Centre for International Governance Innovation

Digital Policy Hub

Digital Policy Hub – Working Paper

Scrambling for Quantum Supremacy in the Global Commons

Kristen Csenkey

Winter 2025

About the Hub

The Digital Policy Hub at CIGI is a collaborative space for emerging scholars and innovative thinkers from the social, natural and applied sciences. It provides opportunities for undergraduate and graduate students and post-doctoral and visiting fellows to share and develop research on the rapid evolution and governance of transformative technologies. The Hub is founded on transdisciplinary approaches that seek to increase understanding of the socio-economic and technological impacts of digitalization and improve the quality and relevance of related research. Core research areas include data, economy and society; artificial intelligence; outer space; digitalization, security and democracy; and the environment and natural resources.

The Digital Policy Hub working papers are the product of research related to the Hub's identified themes prepared by participants during their fellowship.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

Partners

Thank you to Mitacs for its partnership and support of Digital Policy Hub fellows through the Accelerate program. We would also like to acknowledge the many universities, governments and private sector partners for their involvement allowing CIGI to offer this holistic research environment.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Key Points

- In the race for quantum supremacy, quantum technologies are increasingly being framed as a space for geopolitical competition and as a tool to gain a strategic advantage in other domains such as cyberspace.
- This working paper uses the global commons conceptual framework to analyze the strategic advantages of quantum technologies in the context of a future where intelligently connected and quantum-enhanced transportation networks are integral to smart cities, encompassing practical application in both physical and cyber domains.
- The analysis suggests ongoing de facto domination of domains by hegemonic powers, notably through standard setting. Rather than interpreting the result as indicative of an expanding sphere of control in the global commons, it could be considered a sphere of opportunity for the integration of democratic governance frameworks.

Introduction

The idea that emerging and transformative technologies are inherently ungovernable because they are "wicked problems" is often used to explain the uncertainties surrounding their development and deployment, especially as understood in policy. This characterization is frequently applied to multifaceted and complex technologies, such as electric vehicle batteries, artificial intelligence (AI), cryptocurrencies, information and communications technologies as part of smart cities, the Internet of Things (IoT) and cybersecurity (E. Malone and M. Malone 2013; Colding, Barthel and Sörqvist 2019; Marchant 2020; Carr and Lesniewska 2020; Lehtimäki et al. 2024).

Generally, wicked problems are difficult to define; they are sometimes ascribed neutrality, possibly related to other wicked problems, and are policy related. Wicked problems essentially lack single definitive solutions (Rittel and Webber 1973), and their "wickedness" stems from the challenge of defining and framing the problem itself (Lehtimäki et al. 2024). B. Guy Peters (2017) provides a conceptual framework that clarifies the broad scope of wicked problems based on the work of Horst W. J. Rittel and Melvin M. Webber (1973). Yet, within the wicked problems space, areas of cooperation on solutions are difficult to identify. This working paper seeks to explore other frameworks for understanding the governance challenges and solutions of technologies such as quantum.

Research Questions and Structure

This working paper moves beyond the concept of wickedness to investigate the geopolitical implications of quantum technologies by instead evaluating them through a global commons lens. Specifically, this paper asks: In the race for supremacy, are quantum technologies considered a part of the global commons in international security? If so, in what way? The answer has implications for the governance of these technologies, cooperation and security issues related to shared spaces of collaboration in solving global problems.

This working paper is structured in six sections to address the research questions. First, the introduction explains the concept of wicked problems, followed by "Background: Wickedness Is Not Enough for Quantum Problems," a section that elaborates on it within the context of global competition for quantum technology supremacy. The next section, "Conceptual Framework: From Wicked Problems to Global Commons," discusses the origins and utility of the global commons concept, arguing that it provides a more effective framework than a focus on wicked problems for addressing global governance challenges in the current era of great-power competition for quantum supremacy. "Applying the Framework to Quantum, Cyber and Intelligent Transportation Systems" evaluates quantum technologies through the conceptual framework of the global commons and the connection to the cyberspace domain. The "Implications" section highlights the findings revealed by the analysis, primarily the potential of certain actors as de facto governors and the need for a more coordinated and inclusive approach to quantum technology governance. The final section offers recommendations based on the findings, focusing on the opportunities for cooperation despite an environment increasingly defined by competition.

Background: Wickedness Is Not Enough for Quantum Problems

Previous research has explored how IoT and cybersecurity exemplify the wicked problem space, creating complex cyber-physical infrastructures with significant global governance challenges (Carr and Lesniewska 2020). This complexity arises from the intricate interplay between technology and human behaviour within these interconnected systems. In the context of quantum technologies, this complexity is amplified in three ways.

First, quantum technologies are many — they include physical elements within digital ecosystems, computing, sensing and communication technologies, and they connect to other existing systems to function or to increase their effectiveness. For instance, AI-enhanced quantum optimization has the potential to improve the efficiency of solving complex challenges, such as the communication and coordination of autonomous vehicle (AV) navigation.

Second, and relatedly, quantum technologies and their existing and potential capabilities operate across multiple domains, therefore horizontally impacting numerous sectors and crossing traditional state borders of authority. In a previous working paper, the author (Csenkey 2025) explored the potential use of quantum technologies within the transportation sector, specifically through the interoperability of systems across national borders, the security of transnational flows of goods and services, the safety of human users and data privacy.

Third, there are intersecting economic, scientific, military and societal implications, opportunities and risks associated with these interlinked technologies. Although this challenge is not unlike other emerging and transformative technologies that have the potential to be used for harm, profit and betterment (such as AI and cryptocurrencies), quantum technologies are now caught in the crosshairs of a global great-power

competition for technology supremacy.[1] Although the quantum sector is relatively small within each country, its global projected value is in the billions of dollars[2] and promises significant advancements in critical sectors, such as health care and defence.

The complexity of quantum technologies is amplified in these three ways and further complicated by their varying stages of development, making it difficult to fully identify associated problems and therefore label them as "wicked." These technologies exist across a spectrum, from early theoretical and experimental research to initial practical uses, and encompass existing technologies that use quantum mechanics, such as magnetic resonance imaging scanners.[3] Therefore, while this complexity creates challenges for global governance, wickedness alone is insufficient to fully characterize the problems or guide solutions, particularly because quantum supremacy is considered both a problem and a solution.

Winning the Race to Supremacy

Quantum supremacy generally has two meanings. The first meaning, widely used in the technical literature and usually applied to computing, refers to the ability of a device using quantum mechanics to perform a computation that would otherwise be impossible for classical[4] computers (Preskill 2018). Described as a "moving target" because the capabilities of classical computing and algorithms are constantly improving, the details of achieving supremacy are still rather "fuzzy" since many of the capabilities of quantum devices are still unknown (Mosca and Piani 2022, 9). However, this has not hampered private sector companies from using the term frequently and tying it to business competition to promote products and hype investments (Arrow 2025).

The competition for quantum supremacy is sometimes referred to as a race for a "practical quantum advantage," meaning that the goal is to find practical use cases so that quantum computing can actually create an advantage when used in the real world (Hibat-Allah et al. 2024). Winning this race has scientific and economic implications because actors that can make a quantum system perform a useful task (make something better or faster and solve problems that would otherwise be unsolvable) would gain an advantage in any number of fields. This is where the second meaning of quantum supremacy intersects.

Prominent within international security and political discourse, the second meaning of quantum supremacy underscores the relationships between technology, national strategy, sovereignty and power projection. Making a quantum system perform a task better and faster and able to solve currently unsolvable problems has obvious strategic advantages for states. This capability could enhance abilities in defence and intelligence; for example, actors possessing a fully fledged quantum computer capable of breaking cryptographic systems in use today could potentially decrypt and allow access to classified information (Csenkey and Bindel 2023). Quantum-enhanced sensing could also increase the efficiency of how threats are tracked

1 For example, see Anwar (2025); Gargeyas (2021); Prisco (2024); Kim and Monroe (2024).

2 With some sources suggesting that the value is in the trillions of dollars; see Quantum Computing Business (2024).

3 There is also the distinction between the technologies associated with periods or revolutions in quantum development (for example, Quantum 1.0 and Quantum 2.0 and the associated technologies therein).

4 Also known as traditional or existing capabilities of computers.

and how military operations are navigated and monitored, with implications for situational awareness in multiple domains (Csenkey et al. 2025). As a result of these potential advantages and risks, governments around the world are "racing" to develop quantum capabilities, which has resulted in, as Michal Krelina (2025, 9) argues, a "new domain" of geopolitical competition and cooperation.

Thus, applying the wicked problems framework to quantum technologies reveals that simply labelling them as "wicked" is insufficient to wholly describe their complexity and may ascribe neutrality, when instead they are spaces of politics. This is partly due to their emerging and transformative status, but also because wickedness acts as a blanket term for complexity, often lacking meaningful solutions.

Technologies can introduce new political dynamics and power considerations to international relations and global governance (Feakin 2024). While Kristi Govella (2019) argues that technology is part of the global commons, the digital-physical intersections of technologies can obscure the respective roles of states and other international actors. For instance, great powers, such as China and the United States, seek to assert authority in the cyber domain by investing in critical technologies, such as quantum, and by establishing a state-first approach to defining a new global order through technology governance. The narrative of competition for technology supremacy often defines the relations between states, as exemplified in Chief Technology Officer of the United States Michael Kratsios's statement: "The shape of the future global order will be defined by whomever leads across AI, quantum, nuclear, and other critical and emerging technologies. Chinese progress in nuclear fusion, quantum technologies and autonomous systems all press home the urgency of the work ahead" (cited in Reuters 2025).

As cooperation on quantum technology research, development and practical application becomes increasingly politicized through the convergence of national economic and security interests, further research on this topic is especially relevant. This is particularly important given the substantial investments made by public-sector actors in this technology as they attempt to influence its application, accessibility and purpose.[5] Therefore, understanding how digital-physical technologies can contribute to global solutions in the cyber domain, rather than exacerbating problems through their complexity, is essential.

Conceptual Framework: From Wicked Problems to Global Commons

Quantum technologies have emerged as a new domain for geopolitical competition and cooperation — a narrative connecting the technological and the political, with significant implications for access to this space and the distribution of benefits. Quantum technologies constitute a domain in and of themselves and also operate across many domains, especially cyber. This development also affects the authority to define

5 For instance, see Chou, Manyika and Neven (2025).

global problems and their practical applications as quantum capabilities that are funded, developed, implemented and translated to future strategic resources. The quantum space is important for international security as states scramble to define the parameters of the domain and to access and harness research for their own strategic objectives.

Domains — or extraterritorial spaces — and their delineation are central to international security and to understanding state competition, cooperation and conflict (Graefrath and Jahn 2024). In the international relations and security literature, these spaces are understood as the "global commons" and fall outside the jurisdiction of any single state, theoretically making them accessible to all (Vogler 2012). These spaces have traditionally included the high seas, polar regions and outer space. States compete for access to these spaces as strategic assets due to their potential for resource extraction, trade and defence activities that offer both economic and military benefits. As states compete to define the jurisdiction, activities, uses and governance of these spaces, they become increasingly politicized, raising the potential for conflict. For example, Jessica West and Jordan Miller (2023) argue that grey zone conflict in outer space stems from a failure of governance to maintain space as a domain for peaceful activities, rather than one for militarization and potential harm.

A challenge in understanding the governance of global commons spaces is that they are often lumped into a single category. As Moritz S. Graefrath and Marcel Jahn (2024) argue, these spaces vary, and some are not truly accessible to all states but rather to a select few. This limited access results in de facto dominance by hegemonic great powers, restricting other states' attempts to gain access without the dominant power's consent. The authors' critique of the global commons concept as a single category leads them to propose a more nuanced distinction therein: "spheres of control" (dominated spaces) and "true commons" (universally accessible spaces) (ibid.).

This updated framework offers a useful conceptual tool for analyzing international political dynamics by dividing the global commons into two types. Applying this distinction can open new opportunities for international cooperation through policy making. This framing allows for a more nuanced exploration of global challenges by highlighting how access to space is important in framing global problems and solutions. Defining national jurisdiction determines a state's territory and therefore its authority, consequently limiting other states' access and potential resource benefits. In the cyber domain, this is particularly complex. Although Graefrath and Jahn (2024) do not explicitly address cyberspace, as states such as China and the United States increasingly compete to dominate all domains and control access to resources (and define values and activities therein), opportunities for cooperation in this domain are diminishing.

To address the research questions posed in this working paper, this study draws on the global commons conceptual framework proposed by Graefrath and Jahn (2024). While building upon previous conceptualizations (for example, Volger 2012; Hughes 2016), the authors refine the concept and offer their framework as a novel conceptual tool, using outer space as an illustrative example. Neither the wicked problem nor the global commons framework has been previously evaluated and applied to quantum technologies.

The novelty of this updated framework lies in its ability to evaluate what truly constitutes a part of the commons — and, consequently, who controls resources within

governed spaces. Importantly, Graefrath and Jahn (2024) suggest that this evaluation can inform deeper consideration of the ethical and normative implications surrounding the use of these spaces and the security implications for global cooperation. This exploratory research, therefore, has the potential to illuminate the governance of quantum technologies within the current context of great-power competition for supremacy.[6]

In the next section, this framework is applied to explore whether quantum technologies operate as new spaces within the cyber domain that are true commons or spheres of control. To further explore the real-world governance implications gleaned from evaluating quantum technologies through a global commons approach, this working paper focuses specifically on the development of quantum-enhanced intelligent transportation systems (QEITS) in the discussion of the results, for two reasons. First, the integration of quantum, particularly algorithms and their optimization capabilities, is a promising near-term and practical application of the technology. Second, this area requires extensive cooperation among private sector actors, academia and government stakeholders. QEITS link quantum technologies, algorithms, vehicles, individuals, and goods and services across jurisdictional borders and geographies, yet they must operate within defined parameters.

Applying the Framework to Quantum, Cyber and Intelligent Transportation Systems

Although mapping out the impacts and intersections of all quantum technologies across all global domains is beyond the scope and feasibility of this working paper, focusing on the cyber domain is especially relevant to current international politics. The cyber domain remains a largely unexplored aspect of Graefrath and Jahn's (ibid.) global commons framework and serves as a space where many emerging and transformative technologies straddle digital and physical spaces. This makes exploring quantum as an emerging, disruptive and transformative technology within the cyber domain particularly relevant to security scholarship. This application is also relevant for formulating policy recommendations that encourage cooperation despite the growing global competition for supremacy.

Cyberspace differs from other global commons domains because it is not an exclusively physical domain such as the sea, sky, space and polar regions (Hughes 2016). Cyber connects with other domains through human use and interactions with technologies that control and order life in digital-physical spaces. For instance, within smart cities, a future of QEITS will connect people, goods and services across geographical spaces and through digital networks (Csenkey 2025). The connected transportation domain relies on communication and navigation assets to function safely and securely. Consequently, smart cities and intelligent transportation systems (ITS) are potentially vulnerable to malicious cyberattacks. Additionally, ITS connect cyberspace and other global commons domains, such as the sea and sky,

6 See, for instance, Anwar (2025).

as smart vehicles act as sensors to the physical and digital world. When quantum-enhanced, the abilities and capabilities of technologies in all domains may be heightened, thereby making them even more strategically advantageous to control.

Considering the potential applications of quantum technologies within smart cities through ITS introduce a further layer of complexity to understanding cyberspace as a global commons. Digital-physical technologies, such as AVs, and the systems facilitating their communication, such as sixth-generation wireless technology, may require integration into smart city infrastructures as urban spaces become increasingly interconnected and digitized (ibid.). The integration of specific quantum technologies, such as sensors for traffic management or optimized routing algorithms, has a practical application within ITS and further aims to increase the efficacy of systems, services and the movement of people, goods and services across physical space. Because these smart transportation networks exist in both physical and digital domains, with devices collecting and communicating information and transforming it into usable data, they connect domains across traditional state territorial jurisdictions. While the goal of optimizing capabilities might offer pathways to increased universal access to cyberspace, the integration of QEITS into smart cities introduces complex governance challenges across domains. A future with interconnected quantum technologies may create barriers to universal access, largely due to the expertise, resources and conditions necessary for participation.

Quantum technologies hold the promise of significant commercial benefits, military advantages and enhanced security in ungoverned spaces or by expanding accessibility to all. However, their rapid development may also disrupt the existing security landscape and create a perceived need for dominance. Yet the ability to dominate global commons spaces remains a prerogative held by a limited number of states.

Quantum research and development requires substantial expertise, resources and other considerations. Achieving quantum supremacy is contingent upon considerable inputs, including intangible assets such as specialized knowledge, highly skilled personnel, training initiatives and dedicated financial resources to support research. Robust institutional frameworks that foster the growth of enterprises within the technology ecosystem, advanced physical infrastructure (including state-of-the-art laboratories and equipment) and conducive market conditions are also important supports. The physical environment is a relevant consideration for some quantum technologies, given that certain quantum processors require very low temperatures and spaces devoid of noise, such as vibrations and electrical interference, for operation (Chalmers University of Technology 2025). Furthermore, quantum technologies, such as computers, may also demand immense energy resources. Without a focus on efficiency, their development, application and use could substantially exacerbate energy consumption, resulting in harmful environmental impacts (Desdentado et al. 2024).

While the concept of cyberspace as a true global commons is debated in the international security literature (Deibert and Crete-Nishihata 2012), the current technological landscape — characterized by increasing digitization and interconnectedness of human activities, services and commodities — shows an expansion of spheres of control. This expansion of control into the cyber domain has resulted, in some cases, in an expansion of authoritarian values (Deibert 2015), as not all states agree on the characterization of spaces as global commons. For instance,

Russia opposes the framing of cyberspace as a global commons and seeks to delineate its perceived territorial control and exert sovereignty over national internets through international fora (Raymond and Sherman 2024). Similarly, China leverages technical capabilities and domestic laws to define acceptable activities within a closed national cyberspace to ensure that it falls within its exclusive jurisdiction of control (Pei 2024). In these cases, an authoritarian vision of sovereignty over a national cyberspace[7] defines governance, guiding values and activities conducted therein (Raymond and Sherman 2023).[8]

Values ultimately define the parameters of acceptable behaviour and use within a given domain and all activities therein. Consequently, the potential capabilities of quantum technologies, particularly computing, present mechanisms for control in the cyber global commons, primarily due to the limitations in widespread accessibility and state capacity to effectively leverage the technologies' strategic advantages. Thus, the scramble for quantum supremacy in the global commons is limited to great-power states as they vie to further enhance the spheres of control in the cyber domain.

Yet this geopolitical competition for technological supremacy has not escalated into direct conflict[9] but rather manifests as economic rivalries rooted in state-centric foreign and domestic technology policies and programs. An example of this is national standard-setting initiatives for post-quantum cryptographic algorithms as mechanisms to dominate global commons spaces. By establishing standards, hegemonic powers can potentially expand their control within the global cyber commons, effectively regulating access to the possible advantages of quantum technologies. This scenario is contingent upon other states' adherence to these rules.

Dominating Spaces Through Standards

Quantum technologies, emerging as a key strategic advantage and as a means of exerting control over other domains in the global commons, are becoming new spaces of geopolitical competition. The analysis in this working paper reveals a central issue: the potential for a few powerful states, possessing the means to control access and set priorities, to dominate the parameters of the quantum advantage.

Powerful actors exert control through regulation and the establishment of standards. Yet, by establishing a common framework, standards may have the potential to foster a true commons, allowing actors to participate on a more equitable basis. For example, the United States' National Institute of Standards and Technology (NIST) is working to establish standard sets of encryption algorithms aimed at securing information from cyberattacks by actors with access to a fully fledged quantum computer. Similarly, the European Telecommunications Standards Institute (ETSI) also sets standards but with a different approach to quantum-safe cryptography.[10] By issuing an open call for quantum-resistant cryptographic algorithm candidates, NIST positioned the establishment of standards as a public competition based on an assumption of equal contribution from all actors (NIST 2025). However, the evaluation

7 Rather than an open and inclusive global commons space.

8 The author is grateful to the reviewers for drawing attention to the issues presented in this paragraph.

9 As of April 2025.

10 See Antipolis (2023). ETSI focuses on the security evaluation of quantum key distribution modules.

criteria and selection process for candidates, while based on public feedback and review, was still constrained by the parameters of national security and economic advantages.[11] The "winning" quantum-safe algorithms-cum-standards are ultimately designed to prioritize the security interests and enhance the strategic advantages of rulemakers — in this case, the United States through the US Department of Commerce.[12]

Great-power states and their standard-setting bodies establish the parameters of what counts as the global commons and ultimately dominate these spaces as spheres of control. This is an important consideration because even states with the expertise, resources and environmental conditions to leverage quantum technologies must decide which standards to adopt. In the global commons framework, quantum-safe cryptographic algorithms that are adopted as standards act as a way to extend the sphere of control over specific quantum technology use and access to resources within cyberspace. While states such as Canada — possessing the expertise and growing resources through public and private investment — theoretically could leverage the future potential of quantum technologies to advance strategic objectives across domains, simply identifying and controlling the global commons is not the only consideration.

Cross-border and domain cooperation is essential for the good governance of quantum technologies because their development, deployment and application — much like their future integration into ITS — cannot succeed in isolation, demanding shared resources and diverse expertise.

In sum, realizing a practical quantum advantage for problem solving across domains requires collaboration. It also requires cooperation among stakeholders from a variety of impacted fields that share a common vision of accessibility. To be sure, the technological landscape is dynamic and constantly changing, with new technologies emerging and existing ones being enhanced. Additionally, private actors and research institutions are also competitors in the race for quantum supremacy — not only states. While the race for technological supremacy continues as digital-physical spaces, technologies and our lives become increasingly interconnected, the pursuit of practical advantages from emerging and transformative technologies offers an opportunity to reframe spheres of control within the global commons as spaces for societal betterment.

Implications

With 2025 designated by the United Nations as the International Year of Quantum Science and Technology, the narrative surrounding digital technologies as part of the global commons has become even more prominent and critical to address. It is essential to identify shared spaces for current and future collaborations on global technology governances rather than dwell on the dilemmas of ungovernable, wicked problems. For example, both the World Economic Forum (Siddarth and Weyl 2021) and the North Atlantic Treaty Organization (2024) emphasize the importance of identifying the current spaces and technologies within the global commons.

11 See https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization; Alagic et al. (2025).

12 NIST is part of the US Department of Commerce.

However, it is still unclear if a true commons is achievable, considering the current policy environment and the politicization of quantum technology development.

Through the application and evaluation of quantum technologies as potentially part of the global commons, this working paper attempts to provide like-minded states with a stronger foundation for initiating cooperation on the ethical and normative implications of these technologies. This is especially important given the current volatility in global cooperation and the increasing influence of the private sector in shaping the parameters of technology governance.

Recommendations

Drawing on the global commons framework, this paper recommends that even as quantum technologies are increasingly brought under the control of select actors to limit their strategic advantages, cooperation should not be seen as an obstacle to achieving a practical quantum advantage. Instead, cooperation on activities such as standard-setting, grounded in and paired with democratic values (such as accountability, equity and inclusivity), offer an opportunity to define the application of quantum technologies for the common good. As Matthew da Mota argues, "Standards are not a perfect governance tool," but they can hold actors accountable (da Mota 2024, 7). Although quantum supremacy is a moving target, and it is still unclear if a true commons is feasible for this domain, actors should focus on creating practical solution spaces. Two such options are offered below.

- **Recommendation 1:** Establish an international multi-stakeholder standards working group focused on promoting accessibility, especially for states without the expertise, resources and suitable conditions for technological advancement and operation in this domain. This group could be comprised of stakeholders in academia, industry, relevant state actors, civil society and citizen groups. Although NIST, ETSI and other standard-setting bodies offer nationally aligned options, barriers to entry exist. Therefore, access must be improved to prevent a future where the world is divided into quantum "haves" with de facto domination and "have-nots." This is an important consideration, as once a fully fledged quantum computer becomes widely available and demonstrates the ability to break existing cryptographic algorithms, states lacking the necessary defences will be vulnerable — and face a quantum disadvantage.

- **Recommendation 2:** Technical standards should be paired with commitments to ethical conduct. Grounded in an emphasis on protecting human rights, commitments to ethical conduct could focus on promoting accountability, inclusivity and equity in technology development and application. The above-mentioned working group could work to balance security and economic interests with the need for global cooperation in defining the use and governance of quantum technologies for societal benefit, shifting the focus away from potential harm and toward a commitment to an open, inclusive and secure space. Collaboration across actor communities is essential to define and reshape conduct in the global commons that would come with access, prioritizing democratic values over the potential for authoritarian control.

Acknowledgements

The author is grateful for the feedback graciously provided by John Bruce, Dariush Ebrahimi, Xiao Han, Laine McCrory and Caleigh Wong. She would also like to thank Reanne Cayenne and Dianna H. English, the Digital Policy Hub team and the CIGI Publications team, especially Susan Bubak. This research was produced with support from CIGI and Mitacs Accelerate as part of the Digital Policy Hub fellowship program. Any errors and omissions are those of the author, and the opinions expressed in this paper do not represent an official position of any affiliated individuals or institutions.

About the Author

Kristen Csenkey, Ph.D., is a post-doctoral fellow with the CIGI Digital Policy Hub and a Social Sciences and Humanities Research Council post-doctoral fellow at the Brian Mulroney Institute of Government, St. Francis Xavier University. Her research broadly focuses on global cyber governance, technology interdependence and geopolitics. Follow her work at www.kristencsenkey.com.

Works Cited

Alagic, Gorjan, Maxime Bros, Pierre Ciadoux, David Cooper, Quynh Dang, Thinh Dang, John Kelsey et al. 2025. *Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process*. NIST Internal Report 8545. https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8545.pdf.

Antipolis, Sophia. 2023. "ETSI releases World First Protection Profile for Quantum Key Distribution." Press release, April 27. www.etsi.org/newsroom/press-releases/2222-etsi-releases-world-first-protection-profile-for-quantum-key-distribution.

Anwar, Ruqiya. 2025. "Why US-China quantum race is the most critical contest of our time." *South China Morning Post*, January 14. www.scmp.com/opinion/china-opinion/article/3294055/why-us-china-quantum-race-most-critical-contest-our-time.

Arrow, Joan. 2025. "Don't believe the hype — quantum tech can't yet solve real-world problems." *Nature* 640 (8059): 572. https://doi.org/10.1038/d41586-025-01142-8.

Carr, Madeline and Feja Lesniewska. 2020. "Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance." *International Relations* 34 (3): 391–412. https://doi.org/10.1177/0047117820948247.

Chalmers University of Technology. 2025. "Record cold quantum refrigerator paves way for reliable quantum computers." *ScienceDaily*, January 9. www.sciencedaily.com/releases/2025/01/250109125828.htm.

Chou, Charina, James Manyika and Hartmut Neven. 2025. "The Race to Lead the Quantum Future." *Foreign Affairs*, January 7. www.foreignaffairs.com/united-states/race-lead-quantum-future-chou-manyika-neven.

Colding, Johan, Stephan Barthel and Patrik Sörqvist. 2019. “Wicked Problems of Smart Cities.” *Smart Cities* 2 (4): 512–21. https://doi.org/10.3390/smartcities2040031.

Csenkey, Kristen. 2025. “Governing the Risks of Quantum-Enhanced Transportation Systems.” Digital Policy Hub Working Paper. www.cigionline.org/static/documents/DPH-paper-Csenkey.pdf.

Csenkey, Kristen and Nina Bindel. 2023. “Post-quantum cryptographic assemblages and the governance of the quantum threat.” *Journal of Cybersecurity* 9 (1): tyad001. https://doi.org/10.1093/cybsec/tyad001.

Csenkey, Kristen, Julie Clark, Benjamin T. Johnson and Alexander Landry. 2025. “Strategic Implications of Quantum Sensors and their Application in the Arctic.” Policy Brief. North American and Arctic Defence and Security Network. https://naadsn.ca/wp-content/uploads/2025/04/25mar-Strategic-Implications-Quantum-Sensors-Arctic_KC-JC-BTJ-AL-NAADSN-Policy-Brief-EN.pdf.

da Mota, Matthew. 2024. “Standards as a Basis for the Global Governance of AI in Research.” Digital Policy Hub Working Paper. www.cigionline.org/static/documents/DPH-paper-daMota_kSzPGNL.pdf.

Deibert, Ronald J. 2015. “Authoritarianism Goes Global: Cyberspace Under Siege.” *Journal of Democracy* 26 (3): 64–78. www.journalofdemocracy.org/articles/authoritarianism-goes-global-cyberspace-under-siege/.

Deibert, Ronald J. and Masashi Crete-Nishihata. 2012. “Global Governance and the Spread of Cyberspace Controls.” *Global Governance* 18 (3): 339–61. www.jstor.org/stable/23269961.

Desdentado, Elena, Coral Calero, Ma Ángeles Moraga, Manuel Serrano and Félix García. 2024. “Exploring the trade-off between computational power and energy efficiency: An analysis of the evolution of quantum computing and its relation to classical computing.” *Journal of Systems and Software* 217: 112165. https://doi.org/10.1016/j.jss.2024.112165.

Feakin, Tobias. 2024. “Navigating the New Geopolitics of Tech.” *Harvard Business Review*, November 11. https://hbr.org/2024/11/navigating-the-new-geopolitics-of-tech.

Gargeyas, Arjun. 2021. “Has China achieved its leap to ‘quantum supremacy’?” *South China Morning Post*, December 23. www.scmp.com/comment/opinion/article/3160523/has-china-achieved-its-leap-quantum-supremacy.

Govella, Kristi. 2019. “Technology and Tensions in the Global Commons.” *Fletcher Security Review* 6 (1): 37–44. www.fletchersecurity.org/summer-2019-national-security.

Graefrath, Moritz S. and Marcel Jahn. 2024. “Political Spaces Beyond the Nation State: The Global Commons in International Security Studies.” *Global Studies Quarterly* 4 (4): ksae087. https://doi.org/10.1093/isagsq/ksae087.

Hibat-Allah, Mohamed, Marta Mauri, Juan Carrasquilla and Alejandro Perdomo-Ortiz. 2024. “A framework for demonstrating practical quantum advantage: comparing quantum against classical generative models.” *Communications Physics* 7, article no. 68. https://doi.org/10.1038/s42005-024-01552-6.

Hughes, Rex B. 2016. “The Autonomous Vehicle Revolution And The Global Commons.” *SAIS Review of International Affairs* 36 (2): 41–56. https://doi.org/10.1353/sais.2016.0019.

Kim, Jungsang and Christopher Monroe. 2024. “America is the undisputed world leader in quantum computing even though China spends 8x more on the technology — but an own goal could soon erode U.S. dominance.” *Fortune*, April 12. https://fortune.com/2024/04/12/america-undisputed-world-leader-quantum-computing-even-though-china-spends-technology-us-dominance/.

Krelina, Michal. 2025. “An Introduction to Military Quantum Technology for Policymakers.” Stockholm International Peace Research Institute Background Paper. March. https://doi.org/10.55163/DRDQ1599.

Lehtimäki, Hanna, Marjaana Karhu, Juha M. Kotilainen, Rauno Sairinen, Ari Jokilaakso, Ulla Lassi and Elina Huttunen-Saarivirta. 2024. “Sustainability of the use of critical raw materials in electric vehicle batteries: A transdisciplinary review.” *Environmental Challenges* 16: 100966. https://doi.org/10.1016/j.envc.2024.100966.

Malone, Eloise F. and Michael J. Malone. 2013. “The ‘wicked problem’ of cybersecurity policy: analysis of United States and Canadian policy response.” *Canadian Foreign Policy Journal* 19 (2): 158–77. https://doi.org/10.1080/11926422.2013.805152.

Marchant, Gary E. 2020. “Governance of Emerging Technologies as a Wicked Problem.” *Vanderbilt Law Review* 73 (6): 1861–77. https://scholarship.law.vanderbilt.edu/vlr/vol73/iss6/8/.

Mosca, Michele and Marco Piani. 2022. *2021 Quantum Threat Timeline Report*. Global Risk Institute. https://info.quintessencelabs.com/hubfs/Quantum-Threat-Timeline-Report-2021-full-report-final%20(1).pdf.

NIST. 2025. “NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption.” News release, March 11. www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption.

North Atlantic Treaty Organization. 2024. “The Scramble for the Global Commons in the Next Security Era.” February 2. www.act.nato.int/article/the-scramble-for-the-global-commons-in-the-next-security-era/.

Pei, Minxin. 2024. “China’s Secret to Controlling the Internet.” *Foreign Policy*, February 18. https://foreignpolicy.com/2024/02/18/china-internet-control-ccp-technology-cyber-surveillance-policy-sentinel-state/.

Peters, B. Guy. 2017. “What is so wicked about wicked problems? A conceptual analysis and a research program.” *Policy and Society* 36 (3): 385–96. https://doi.org/10.1080/14494035.2017.1361633.

Preskill, John. 2018. “Quantum Computing in the NISQ era and beyond.” *Quantum* 2: 79. https://doi.org/10.22331/q-2018-08-06-79.

Prisco, John. 2024. “It’s A Two-Way Race For Quantum Supremacy.” *Forbes*, November 14. www.forbes.com/councils/forbestechcouncil/2024/11/14/its-a-two-way-race-for-quantum-supremacy/.

Quantum Computing Business. 2024. “The Quantum Insider Projects $1 Trillion In Economic Impact From Quantum Computing By 2035.” Quantum Insider, September 13. https://thequantuminsider.com/2024/09/13/the-quantum-insider-projects-1-trillion-in-economic-impact-from-quantum-computing-by-2035/.

Raymond, Mark and Justin Sherman. 2023. “Authoritarian multilateralism in the global cyber regime complex: The double transformation of an international diplomatic practice.” *Contemporary Security Policy* 45 (1): 110–40. https://doi.org/10.1080/13523260.2023.2269809.

– – –. 2024. “Russia’s UN cyber treaty is a warning for the future of the internet.” *Binding Hook*, October 2. https://bindinghook.com/articles-hooked-on-trends/russias-un-cyber-treaty-is-a-warning-for-the-future-of-the-internet/.

Reuters. 2025. “Trump science policy nominee calls China most formidable technology, science competitor.” *South China Morning Post*, February 25. www.scmp.com/

news/world/united-states-canada/article/3299973/trump-science-policy-nominee-calls-china-most-formidable-technology-science-competitor.

Rittel, Horst W. J. and Melvin M. Webber. 1973. “Dilemmas in a general theory of planning.” *Policy Sciences* 4 (2): 155–69. https://doi.org/10.1007/BF01405730.

Siddarth, Divya and E. Glen Weyl. 2021. “The case for the digital commons.” World Economic Forum, June 2. www.weforum.org/stories/2021/06/the-case-for-the-digital-commons/.

Vogler, John. 2012. “Global Commons Revisited.” *Global Policy* 3 (1): 61–71. https://doi.org/10.1111/j.1758-5899.2011.00156.x.

West, Jessica and Jordan Miller. 2023. *Clearing the Fog: The Grey Zones of Space Governance*. CIGI Paper No. 287. Waterloo, ON: CIGI. www.cigionline.org/publications/clearing-the-fog-the-grey-zones-of-space-governance/.