The Quantum Zoo of International Relations

Photo: Frozen Design/Adobe Stock

Commentary by **Zhanna L. Malekos Smith**
Published July 26, 2021

Enter the "Quantum Zoo of International Relations"—our main attraction is a towering behemoth machine with tiger stripes of tubes, wires, and a long steel cylinder snout. Peering into the cage with intense curiosity, states are increasingly studying quantum computers to gain a technical edge in cybersecurity and intelligence operations and promote economic growth.

Quantum computers are highly advanced machines that can solve complex mathematical problems more efficiently than classical computers (an impressive list of 65 quantum algorithms is available here). According to the U.S. intelligence community's 2021 annual threat assessment, the United States, China, and Russia are

vying to become the global leader in advanced computing. Last month, Germany became the first European country, in partnership with IBM, to develop a quantum computer.

But could universal quantum computing also help promote stability in international relations?

Applying Systems Thinking

In the so-called bizarre world of quantum mechanics, an atom can occupy multiple states at the same time, a phenomenon called superposition. An atom can "contain much more information than a 0 or 1," explains theoretical physicist Michio Kaku. That is why quantum computing uses different information storage units called quantum bits, or "qubits," rather than classical computing bits of 0 or 1.

Another way to conceptualize this is with Plato's famous allegory of the cave: Imagine a group of prisoners who are chained inside a cave and unable to turn their heads. The prisoners' knowledge of "reality" is based solely on watching shadows cast on the wall from carved figurines illuminated by a fire—their thinking model represents classical computing bits of 0 or 1. In contrast to classical computing, the prisoner who escapes outside of the cave, let's call him Prisoner Qubit, sees the world illuminated by natural sunlight and gains wisdom about quantum superposition—that multiple realities or forms can simultaneously exist. As a systems thinking method, combining Plato's cave with computing allows us to conceptualize quantum systems as a whole, before splitting the elements apart and exploring design solutions to promote international cooperation.

Could Quantum Promote Stability in International Relations?

Theoretically, yes.

Universal quantum computers could enable confidence-building measures (CBMs) in international relations in several ways. CBMs are state actions that promote trust in diplomacy by mitigating potential hostilities and increasing communication about one's capabilities and intent—like establishing a crisis hotline between two nations' leadership.

First, quantum technology could enhance trust in the attribution processes used to investigate state-sponsored cybercrime and other malicious information and communications technology (ICT) incidents.

Granted, attribution –associating data with an entity–is not a plain vanilla concept. Rather, it comes in a variety of flavors like technical forensic analysis, legal attribution, and the political decision to attribute an actor's misconduct. States have strong sensitivities to attributing ICT incidents, as revealed in the UN Group of Governmental Experts 2019-2021 consensus report, which recommends future work by the United Nations on "consider[ing] how to foster common understandings and exchanges of practice on attribution."

With advanced computational speeds to perform unstructured searches, quantum could better streamline the process for states to "substantiate their concerns and findings" on malicious ICT incidents. Additionally, applying quantum technology to detect suspicious patterns in network activity and quarantine compromised nodes in the system could augment the incident response recovery process for organizations. From a threat intelligence perspective, this could afford organizations better situational awareness of an ever-evolving threat environment to improve security measures and the incident handling process.

Supporting International Norms of Responsible State Behavior

Second, layering quantum technologies with CBMs could serve as a conduit to support international norms of responsible state behavior. There is a growing call amongst national security experts for the United States to explore other foreign policy tools– apart from punitive sanctions –in response to state-sponsored cyberattacks.

In April the administration issued an executive order to impose sanctions against Russia for the SolarWinds hack and 2020 election interference, and another executive order in May to bolster the nation's cybersecurity. However, following the July ransomware attack by REvil against Kaseya, a U.S. software management vendor, and other recent cyberattacks on U.S. entities like JBS and Colonial Pipeline, the Biden administration announced it was reevaluating how to impose "punitive sanctions" and work multilaterally with allies.

To that point, implementing quantum technology may also benefit the legal process of holding cybercriminals and state actors accountable for misconduct via indictments. Legal indictments, like the Department of Justice's recent indictment of four Chinese nationals involved in a global cyberespionage campaign, can serve as a useful signaling mechanism to states and foreign hackers working on their behalf. Moreover, with advanced computational power to factorize large numbers to weaken an adversary's encryption tools, quantum computing could help promote transparency by holding actors globally accountable and support the timely collection, review, and presentation of evidence before a federal grand jury. Because of quantum's impressive computational advantages, some scientists are lauding them as "the ultimate computers."

On the other hand, there are significant concerns among cryptographers that universal, large-scale quantum computers could be applied to break "many of the public-key cryptosystems currently in use," like RSA, thereby compromising the confidentiality and integrity of the communications systems we rely upon daily. According to a panel of experts at CSIS's Cybersecurity in the Quantum Future event, quantum computers could be applied to break advanced encryption in as little as eight hours. In response to this burgeoning risk, the National Institute of Standards and Technology opened a call for research proposals as part of its ongoing efforts to develop quantum-resistant public-key cryptographic algorithms, also called post-quantum cryptography.

As with any thought exercise involving quantum, it's important to bear in mind Amara's Law that "we tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run." Thus, this piece strives for a moderate approach in envisioning how universal quantum computing could one day support CBMs in the Quantum Zoo of International Relations.

Zhanna Malekos Smith, JD, is a senior associate with the Strategic Technologies Program at the Center for Strategic and International Studies in Washington, D.C., and an assistant professor in the Department of Systems Engineering at the U.S. Military Academy at West Point. The views expressed are those of the author and do not

necessarily reflect the official policy or position of the Department of Defense or the U.S. government.

With special thanks to William Crumpler.