MEMORANDUM

To: U.S. Secretary of State Antony Blinken

From: Anisha Talreja

Date: April 3, 2022

RE: The United States Must Ensure International Cooperation on Quantum Cryptography Efforts

Executive Summary

While advances in quantum computing are revealing that its applications to improving society are far-reaching, with these advances come a major reckoning regarding encryption, as quantum algorithms can crack classical encryption. Ramifications of this discovery have led to innovative efforts to create post-quantum cryptography protocols within many countries competing in the quantum computing race, such as the United States and China. The best course of action for preserving international relations and the global economy, however, is a united approach to selecting a standard protocol for communicating encrypted information. Accordingly, I suggest the creation of an international organization with the purpose of ensuring common progress and regulations regarding post-quantum cryptography efforts to make transactions across the globe more secure.

Background

Quantum algorithms such as Shor's algorithm, which can quickly compute the prime factorization of large numbers, can easily crack encrypted information, because the widely-used Rivest–Shamir–Adleman(RSA) cryptography system relies on the assumption that prime factorization is difficult for classical computers to compute. This means that any classical applications using cryptography are vulnerable; any information currently exchanged over through these applications, including passwords and intelligence information, is at risk of being decrypted, as hackers can simply steal and store information currently believed to be encrypted with the potential to decrypt it in a matter of a few years. Noting the speed with which algorithms such as Shor's are being optimized, many experts in the fields of cryptography and quantum computing have proposed the use of several post-quantum protocols that cannot be "hacked" through quantum computing efforts(Haney).

Key Findings

Because cryptography efforts largely involve multiple entities, a standard post-quantum protocol must be established for efforts to improve information security. In the United States, the National Institute of Standards and Technology(NIST) is overseeing a multi-stage standardization process; the Chinese Association for Cryptologic Research (CACR) is following a similar process, though it is only open to Chinese scientists. Because of the difference in the selection pool, the finalists are already vastly different in their approaches. The CACR selection focused on digital signature, public-key encryption and key agreement protocols of two security levels (128 and 256 bits), which are analogous to NIST levels I and V ("CACR Post-Quantum Competition").With these two separate paths, it is clear that even after the lengthy domestic selection process, additional time will be needed to agree upon a global standard post-quantum protocol.

It is crucial that a standard post-quantum protocol be established as soon as possible because every day, billions of pieces of information are put at risk when they are exchanged through now-insecure classical encryption systems. Furthermore, cryptography is intentionally inconvenient to update; in most devices, cryptography for verifying updates is not always part of a remote update so that it must be done physically, not remotely. The World Economic Forum approximates that more than 20 billion digital devices around the globe will need to be updated or replaced in order to comply with emerging quantum safety guidelines. NIST estimates that within approximately 20 years, "sufficiently large quantum computers will be built to break essentially all public key schemes currently in use"("Post-Quantum Cryptography | CSRC"). An international effort is required in order to ensure the compatibility of all devices with a common standard for global communication to continue unhindered by the time such quantum computers are built.

The United States has previously sanctioned China for its attempts to use quantum computing to strengthen their military, demonstrating that the leaders in the quantum computing race do not always agree on applications of the technology being developed. Still, a worldwide organization must still be established despite existing tensions because the United States, China, and many other countries with individual post-quantum protocols still communicate with each other often through secure, encrypted methods. Such communications include but are not limited to emails, texts, work conferences, calls. The organization must involve the governments of member countries, unlike the existing World Economic Forum's Center for Cybersecurity, in order to ensure compliance with regulations agreed upon; such compliance can be achieved more easily

at a domestic level through government leaders. Furthermore, while new protocols may still be backwards compatible with older encryption systems, if third world countries do not update their devices and applications, weaker systems that are part of global encrypted networks will still leave information vulnerable to hackers. A global effort will expand opportunities to improve information security in countries not in the quantum computing race.

Recommendations

Recognizing the need for cooperative efforts to create quantum-safe protocols for cryptography to ensure information security, I recommend:

- The creation of a specialized agency within the United Nations: This will ensure a common, worldwide effort to create the most quantum-safe encryption for global citizens.
- Work with other countries to ensure participation in this agency: Global cooperation is essential for setting a standard post-quantum protocol.
- Set a goal to achieve a standard global post-quantum protocol by the year 2030: It is crucial to set a deadline to ensure efficiency in selecting the most viable post-quantum protocol in order to begin updating devices and applications that use encryption so as to prevent further exposure of vulnerable data currently secured by hackable cryptography systems. Setting the deadline in 2030 will allow for approximately one decade to update devices and applications before quantum computers will be able to hack almost all public key schemes.

Conclusion

While competition exists on both the domestic and international levels of the quantum computing and cryptography fields, cooperation is vital to ensure the safety of data around the world. The best method to facilitate a global effort towards this goal is to create an international entity involving the governments of all countries because it will ensure efficiency in the process of selecting a standard post-quantum protocol and efficacy in the implementation of the quantum-safe measures.

Works Cited

"CACR Post-Quantum Competition." *QApp*, en.qapp.tech/help/cacr. Accessed 4 Apr. 2022.

"Centre for Cybersecurity." *World Economic Forum*, www.weforum.org/platforms/the-centre-for-cybersecurity. Accessed 4 Apr. 2022.

Haney, Brian Seamus. "Blockchain: Post-Quantum Security and Legal Economics." *Carolina Law Scholarship Repository*, scholarship.law.unc.edu/ncbi/vol24/iss1/8/?utm_source=scholarship.law.unc.edu%2Fncbi%2Fvol24%2Fiss1%2F8&utm_medium=PDF&utm_campaign=PDFCoverPages. Accessed 4 Apr. 2022.

IBMPolicy, et al. "Embracing Our Quantum Future - IBM Policy Lab." *IBM Policy*, 3 Jan. 2022, www.ibm.com/policy/quantum-future.

"Is Your Cybersecurity Ready to Take the Quantum Leap?" *World Economic Forum*, 14 Mar. 2022, www.weforum.org/agenda/2021/05/cybersecurity-quantum-computing-algorithms.

"Key-Issues." *IBM Policy*, 13 Mar. 2020, www.ibm.com/policy/government-regulatory-affairs/key-issues.

"Post-Quantum Cryptography | CSRC." *National Institute for Standards and Technology*, csrc.nist.gov/Projects/post-quantum-cryptography. Accessed 4 Apr. 2022.

World Economics Forum. "Global Future Council on Quantum Computing Frequently Asked Questions." *World Economics Forum*, June 2020, www3.weforum.org/docs/WEF_Global_Future_Council_on_Quantum_Computing.pdf.