Centre for International Governance Innovation

Digital Policy Hub

Digital Policy Hub — Working Paper

Governing the Risks of Quantum-Enhanced Transportation Systems

Kristen Csenkey

Fall 2024 cohort

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.

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.

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.

Copyright © 2025 by Kristen Csenkey

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

Centre for International Governance Innovation and CIGI are registered trademarks.

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

Key Points

- Digital technologies integrated into smart city infrastructures are increasingly interconnected, and transformative technologies, such as artificial intelligence and quantum computing, offer new opportunities to enhance and optimize the functioning of transportation networks.
- Understanding the interconnections between these technologies is critical for identifying potential vulnerabilities and developing effective mitigation strategies. However, formal governance frameworks to address these vulnerabilities and that seek to promote security cooperation are absent among democratic states.
- The main objective of this working paper is to explore the transformative technologies connected within the transportation sector as part of smart cities, identify the associated cyber risks and threats and offer recommendations to cooperating democratic states. This paper employs a systematic review of interdisciplinary literature on quantum-enhanced intelligent transportation systems to accomplish this objective. The findings highlight nine key technology areas and the two interrelated concepts of communication and navigation.
- Key cyber risks and corresponding mitigation strategies are identified, emphasizing the need for coordinated data security and the standardization of algorithms to protect against quantum attacks.
- The governance of quantum-enhanced intelligent transportation systems as part of smart cities is particularly relevant to Group of Seven states, especially ahead of the 2025 meeting.

Introduction

Cities bring together people, shared spaces, goods and services through intricate networks of interdependence. Digital technologies play a crucial role in modern urban life, as digitization levels continue to increase globally (Statista 2024, 3). As more people live and work in cities,[1] connected urban environments have become an important interface to address the needs of growing populations, including by improving quality of life, optimizing services and promoting sustainability.

Smart cities are generally characterized by the deployment of technologies in urban spaces to efficiently address specific city-related challenges (Green 2019). Technologies such as artificial intelligence (AI), big data analytics, computers, sensors and communication devices are important to the functioning of society through intelligent transportation systems (ITS) (Chan, Lim and Parthiban 2023; Rani and Sharma 2023; Zhu et al. 2019). The integration of these transformative technologies within ITS has the potential to improve services for users, autonomous vehicle (AV) navigation, traffic management and system efficiency, among other areas (Tchappi et al. 2020; Singh and Gupta 2015). The integration of quantum technologies, in particular, into ITS serves to enhance data processing abilities, security and reliability (Yi et al. 2022). Quantum computing specifically offers the potential to optimize ITS (Wang et al. 2021). Known as quantum-enhanced intelligent transportation systems (QEITS), these technologies have the potential to accelerate the efficiency of smart cities (Agrewal and Sood 2024).

1 See www.statista.com/statistics/270860/urbanization-by-continent/.

The governance of smart cities is increasingly a priority area for states as the process of digitization continues to accelerate the integration of technologies into daily life, especially through the transportation sector. Although viewing smart cities through a technology-centric lens may oversimplify the complexities of urban life (Green 2019), in an era increasingly shaped by technology-defined sovereignty and geopolitical competition, it is crucial to understand how new technologies interact and how states may leverage them to exert their influence in the world. For instance, states with poor human rights records, such as the People's Republic of China, exert significant influence over the development, adoption and deployment of smart city technologies worldwide (Wright, Weber and Walton 2023). Chinese associated companies, such as Huawei, have notably developed and advanced AI-enabled smart city technologies focused on "safety" through surveillance (Cao 2016). Many of these technology systems have already been integrated into city infrastructures across Europe (Briganti 2021) and Asia (Yan 2019), raising security concerns among democratic states (Walton and Weber 2023).

Transportation systems underlie the foundation of a functioning city and are an important part of critical infrastructure. These systems link people, services and goods across regions and borders. ITS is a transformative approach to modernizing transportation infrastructure and is one of the foundations of smart city networks. Yet connected transportation-related devices, vehicles, software and hardware are increasingly vulnerable in an array of environments (Csenkey and Rapin 2024a, 2024b). In addition, ITS and QEITS pose several governance challenges for democratic states as they seek to manage the multiple risks and challenges associated with smart city technologies and their infrastructure. Some examples include the interoperability of systems across national borders, the security of transnational flows of goods and services, the safety of human users and data privacy. This paper seeks to identify the risks and challenge areas associated with QEITS by focusing on their cybersecurity and resiliency.

Objective

Among cooperating democratic and high-tech states within the Group of Seven (G7),[2] the governance of transformative technologies is often positioned as a key to solving societal challenges, ensuring climate-focused economic transitions and national security through regulatory frameworks (G7 Science and Technology Ministers 2024). G7 states are also increasingly considering the need to develop innovative initiatives to address connected global cybersecurity and technology challenges. For instance, the G7 Cyber Expert Group (CEG) recently released a public statement on planning for the opportunities and risks associated with quantum computing (US Department of the Treasury 2024). Yet the CEG's review and recommendations primarily focus on the cybersecurity and resilience of financial systems. More attention is needed to expand the focus to smart cities and transportation systems that are also vulnerable to quantum-enabled threat activity.

Industry and academic leaders have urged for a greater focus on quantum technologies to emphasize national innovation and global cooperation. Tracey Forrest, Paul Samson and Raymond Laflamme (2024) advocate for Canada to lead international quantum science and technology development, while aligning with North Atlantic Treaty Organization spending targets and leveraging the 2025 G7 presidency. The International Council of Quantum Industry Associations' 2024 open letter to Prime

2 The G7 membership is generally defined as states with advanced economies: Canada, France, Germany, Italy, Japan, the United Kingdom and the United States.

Minister Justin Trudeau also stresses the importance of quantum technologies during the G7 presidency.[3] To further highlight the urgency and tangible impact of quantum technologies, this working paper integrates them into real-world applications in the transportation sector within connected smart cities.

Currently, there are no formal international governance frameworks to manage connected technologies in their future applications in smart cities. It is important that states prioritize the integration of democratic values into technology policies and strategies (Csenkey and Graver 2024). This paper seeks to address this policy gap through evidence-based research and nuanced recommendations. Its goal is to provide a set of recommendations for G7 leaders ahead of the 2025 meeting in Alberta.

In light of the global challenge of smart city governance, it is important to ask: What transformative technologies are associated with the contemporary landscape of QEITS? And, relatedly, how are these technologies connected to the infrastructure of smart city transportation systems?

Identifying and Situating the Technologies

A systematic literature review explores the interdisciplinary literature on smart cities, transportation systems and infrastructure (Elvas and Ferreira 2021; Bahmanova and Lace 2024). This review focuses on transformative technologies in ITS and QEITS by drawing on the Web of Science Core Collection database and covering the period from 2004 to the present. To further refine the literature search, relevant keyword[4] searches using Boolean operators were employed. The top 10 Web of Science categories[5] were selected and ranked, and a set of exclusion criteria was further applied.[6] The results of the systematic literature review are presented in Table 1 and accompanied by an analysis of the emergent key technologies and concepts, following Luis B. Elvas and Joao C. Ferreira (2021) and Monika Agrewal and Sandeep Kumar Sood (2024). The review further explores the core concepts associated with cyber risks and threats, partially drawing on the cybersecurity literature reviewed by Alona Bahmanova and Natalja Lace (2024) and relying on the data set developed during the course of this study. The details are discussed in the proceeding section.

3 International Council of Quantum Industry Associations to Trudeau: www.quantumindustrycanada.ca/wp-content/uploads/2024/10/ENG-20241011-ICQIA-letter-to-Canadas-Prime-Minister-re.-G7-quantum.pdf.

4 The initial search included a keyword search in the topic area of "intelligent transportation systems" OR "ITS" AND "technolog.*" This resulted in an initial n=577,554 hits. The results were further refined to n=338,848 after exclusions were applied to the first data corpus. The second search resulted in n=5,681 hits after the application of the following keywords: "smart cit*" AND "transport* system*" AND "infrastructur*" to the initial search topic areas. In the third search, the results were further refined by including only the top 10 Web of Science categories, which further narrowed the results to n=4,879 hits. The final search result was n=18 after the inclusion of the keyword "quantum" and a preliminary manual validation of sources. This reduced the data to a more manageable number for manual analysis, which included ensuring applicability, and reading and reviewing the papers.

5 Recognizing that articles can have multiple Web of Science categories ascribed to them, the top 10 categories were selected because they comprise more than 50 percent of the second search results (n=5,681).

6 Exclusions included non-peer-reviewed academic articles and publications outside of the date range. In the third search, exclusions included articles outside of the top 10 Web of Science categories. The top 10 Web of Science categories are: engineering electrical electronic; transportation science technology; engineering civil; telecommunications; computer science information systems; computer science artificial intelligence; transportation; instruments instrumentation; computer science theory methods; and engineering multidisciplinary.

Table 1: Key Technologies Associated with QEITS

Technology or System		Reference(s)
6G		Noor-A-Rahim et al. (2022)
AI/machine learning/deep learning		Hamza et al. (2022); Derrouz et al. (2022); Lakshmi et al. (2022); Noor-A-Rahim et al. (2022); Qu, Liu and Zheng (2023); Yamany, Moustafa and Turnbull (2023)
AVs		He et al. (2024); Noor-A-Rahim et al. (2022); Yamany, Moustafa and Turnbull (2023)
Blockchain		Yi (2023)
Edge/cloud computing		Shu and Li (2023)
IoV		Hamza et al. (2022); Yang et al. (2024); Yi et al. (2022)
PKI		Pu et al. (2024)
VANETs		Dharminder and Mishra (2020); Liu et al. (2019, 2022); Pu et al. (2024); Shu and Li (2023)
Quantum technology	Post-quantum algorithms and validation schemes, quantum-safe encryption	Dharminder and Mishra (2020); Khalid et al. (2024); Yi (2023)
	Quantum key distribution	Khalid et al. (2024); Yang et al. (2024); Yi et al. (2022)
	Quantum computing and algorithms for optimization	Hamza et al. (2022); Azad et al. (2023); Derrouz et al. (2022); Dharminder and Mishra (2020); Feng et al. (2021); Lakshmi et al. (2022); Lin and Tang (2022); Shu and Li (2023); Qu, Liu and Zheng (2023); Yamany, Moustafa and Turnbull (2023)
	Quantum-enhanced machine learning/AI	Yi (2023)
	Quantum sensing	He et al. (2024)

Source: Author and citations therein.

Emergent Key Technologies and Concepts in Smart Cities

QEITS rely on several interrelated technologies, which are essential components of broader smart city infrastructures. The review identified nine key technology areas within this emerging field. They are simplified for ease of understanding:

- sixth generation (6G);
- AI/machine learning/deep learning;[7]
- AVs;
- blockchain;
- edge and cloud computing;

7 Although there are differences in the details of AI, machine learning and deep learning, these technologies were categorized together for ease of understanding.

- Internet of Vehicles (IoV);
- public key infrastructure (PKI);
- vehicular ad hoc networks (VANETs); and
- quantum technologies.

The nine technology areas include a range of software, hardware, physical devices and platform technologies. Quantum technologies are categorized into five general subcategories to better understand their nuanced connections within the broader smart city infrastructure.

The technologies listed in Table 1 are connected to the infrastructure of smart city transportation systems through the interrelated concepts of communication and navigation.

Transformative technologies are connected through shared communication goals, which are essential for traffic management and navigation, coordination and fleet management, among other objectives. These technologies, including VANETs, IoV, blockchain, cloud computing and 6G, enable device communication and data exchange. AI-enhanced technologies improve the efficiency of communication by facilitating real-time decision making and predictive maintenance. The application and integration of quantum algorithms into the cyber ecosystem aim to further optimize decision making and predictions by surpassing the limitations of classical computing capabilities. Quantum optimization, often enhanced by AI, has the potential to improve the efficiency of solving complex challenges, including the communication and coordination of AV navigation.

Underpinning both communication and navigation is the need for secure digital infrastructure, systems and data. Unfortunately, the technologies that underpin the connected and transformative technology-enhanced transportation sector pose cybersecurity risks within the continually evolving digital threat landscape. These risks and possible mitigation strategies are explored in the next subsection.

Cybersecurity Risks and Mitigation Strategies

Although the main objective of ITS is to enhance services and the movement of goods and people, there are other second-order effects that must be considered by cooperating states. Cyber risks and attacks associated with the transportation digital ecosystem as part of modern smart cities are one such second-order effect that may impact the functioning of the overall system.

Based on the analysis of the review results,[8] there are several primary cyber risks that emerge from the key technology areas, including:

- data privacy breaches and data corruption that may expose sensitive data or alter information;
- adversarial attacks on AI/machine learning models that may train data to change decision-making outcomes, including those related to communication and navigation goals; and

8 The results are n=18 articles, as specified in Table 1.

- quantum attacks using a quantum computer to break classical cryptographic algorithms. This type of attack could result in compromised sensitive information.

The safety and security of data is an integral part of the operation of smart cities. Connected, enhanced and intelligent transportation technologies collect, process and store vast amounts of data about the surrounding environment and human behaviours (Agrewal and Sood 2024). This data has the potential to be exploited, disrupted and manipulated by malicious state and non-state actors for the purposes of harm, including to support military objectives, and intelligence-gathering, espionage, criminal and commercial surveillance activities. These harms could be exacerbated by using quantum and AI technologies separately or combined. Enhancing cyber resiliency is crucial to mitigating the potential threats. This leads to the question: What solutions are available to address the associated risks as part of cyber resiliency?

By focusing on data protection throughout its life cycle — from collection to deployment — cyber resiliency can be significantly enhanced. One way to accomplish this task is through implementing strong encryption through robust security protocols. Another important strategy to mitigate cybersecurity-related risks is through the coordinated adoption of quantum-resistant cryptographic algorithms (Csenkey and Bindel 2023). These types of algorithms have the potential to protect sensitive information against attacks by malicious actors via the use of quantum computers. By implementing robust security protocols and standardized post-quantum cryptographic algorithms to ensure the protection of data, the risks associated with QEITS as part of smart cities can be mitigated.

The integration of AI into smart city infrastructures through QEITS may further enhance decision-making capabilities, but it also exposes these systems to significant cybersecurity risks. Strong cybersecurity measures are essential to mitigate these threats and protect critical infrastructure. National governments must be deliberate in their efforts to secure AI systems as they are integrated within QEITS. Cooperating states, as part of the Five Eyes[9] alliance, are currently working to enhance the safe design and secure implementation of AI systems. For instance, in April 2024, the Five Eyes jointly released an advisory with best practices for deploying secure and resilient AI systems. Some of the security measures set out in the advisory underscore the importance of applying secure-by-design principles and using cryptographic methods and digital signatures to protect sensitive information from unauthorized access (US National Security Agency Artificial Intelligence Security Center et al. 2024, 4, 5). The interplay between transformative technologies such as AI and cybersecurity within QEITS must be understood within international governance frameworks.

To be sure, many of the technologies examined in this study are still in the early stages of development and have not yet reached full operational maturity. Similarly, many of the cyberthreats associated with these technologies have yet to be realized — for instance, an actor possessing a fully fledged quantum computer capable of breaking existing encryption standards. Furthermore, many smart cities rely on a complex interplay of digital, legacy and analogue technologies, creating intricate cyber-physical infrastructures that are continually evolving.

There are many things that we do not know about the risks and consequences of intricately connected transportation systems. For example, do all stakeholders

9 The Five Eyes member states are Australia, Canada, New Zealand, the United Kingdom and the United States. These states cooperate on intelligence sharing and other security-related activities.

in the cyber ecosystem, including private sector parts manufacturers, adhere to similar security protocols? Would they follow suggested recommendations or are more binding solutions needed? Will the innovative solutions presented by the many connected technologies within the ecosystem truly result in operational efficiency? What is clear, however, is that these technologies and systems underlie critical infrastructure and data — and therefore people, goods, the environment and services are potentially vulnerable to cybersecurity threats. Moreover, transportation networks connect people, services and goods across national borders, creating a need for states to find ways to cooperate on their security. While the future of smart cities may be shaped by the complexities of the integration of many technologies, it is clear that effective global technology governance will be key to addressing these challenges. Good data governance and coordination on standardization are two such recommendations gleaned from this study and are described in the proceeding section.

Recommendations for G7 Member States

Technologies — whether AI or quantum-enhanced — are not independent from the political, economic and social aspects of society. Technologies can be used by states and other actors to shift power in the international system, gain a competitive advantage over others, and control and monitor human behaviour. Yet cities, in which humans increasingly live, work and interact, must function in the public interest to ultimately benefit society. This is where G7 states can play an important role in technology governance. Global technology leaders and government decision makers must work together to implement strategies that understand the interconnected technologies and risks and build in mitigation plans to ensure a future of safe and secure connection through increasingly digitized transportation networks. Based on the results, discussion and analysis conducted in this paper, it is recommended that G7 states specifically place the issue of governing the risks of QEITS on the agenda at the 2025 annual meeting. The following recommendations could be led through the G7 Science and Technology Ministers' Meeting and the CEG.

- **Recommendation 1:** Build durable partnerships to develop a shared language of transportation-focused cybersecurity with a specific emphasis on data security. These partnerships should include an emphasis on identifying, streamlining and sustaining consistent approaches to international collaboration on data governance. Part of this approach to data governance must include the safety and security of humans in the development and diffusion of technologies without ascribing authoritarian and autocratic principles. Increased efficiency and optimization of ITS must not come at the expense of human security and democratic AI governance principles.

- **Recommendation 2:** Coordinate the adoption of encryption standards across cooperating states to ensure that transnational data flows — and the movement of people, goods and services — are secure in a future with accessible, fully fledged quantum computers. Although G7 states have their own standardization bodies[10] and are working toward the transition from quantum-vulnerable cryptographic algorithms to post-quantum algorithms, much of this work is national in focus (for example, see Moody et al. 2024). International coordination of standards through engagement with multi-level governmental stakeholders across borders is important to facilitate the adoption of post-quantum cryptography. Coordinated efforts

10 Including the US National Institute of Standards and Technology, the European Telecommunications Standards Institute and the Japanese Industrial Standards Committee.

should include streamlined timelines and achievable deadlines to protect digital infrastructure.

Conclusion

As Nanjira Sambuli aptly notes, "It takes more than infrastructure to build a city" (quoted in Klaus et al. 2024). In the context of digitally connected and technology-enhanced smart cities, it will take a coordinated effort to ensure the safety and security of the transportation sector — and, to an extent, broader society. The increasing rates of digitization and urbanization necessitate shared goals between like-minded states to advance democratic values despite increasing geopolitical fragmentation and technological competition. Combining data protections and the implementation of globally aligned encryption standards with a balanced understanding of the technologies and associated risks, will help ensure more nuanced approaches to governance. The recommendations put forward in this study must be accompanied by an open sharing of best practices and experiences and a focus on identifying common interests between cooperating states. The 2025 G7 meeting in Canada is the ideal place to discuss the enactment of these recommendations.

Acronyms and Abbreviations

6G	sixth generation
AI	artificial intelligence
AV	autonomous vehicle
CEG	Cyber Expert Group
G7	Group of Seven
IoV	Internet of Vehicles
ITS	intelligent transportation systems
PKI	public key infrastructure
QEITS	quantum-enhanced intelligent transportation systems
VANETs	vehicular ad hoc networks

Acknowledgements

The author is grateful for the feedback graciously provided by John Bruce, Dariush Ebrahimi and Michael P. A. Murphy. She would also like to thank the Digital Policy Hub team (especially Reanne Cayenne and Dianna H. English) for their continued support, and the CIGI Publications team (especially Susan Bubak). The author's work was funded by a Mitacs Accelerate Fellowship through CIGI and Wilfrid Laurier University. 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 CIGI Digital Policy Hub post-doctoral fellow, a Canadian Maritime Security Network post-doctoral fellow, and a North American and Arctic Defence and Security Network research fellow. Her research broadly focuses on global cyber governance, technology interdependence and geopolitics. Follow her work at www.kristencsenkey.com.

Works Cited

Agrewal, Monika and Sandeep Kumar Sood. 2024. "A scientometric analysis of quantum driven innovations in intelligent transportation systems." *Engineering Applications of Artificial Intelligence* 138: 109258. https://doi.org/10.1016/j.engappai.2024.109258.

Azad, Utkarsh, Bikash K. Behera, Emad A. Ahmed, Prasanta K. Panigrahi and Ahmed Farouk. 2023. "Solving Vehicle Routing Problem Using Quantum Approximate Optimization Algorithm." *IEEE Transactions on Intelligent Transportation Systems* 24 (7): 7564–73. https://doi.org/10.1109/TITS.2022.3172241.

Bahmanova, Alona and Natalja Lace. 2024. "From cyber security to cyber resilience: Safeguarding against evolving risks in the digital landscape." In *New Trends in Contemporary Economics, Business and Management. Selected Proceedings of the 14th International Scientific Conference "Business and Management 2024"*, 345–53. Vilnius, Lithuania: Vilnius Gediminas Technical University. https://doi.org/10.3846/bm.2024.1317.

Briganti, Alessandra. 2021. "Serbia's smart city has become a political flashpoint." *Wired*, August 10. www.wired.com/story/belgrade-huawei-cameras/.

Cao, Zhihui. 2016. "Nowhere to hide: Building safe cities with technology enablers and AI." HuaweiTech. July. www.huawei.com/en/huaweitech/publication/winwin/ai/nowhere-to-hide.

Chan, Robin Kuok Cheong, Joanne Mun-Yee Lim and Rajendran Parthiban. 2023. "Missing Traffic Data Imputation for Artificial Intelligence in Intelligent Transportation Systems: Review of Methods, Limitations, and Challenges." *IEEE Access* 11: 34080–93. https://doi.org/10.1109/ACCESS.2023.3264216.

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 and Aniska Graver. 2024. "Canada's national quantum strategy one year on." *Canadian Foreign Policy Journal* 30 (3): 295–306. https://doi.org/10.1080/11926422.2024.2397970.

Csenkey, Kristen and Alexis Rapin. 2024a. "Entre puissance et tension: l'électrification des armées face aux défis de la cybersécurité." Le Rubicon, May 2. https://lerubicon.org/entre-puissance-et-tension-lelectrification-des-armees-face-aux-defis-de-la-cybersecurite/.

– – –. 2024b. "Power and Tension: The Cyber Security Problems of Military Electrification." War on the Rocks, June 4. https://warontherocks.com/2024/06/power-and-tension-the-cyber-security-problems-of-military-electrification/.

Derrouz, Hatim, Alberto Cabri, Hamd Ait Abdelali, Rachid Oulad Haj Thami, François Bourzeix, Stefano Rovetta and Francesco Masulli. 2022. "End-to-end quantum-inspired method for vehicle classification based on video stream." *Neural Computing and Applications* 34 (7): 5561–76. https://doi.org/10.1007/s00521-021-06718-9.

Dharminder, Dharminder and Dheerendra Mishra. 2020. "LCPPA: Lattice-based conditional privacy preserving authentication in vehicular communication." *Transactions on Emerging Telecommunications Technologies* 31 (2): e3810. https://doi.org/10.1002/ett.3810.

Elvas, Luis B. and Joao C. Ferreira. 2021. "Intelligent Transportation Systems for Electric Vehicles." *Energies* 14 (17): 5550. https://doi.org/10.3390/en14175550.

Feng, Li, Amjad Ali, Muddesar Iqbal, Farman Ali, Imran Raza, Muhammad Hameed Siddiqi, Muhammad Shafiq and Syed Asad Hussain. 2021. "Dynamic Wireless Information and Power Transfer Scheme for Nano-Empowered Vehicular Networks." *IEEE Transactions on Intelligent Transportation Systems* 22 (7): 4088–99. https://doi.org/10.1109/TITS.2020.3020254.

Forrest, Tracey, Paul Samson and Raymond Laflamme. 2024. "Quantum Technology, National Security and Defence Spending: A New Frontier." Opinion, Centre for International Governance Innovation, July 8. www.cigionline.org/articles/quantum-technology-national-security-and-defence-spending-a-new-frontier/.

G7 Science and Technology Ministers. 2024. "G7 Science and Technology Ministers' Meeting Communiqué." July 9–11. www.g7italy.it/wp-content/uploads/G7-Science-and-Technology-Ministers-Meeting-Communique.pdf.

Green, Ben. 2019. *The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future*. Cambridge, MA: The MIT Press. https://doi.org/10.7551/mitpress/11555.001.0001.

Hamza, Manar Ahmed, Haya Mesfer Alshahrani, Fahd N. Al-Wesabi, Mesfer Al Duhayyim, Anwer Mustafa Hilal and Hany Mahgoub. 2022. "Artificial Intelligence Based Clustering with Routing Protocol for Internet of Vehicles." *Computers, Materials & Continua* 70 (3): 5835–53. https://doi.org/10.32604/cmc.2022.021059.

He, Wei, Yong Wang, Mu Zhou, Ruidong Li, Liangbo Xie and Zhou Su. 2024. "An Efficient and Robust Fusion Positioning System Based on Entangled Photons." *IEEE Journal on Selected Areas in Communications* 42 (1): 78–92. https://doi.org/10.1109/JSAC.2023.3322759.

Khalid, Haqi, Shaiful Jahari Hashim, Fazirulhisyam Hashim, Waleed Ameen Mahmoud Al-Jawher, Muhammad Akmal Chaudhary and Hamza H. M. Altarturi. 2024. "RAVEN: Robust Anonymous Vehicular End-to-End Encryption and Efficient Mutual Authentication for Post-Quantum Intelligent Transportation Systems." *IEEE Transactions on Intelligent Transportation Systems* 25 (11): 17574–86. https://doi.org/10.1109/TITS.2024.3416060.

Klaus, Ian, Nick Hannes, Dorina Pojani, Nanjira Sambuli and Micah Weinberg. 2024. "New Cities and Capitals: The Future of Urban Planning." Carnegie Endowment of International Peace. Event, September 25. https://carnegieendowment.org/events/2024/09/california-new-cities-and-capitals?lang=en.

Lakshmi, K., Srinivas Nagineni, E. Laxmi Lydia, A. Francis Saviour Devaraj, Sachi Nandan Mohanty, Irina V. Pustokhina and Denis A. Pustokhin. 2022. "An Optimal Deep Learning for Cooperative Intelligent Transportation System." *Computers, Materials & Continua* 72 (1): 19–35. https://doi.org/10.32604/cmc.2022.020244.

Li, Quanrun, Debiao He, Zhichao Yang, Qi Xie and Kim-Kwang Raymond Choo. 2022. "Lattice-Based Conditional Privacy-Preserving Authentication Protocol for the Vehicular Ad Hoc Network." *IEEE Transactions on Vehicular Technology* 71 (4): 4336–47. https://doi.org/10.1109/TVT.2022.3147875.

Lin, Haifeng and Chengpei Tang. 2022. "Intelligent Bus Operation Optimization by Integrating Cases and Data Driven Based on Business Chain and Enhanced Quantum Genetic Algorithm." *IEEE Transactions on Intelligent Transportation Systems* 23 (7): 9869–82. https://doi.org/10.1109/TITS.2021.3121289.

Liu, Hui, Yining Sun, Yan Xu, Rui Xu and Zhuo Wei. 2019. “A secure lattice-based anonymous authentication scheme for VANETs.” *Journal of the Chinese Institute of Engineers* 42 (1): 66–73. https://doi.org/10.1080/02533839.2018.1537804.

Moody, Dustin, Ray Perlner, Andrew Regenscheid, Angela Robinson and David Cooper. 2024. “Transition to Post-Quantum Cryptography Standards.” NIST Internal Report 8547 ipd. November. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8547.ipd.

Noor-A-Rahim, Md., Zilong Liu, Haeyoung Lee, Mohammad Omar Khyam, Jianhua He, Dirk Pesch, Klaus Moessner, Walid Saad and H. Vincent Poor. 2022. “6G for Vehicle-to-Everything (V2X) Communications: Enabling Technologies, Challenges, and Opportunities.” *Proceedings of the IEEE* 110 (6): 712–34. https://doi.org/10.1109/JPROC.2022.3173031.

Pu, Lang, Chao Lin, Jingjing Gu, Xinyi Huang and Debiao He. 2024. “Generic Construction of Conditional Privacy-Preserving Certificateless Signatures With Efficient Instantiations for VANETs.” *IEEE Transactions on Information Forensics and Security* 19: 5449–63. https://doi.org/10.1109/TIFS.2024.3402992.

Qu, Zhiguo, Xinzhu Liu and Min Zheng. 2023. “Temporal-Spatial Quantum Graph Convolutional Neural Network Based on Schrödinger Approach for Traffic Congestion Prediction.” *IEEE Transactions on Intelligent Transportation Systems* 24 (8): 8677–86. https://doi.org/10.1109/TITS.2022.3203791.

Rani, Preeti and Rohit Sharma. 2023. “Intelligent transportation system for internet of vehicles based vehicular networks for smart cities.” *Computers and Electrical Engineering* 105: 108543. https://doi.org/10.1016/j.compeleceng.2022.108543.

Shu, Wanneng and Yan Li. 2023. “Joint offloading strategy based on quantum particle swarm optimization for MEC-enabled vehicular networks.” *Digital Communications and Networks* 9 (1): 56–66. https://doi.org/10.1016/j.dcan.2022.03.009.

Singh, Bhupendra and Ankit Gupta. 2015. “Recent trends in intelligent transportation systems: a review.” *Journal of Transport Literature* 9 (2): 30–34. https://doi.org/10.1590/2238-1031.jtl.v9n2a6.

Statista. 2024. *Digital transformation: Statistics report on digital transformation worldwide*. www.statista.com/study/74997/dossier-digital-transformation/.

Tchappi, Igor H., Stéphane Galland, Vivient Corneille Kamla, Jean Claude Kamgang, Yazan Mualla, Amro Najjar and Vincent Hilaire. 2020. “A critical review of the use of holonic paradigm in traffic and transportation systems.” *Engineering Applications of Artificial Intelligence* 90: 103503. https://doi.org/10.1016/j.engappai.2020.103503.

US Department of the Treasury. 2024. “G7 Cyber Expert Group Recommends Action to Combat Financial Sector Risks from Quantum Computing.” Press release, September 25. https://home.treasury.gov/news/press-releases/jy2609.

US National Security Agency Artificial Intelligence Security Center, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, Australian Government (Australian Signals Directorate, Australian Cyber Security Centre), Communications Security Establishment Canada (Canadian Centre for Cyber Security), New Zealand National Cyber Security Centre and UK National Cyber Security Centre. 2024. “Deploying AI Systems Securely: Best Practices for Deploying Secure and Resilient AI Systems.” April. https://media.defense.gov/2024/Apr/15/2003439257/-1/-1/0/CSI-DEPLOYING-AI-SYSTEMS-SECURELY.PDF.

Walton, Gregory and Valentin Weber. 2023. “AI for Urban Public Security: Threats to European Security and Values.” In *Europe’s Strategic Technology Autonomy from China: Assessing Foundational and Emerging Technologies*, edited by Tim Rühlig, 105–17. https://dgap.org/system/files/article_pdfs/DPC%20-%20fully%20study%202023%20-%20final.pdf.

Wang, Sumin, Zhi Pei, Chao Wang and Jie Wu. 2021. “Shaping the Future of the Application of Quantum Computing in Intelligent Transportation System.” *Intelligent and Converged Networks* 2 (4): 259–76. https://doi.org/10.23919/ICN.2021.0019.

Wright, Joss, Valentin Weber and Gregory Finn Walton. 2023. “Identifying potential emerging human rights implications in Chinese smart cities via machine-learning aided patent analysis.” *Internet Policy Review* 12 (3): 1–26. https://doi.org/10.14763/2023.3.1718.

Yamany, Waleed, Nour Moustafa and Benjamin Turnbull. 2023. “OQFL: An Optimized Quantum-Based Federated Learning Framework for Defending Against Adversarial Attacks in Intelligent Transportation Systems.” *IEEE Transactions on Intelligent Transportation Systems* 24 (1): 893–903. https://doi.org/10.1109/TITS.2021.3130906.

Yan, Yau Tsz. 2019. “Smart Cities or Surveillance? Huawei in Central Asia.” The Diplomat, August 7. https://thediplomat.com/2019/08/smart-cities-or-surveillance-huawei-in-central-asia/.

Yang, Ze, Qin Shi, Teng Cheng, Xunji Wang, Rutong Zhang and Lin Yu. 2024. “A security-enhanced authentication scheme for quantum-key-distribution (QKD) enabled Internet of vehicles in multi-cloud environment.” *Vehicular Communications* 48: 100789. https://doi.org/10.1016/j.vehcom.2024.100789.

Yi, Haibo. 2023. “A post-quantum blockchain notary scheme for cross-blockchain exchange.” *Computers and Electrical Engineering* 110: 108832. https://doi.org/10.1016/j.compeleceng.2023.108832.

Yi, Haibo, Ruinan Chi, Xin Huang, Xuejun Cai and Zhe Nie. 2022. “Improving Security of Internet of Vehicles Based on Post-quantum Signatures with Systolic Divisions.” ACM Transactions on Internet Technology 22 (4): 1–15. https://doi.org/10.1145/3410445.

Zhu, Li, Fei Richard Yu, Yige Wang, Bin Ning and Tao Tang. 2019. “Big Data Analytics in Intelligent Transportation Systems: A Survey.” *IEEE Transactions on Intelligent Transportation Systems* 20 (1): 383–98. https://doi.org/10.1109/TITS.2018.2815678.