technological measures of protection also be explored (NSA 2022).

Nevertheless, while these directives do not yet fully address the immediacy of the national security threat created by "harvest now, decrypt later" attacks, they establish an institutional framework that identifies key agencies, sets compliance deadlines, and standardizes encryption requirements upon which a comprehensive quantum security strategy can build.

II. Analysis

The United States has already assigned agencies roles in securing government systems in preparation for post-quantum cryptography (U.S. Congress 2022). NIST leads the technical process through its PQC Standardization Project, publishing Federal Information Processing Standards (FIPS) that outline encryption standards and algorithms. In 2024, NIST released FIPS 203–205, which establishes quantum-resistant approaches for key establishment and digital signatures (NIST 2024b; NIST 2024c; NIST 2024d). The Office of Management and Budget (OMB) allocates funds and converts the standards into government-wide guidance (OMB 2022). The method of implementation is at the discretion of the agency: the NSA is responsible for national security systems, the Cybersecurity and Infrastructure Security Agency (CISA) oversees civilian federal networks, and the Department of Homeland Security (DHS) works to support critical infrastructure. Each body has issued roadmaps and memoranda that reflect their specific responsibilities.

While the United States is building a coordinated federal approach, potential adversaries have begun their own quantum initiatives to gain an advantage. The Russian government has committed $1.83 billion toward research and development (Ivezic 2024). China has committed roughly $15 billion to quantum technology and publishes more quantum research papers annually than any other country, outpacing both the United States at $7.67 billion and the combined investments of European countries (QURECA 2025). These trends demonstrate that competitors are investing in quantum technologies with high potential to shape strategic stability before quantum-resistant systems are developed and widely available.

To assess the scale of this issue, it is useful to consider the effects of past incidents involving

unprotected or compromised data. The 2015 Office of Personnel Management breach exposed sensitive information from 21.5 million security clearance forms, including details that adversaries could use for targeting or coercion. Another example is the release of roughly 250,000 diplomatic cables through WikiLeaks, which revealed an assessment of foreign leaders and governments (House Committee 2016). These disclosures not only strained bilateral relationships but also fueled a diplomatic crisis. Reports indicated that some Arab governments, including Saudi Arabia, urged the United States to take military action against Iran after cables highlighted concerns over its nuclear program (The Guardian 2010). A situation like this foreshadows unintended consequences with major world powers like Russia. If unencrypted or improperly secured information could provoke such far-reaching consequences, decrypted archives containing weapons designs, infrastructure software, or operational plans would present an even greater risk. These cases highlight why the timely adoption of post-quantum cryptography, along with re-encryption of long-lived sensitive archives, is a significant national security priority.

III. Policy Options

To address the follow-on effects of a mass decryption event caused by advances in quantum computing, three separate quantum security actions are proposed: (1) accelerating the transition to PQC across critical sectors, (2) establishing an international transparency body to preserve strategic stability, and (3) initiating a re-encryption effort to protect existing data.

i. Course of action 1: Accelerated migration to PQC standards

This effort aims to reduce the amount of decryptable data available to adversaries by updating federal systems ahead of schedule. To close this vulnerability window, I propose that subsection 4(f)(ii) of Executive Order 14144 is adjusted to move the compliance deadline from 2030 to January 2, 2028. In similar instances, the Government Accountability Office (GAO) reported that federal IT modernization efforts required $175 million when agencies compressed modernization schedules, mirroring the budget needed for standard acceleration (GAO 2025). Drawing from comparable accelerated modernization efforts identified by the GAO, I propose reallocating $100 million annually, split evenly between the NSA and DHS, from the Department of Defense's existing cyberspace activities budget to support an expedited PQC transition. To contextualize the source of this funding, in 2026 the DOD requested $9.1 billion for cyberspace activities supporting objectives including weapons systems, supply chain risk management, and defense critical infrastructure (Congress 2026). Given the immediacy of the quantum threat, this reallocation would redirect funds from lower-priority cybersecurity objectives toward defense critical infrastructure, devoted solely to upgrading to PQC systems. Directed through OMB, this funding would accelerate implementation, expand testing capacity, and support the personnel required for an earlier PQC transition.

A potential drawback is the precedent set by federal modernization efforts, which have historically fallen susceptible to shifting administrations and changing standards (Mosca and Piani 2024). Without proper implementation measures, clear directives, and designated funding, attempts to accelerate the compliance deadline risk pushing the original timeline further while creating tradeoffs with other national security priorities. On the other hand, successful acceleration of PQC adoption would directly address the vulnerability, build upon existing policy infrastructure, and narrow the window during which adversaries can expand harvest now, decrypt later operations.

ii. Course of action 2: The International Quantum Transparency Committee (IQTC)

To manage the strategic risks posed by CRQCs, this COA proposes the establishment of the IQTC within the Bureau of Arms Control, Verification and Compliance (AVC), operating under its Office of Emerging Security Challenges (AVC/ESC). The AVC/ESC is already mandated to provide research, analysis, and recommendations on cyber strategic stability and transparency and confidence building measures, making it optimal for quantum oversight (U.S. State Department 2017). Modeled after the Strategic Arms Reduction Treaty (START) verification framework, the IQTC would promote transparency and trust between the United States and adversaries through on-site inspections, bi-annual data exchanges, and unique identifiers for declared quantum systems. In terms of composition,

the IQTC would employ AVC/ESC personnel to oversee inspections and technical advisors from NIST and the NSA for quantum-specific technical expertise. The committee would report findings directly to the Deputy Assistant Secretary for Emerging Security Challenges and Defense Policy. The initiative would require an estimated $20 million per year, totaling $60 million over three years, drawn from the State Department budget. Given that comparable arms-control support offices operate on annual budgets of $100–150 million, this represents a proportional and conservative investment for a new verification body (CRS 2020). Though its near-term impact would be limited, the IQTC would lay the foundation for future international agreements addressing both the immediate threat of harvest now, decrypt later attacks and the broader strategic risks quantum computing poses to global deterrence.

The IQTC's effectiveness would be contingent on the voluntary participation of adversaries possessing a CRQC, a condition that cannot be assumed given fluctuating geopolitical tensions. Unlike the nuclear arms race, which created a mutually recognized existential threat that brought both sides to the negotiating table, the quantum computing competition has yet to produce a comparable sense of shared urgency. Although the potential exposure of sensitive government information, particularly involving nuclear weapons systems or critical civilian infrastructure, could create mutual incentives for cooperation among major powers. Nevertheless, an effective IQTC would not only prevent the weaponization of quantum computers but its success in bilateral relations could serve as a model for continued diplomatic cooperation of rivaling hegemonic powers, similar to that of the International Space Station (Krishna 2024).

iii. Course of action 3: The Quantum Resistant Infrastructure Committee (QRIC)

I propose the Department of Commerce establish the QRIC to lead a quantum re-encryption campaign to incentivize private industry toward PQC standards. This initiative would provide up to $500 million in subsidies to incentivize private-sector migration to PQC standards. Given that the U.S. government projects approximately $7.1 billion will be required to complete the post-quantum cryptography transition for non-national-security systems alone, a targeted $500 million subsidy represents a reasonable and proportional investment to accelerate private-sector re-encryption and reduce long-term national exposure (LaMacchia, Campagna, and Gropp 2025). Beginning January 2, 2028, publicly traded companies would be required to report their quantum readiness in SEC filings. The framework would be developed in conjunction with NIST and the SEC to ensure technical and regulatory standards align. Major tech companies such as Google, Microsoft, and Amazon would provide re-encryption tools for consumers and small businesses in an effort to make them widely accessible.

The QRIC's function would be to support passive policy that companies choose to partake in, and without enforcement methods companies may not be incentivized enough to undertake a large-scale migration effort. SEC reporting requirements may also face lobbying pushback from corporations opposed to mandatory disclosure. However, its success would secure civilian systems and promote private corporations to take their own initiative in the new era of quantum information security.

II. Policy recommendation

This paper recommends revitalizing quantum security strategy by accelerating implementation timelines, establishing federal committees, and fostering greater private sector initiative. Implementing a revised federal strategy requires updating existing regulations and overturning previous timelines that are no longer aligned with technological reality. Federal migration deadlines to PQC standards are falling behind emerging risks, and the time required for enforcement and implementation leaves a vulnerability window open longer than intended. Funding for this accelerated migration would come primarily from the reallocation of Department of Defense cyber modernization accounts, directed through OMB, along with economic incentives for private-sector organizations to finance their own transitions. Additional market pressure would come from SEC quantum-readiness reporting requirements. These combined funding sources would be allocated to NIST, OMB, NSA, and DHS to accelerate current initiatives and support new ones outlined in earlier sections. The risks of inaction are substantial. Delayed migration leaves years of exposure, allowing

bad actors to accumulate large volumes of sensitive data for future decryption.

The three presented policy recommendations are intended to function as complementary strategies addressing "harvest-now, decrypt-later" threats from civilian, federal, and geopolitical perspectives. While each recommendation independently mitigates aspects of the CRQC threat, their combined implementation provides the most comprehensive defense. Feasibility constraints, however, may limit the extent to which any single recommendation can be fully implemented. Therefore, to protect the general welfare of the United States, policymakers should pursue all three initiatives simultaneously whenever possible.

References

Krishna, Swapna. 2024. "How Does the U.S.-Russia Partnership Work on the ISS?" Ad Astra. 2024. https://www.adastraspace.com/p/us-russia-iss.

Barenkamp, Marco. 2022. "'Steal Now, Decrypt Later.'" Informatik-Spektrum 45, no. 6: 349–55. https://doi.org/10.1007/s00287-022-01474-z.

Congressional Research Service (CRS). 2020. Arms Control and Nonproliferation Budget Trends. Washington, DC: Congressional Research Service. https://www.congress.gov/crs-product/RL33865

Congress.gov. "FY2026 Department of Defense Cyber Budget Request." March 28, 2026. https://www.congress.gov/crs-product/IN1261.

House Committee on Oversight and Government Reform, Majority Staff. 2016. The OPM Data Breach: How the Government Jeopardized Our National Security for More Than a Generation. Washington, D.C.: U.S. House of Representatives. https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf.

Ivezic, Marin. 2024. "Quantum Technologies and Quantum Computing in Russia." PostQuantum – Quantum Computing, Quantum Security, PQC, December 26, 2024. https://postquantum.com/quantum-computing/quantum-russia/.

LaMacchia, Brian, Matt Campagna, and William Gropp. 2025. "The Post-Quantum Cryptography Transition: Making Progress, But Still a Long Road Ahead." 2024-2025 CRA Quadrennial Paper. arXiv, March 3, 2025. https://doi.org/10.48550/arXiv.2503.04806.

Mailloux, Logan O., Casey Riggs Lewis II, and Michael R. Grimaila. 2016. "Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals." IT Professional 18, no. 5: 42–47. https://doi.org/10.1109/mitp.2016.77.

Mosca, Michele and Marco Piani. 2024. Quantum Threat Timeline Report 2024. Toronto: Global Risk Institute in Financial Services. https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/

National Institute of Standards and Technology (NIST). 2024a. "What Is Post-Quantum Cryptography?" August 13, 2024. https://www.nist.gov/cybersecurity/what-post-quantum-cryptography.

National Institute of Standards and Technology (NIST). 2024b. Module-Lattice-Based Key-Encapsulation Mechanism Standard (FIPS 203). Washington, DC: U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203.

National Institute of Standards and Technology (NIST). 2024c. Module-Lattice-Based Digital Signature Standard (FIPS 204). Washington, DC: U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.204.

National Institute of Standards and Technology (NIST). 2024d. Stateless Hash-Based Digital Signature Standard (FIPS 205). Washington, DC: U.S. Department of Commerce. https://doi.org/106028/NIST.FIPS.205.

National Security Agency (NSA). "Post-Quantum Cybersecurity Perspective: NSA's Cybersecurity Perspective on Post-Quantum Cryptography Algorithms." August 4, 2021. https://www.nsa.gov/Cybersecurity/NSAs-Cybersecurity-Perspective-on-Post-Quantum-Cryptography-Algorithms/.

National Security Agency (NSA). 2022. Commercial National Security Algorithm Suite 2.0. Cybersecurity Advisory PP-22-1338. Fort Meade, MD: NSA. https://media.defense.gov/2025/May/30/2003728741/-1/1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

Office of Management and Budget (OMB). 2022. Memorandum on Migrating to Post-Quantum Cryptography (M-23-02). Washington, DC: Executive Office of the President. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

Palo Alto Networks. 2025. "Harvest Now, Decrypt Later (HNDL)." Accessed November 18, 2025. https://www.paloaltonetworks.com/cyberpedia/harvest-now-decrypt-later-hndl.

QURECA. 2025. "Quantum Initiatives Worldwide 2025." October 15, 2025. https://www.qureca.com/es/quantum-initiatives-worldwide/.

Shor, Peter W. 1997. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer." SIAM Journal on Computing 26, no. 5: 1484–1509. https://doi.org/10.1137/s0097539795293172.

The Guardian. 2010. "WikiLeaks Embassy Cables: Key Points at a Glance." The Guardian, November 29, 2010. https://www.theguardian.com/world/2010/nov/29/wikileaks-embassy-cables-key-points.

U.S. Department of State. 2017. "Office of Emerging Security Challenges (AVC/ESC)." Bureau of Arms Control, Verification and Compliance. Accessed March 28, 2026. https://2009-2017.state.gov/t/avc/c21764.htm.

U.S. Government Accountability Office (GAO). 2025. IT Systems Annual Assessment: DOD Needs to Improve Performance Reporting and Cybersecurity Planning. GAO-25-107649. Washington, DC: U.S. Government Accountability Office. https://www.gao.gov/products/gao-25-107649

United States Congress. 2022. Quantum Computing Cybersecurity Preparedness Act. Public Law 117–260, 136 Stat. 2389. https://www.congress.gov/bill/117th-congress/house-bill/7535

White House. 2022. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. May 4, 2022. https://www.presidency.ucsb.edu/documents/memorandum-promoting-united-states-leadership-quantum-computing-while-mitigating-risks

White House. 2025a. "Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144." June 6, 2025. https://www.whitehouse.gov/presidential-actions.

White House. 2025b. Executive Order 14144: Strengthening and Promoting Innovation in the Nation's Cybersecurity. June 2025. https://static.carahsoft.com/concrete/files/7517/3869/6330/Executive_Order_Executive_Order_14144_Strengthening_and_Promoting_Innovation_in_the_Nations_Cybersecurity.pdf

Christian Custodio earned his Bachelor of Science from the United States Military Academy, where he majored in Physics and minored in Russian. While at West Point, his research focused on the development of a quantum antenna at the Quantum Information Science Laboratory and the creation of experimental optics guides. He currently serves as a Second Lieutenant in the U.S. Army as an Aviation officer.

Acknowledgements

I would like to thank COL Diana Loucks for her mentorship and for creating the academic environment that allowed this research to develop. I am also grateful to my research advisor, Dr. David Kasinski, for his invaluable guidance in bridging quantum theory, experimentation, and policy. Finally, I would like to acknowledge the Department of Physics and Nuclear Engineering at West Point for providing the resources and support necessary to complete this work.