# Encoding and Securing Space Activities: Legal Challenges Arising from the Advent of 'Quantum Technology for Space'

*Anne-Sophie Martin*[*] *and Steven Freeland*[**]

**Abstract**

Quantum Technologies (QT), and their use in space applications, are potentially transformative innovations with fundamental implications for society and the global economy. A new era of QT is emerging in the space domain, with a range of space missions already carrying quantum cryptography payloads. Both the quantum and space domains have evolved as strategically important technology sectors that address some of the major challenges of the modern digital era, and now they are being used inter-operatively. The paper analyses the intersections between these two sectors. It highlights legal and regulatory issues to be considered at this relatively early stage of 'quantum technology for space', in particular cybersecurity, data transfer protection and liability. As quantum cryptography becomes increasingly important, it is necessary to assess the extent to which those quantum systems utilised in space missions will comply with applicable cybersecurity regulations, current encryption standards, as well as data transfer and protection regulations. The paper also examines the applicability of the UN Space Treaties.

**Keywords:** Quantum technology, space applications, international law, space law, national policy, strategy.

## 1. Introduction – Quantum Technologies as a Transformative Enabler

The paper intends to present a general overview of the legal challenges and principles of quantum technology (QT) applicable to space activities. Quantum technologies are 'enabling and disruptive dual-use technologies',

* Department of Political Sciences, Sapienza University of Rome, Piazzale Aldo Moro, 5, 00185, Rome (Italy) - martin.annesophie@yahoo.fr.

** Emeritus Professor, Western Sydney University and Professorial Fellow, Bond University, Australia – s.freeland@westernsydney.edu.au.

which can be used for both virtuous and malicious goals, as well as for civil and military purposes.[1] QT represents a revolution in the advancement of industry and innovation. The first QT revolution, developed in the 1940s, exploited natural quantum effects, including the Nuclear Magnetic Resonance (NMR) technique.[2] These inventions provided us with computers, optical fibre communications and, ultimately, GPS.

We are now in the second quantum generation[3] based on the creation and control of individual quantum states, which includes quantum computation and quantum cryptography.

Quantum technology is transforming the way activities are conducted in various fields of industry such as aerospace, naval and submarine, chemistry, health care and pharmaceuticals, robotics as well as finance.[4] In particular, it will provide better data prediction, modelling systems, transaction, cryptography and imaging.[5]

In addition, QT might have a significant role to play in helping us to achieve the Sustainable Development Goals (SDGs), as it could offer a new platform for innovation with the potential to transform key activities in a number of industries and domains.[6] In particular, QT can enhance space-based climate data and environmental process modelling, and can reinforce our ability to better assess and predict climate change and natural disasters.[7]

1 M. Krelina, D. Dúbravčík, *Quantum Technology for Defence*, Journal of the Joint Air Power Competence Centre, 35 (2023) 39-46.

2 *The Second Quantum Revolution*, https://www.bnl.gov/quantumcenter/research.php (accessed 07.06.2023).

3 *A Glance at the Second Quantum Revolution*, QTI Blog, 4 May 2022, https://www.qticompany.com/a-glance-at-the-second-quantum-revolution/ (accessed 07.06.2023); A. Hickey, *The quantum revolution: Who, what, when, where, why and how?*, 26 October 2017, https://www.ciodive.com/news/the-quantum-revolution-who-what-when-where-why-and-how/508195/ (accessed 07.06.2023); *see* NATO, *NATO Exploration Quantum Technology for Future Challenges*, 14 October 2022, https://www.act.nato.int/article/nato-exploring-quantum-technology-for-future-challenges/ (accessed 07.06.2023).

4 *How Quantum Will Transform the Future of 5 Industries*, Honeywell, 2020, https://www.honeywell.com/us/en/news/2020/07/how-quantum-will-transform-the-future-of-5-industries (accessed 07.06.2023).

5 J. Farinha et al., *Identifying future critical technologies for space, defence and related civil industries*, European Commission's Joint Research Centre, Publications Office of the European Union, 2023, 12 ss.

6 *See* Capgemini, *Sustainable Development – How Quantum Technologies Can Help Drive the UN's Sustainable Development Goals*, 2022, https://prod.ucwe.capgemini.com/wp-content/uploads/2022/10/Quantum-Technologies__Sustainability_20-09-2022_final.pdf (accessed 07.06.2023).

7 European Commission, Defence Industry and Space, *Quantum Technologies*, https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-research/quantum-technologies_en (accessed 07.06.2023).

Furthermore, quantum technology, in combination with artificial intelligence[8] and machine learning, will be significantly faster and more efficient in many essential functions than the conventional computers.[9]
Even as this technology opens up additional opportunity, there are a range of obstacles and risks to overcome, including interference, error correction and output observance.[10]
One fundamental issue to determine is which law(s) applies to quantum technology? What elements of the UN space treaties apply to the use of quantum technology in space activities?
In this paper, we seek to define the concept of QT and its interactions with space activities, address the challenges at international level, discuss the applicability of the international space legal regime to the use of QT, and consider relevant existing national policies.

## 2. The Concept of Quantum Technology and Its Interactions with Space Activities

In our connected and digitalised society, the reliability of space assets is crucial, and the use of QT will have a role to play in addressing the challenges and threats that can be encountered in space activities.[11]
Quantum technology can be categorised into three main types: (i) quantum sensing and imaging; (ii) communications; and (iii) computing.
*Quantum sensing* is an advanced sensor technology that improves the accuracy of how data are measured and collected,[12] and thus renders data analysis more efficient and productive.
In particular, it will enable less vulnerable guidance systems in outer space, under water, and in the zones overwhelmed by radio-frequency signals.

8 *See* A.S. Martin, S. Freeland, *The Advent of Artificial Intelligence in Space Activities: New Legal Challenges*, Space Policy *55* (2021) (https://doi.org/10.1016/j.spacepol.2020.101408); A.S. Martin, S. Freeland, *Artificial Intelligence –A Challenging Realm for Regulating Space Activities*, Annals of Air and Space Law, XLV(2020) 275-306.

9 P. Lipman, *How Quantum Computing Will Transform Cybersecurity*, January 2021, https://www.forbes.com/sites/forbestechcouncil/2021/01/04/how-quantum-computing-will-transform-cybersecurity/?sh=4c175d1f7d3f (accessed 07.06.2023).

10 A.S. Gillis, *Quantum Computing*, https://www.techtarget.com/whatis/definition/quantum-computing (accessed 07.06.2023).

11 *Quantum Technologies in Space*, Policy White Paper, August 2019, http://www.qtspace.eu/sites/testqtspace.eu/files/other_files/QT%20In%20Space%20-%20White%20Paper%20Final_0.pdf (accessed 07.06.2023).

12 *What is Quantum Sensing?*, BAE Systems, https://www.baesystems.com/en-us/definition/what-is-quantum-sensing#:~:text=is%20Quantum%20Sensing%3F-,What%20is%20Quantum%20Sensing%3F,collected%20at%20the%20atomic%20level (accessed 07.06.2023).

Quantum sensing is expected to improve capabilities for aircraft manufacturers, cybersecurity, defense and intelligence systems, law enforcement, space exploration, mining and more.[13]

*Quantum communications* deal *inter alia* with the protection of data.[14] Today, sensitive data is typically encrypted and then sent across fibre-optic cables and other channels, together with the digital "keys" needed to decode the information. The data and the keys are sent as classical bits—a stream of electrical or optical pulses representing *1*s and *0*s. That makes them vulnerable, as hackers can read and copy bits in transit. Quantum communications takes advantage of the laws of quantum physics to protect data. These laws allow particles to take on a state of super-position, meaning that they can represent multiple combinations of *1* and *0* simultaneously. The particles are known as quantum bits, or *qubits*.
Some companies have taken advantage of this property to create networks for transmitting highly sensitive data based on a process called quantum key distribution (QKD) in which the keys to decrypt the information are encoded and transmitted in a quantum state using *qubits*.

*Quantum computing* is the use of quantum mechanical phenomena, such as superposition and entanglement[15] to solve complex problems and to perform multiple complex calculations simultaneously.[16] This technology is being developed worldwide by companies as Amazon, Google, Hewlett Packard, Hitachi, IBM, and Microsoft.[17]
A new era of QT is emerging in industry, especially in the space domain,[18] with the development of a "quantum space ecosystem"[19] from ground

13 *Idem*.
14 M. Giles, *Explainer: What is quantum communications ?*, MIT Technology Review, 2019, https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/ (accessed 07.06.2023).
15 *Quantum Computers in the Revolution of Artificial Intelligence and Machine Learning*, Medium, March 2023, https://towardsdatascience.com/quantum-computers-in-the-revolution-of-artificial-intelligence-and-machine-learning-c5b0356903f3 (accessed 07.06.2023).
16 A. Pannier, *Strategic Calculation: High-Peformance Computing and Quantum Computing in Europe's Quest for Technological Power*, Etudes de l'IFRI, Ifri, October 2021, 24 ss; IBM, *What is quantum computing ?*, https://www.ibm.com/topics/quantum-computing (accessed 07.06.2023).
17 A.S Gillis, *op. cit.*
18 European Patent Office, *Quantum technologies on the rise in the space sector*, 2 November 2021, https://www.epo.org/news-events/news/2021/20211102a.html (accessed 07.06.2023).
19 M. Krelina, D. Dúbravčík, *Quantum Technology for Defence...*, *op.cit.*, 45. "Quantum ecosystem in space: quantum countermeasures, Quantum communication, quantum sensing, quantum space radar".

segment to GEO and beyond. In fact, QT can be used in space secure communications, in time and frequency transfer, as well as in Earth sensing and observation.[20] A range of space missions have already carried quantum cryptography payloads, such as China's Micius satellite[21] in 2016 providing long-range secure communication. The satellite is used to distribute quantum cryptographic keys to ground stations. In 2019, the nano-satellite SpooQy-1 mission with QKD, developed by the National University of Singapore, utilised for the first time quantum entanglement in space.[22]

Many other projects are exploring, on a national and regional basis, the potential of space-based QT for distributing keys in the field of cryptography, including the European IRIS[2] telecommunications programme,[23] which relies on quantum cryptography through the European Quantum Communication Infrastructure (EuroQCI),[24] and enhanced cybersecurity through a secure-by-design approach for the infrastructure.[25] The EuroQCI will be a secure quantum communications infrastructure, composed of a terrestrial segment relying on a fibre communications networks and a space segment based on satellites. It will safeguard sensitive data and critical infrastructures by integrating quantum-based systems into existing communications infrastructures, providing an additional security layer based on quantum physics. In this way it will emerge as one of the main pillars of the EU's Cybersecurity Strategy over coming decades.

Both the quantum and space domains have evolved as strategically important technology sectors that address some of the major challenges of the modern digital era, and now they are being used inter-operatively.[26] All actors in the

20 ESPI Patent insight report, *Quantum technologies and space*, European Patent Office, 2021, 6 ss.

21 H. Siljak, *China's Quantum Satellite Enables First Totally Secure Long-Rance Messages*, 17 June 2020, https://theconversation.com/chinas-quantum-satellite-enables-first-totally-secure-long-range-messages-140803 (accessed 07.06.2023)

22 *SpooQy-1 shows promise of nanosatellites for quantum networks*, Centre for Quantum Technologies, 25 June 2020; ESA, EO Portal, *SpooQy-1 CubeSat Mission*, December 2019.

23 European Commission, *IRIS²: the New EU Secure Satellite Constellation, Infrastructure for Resilience, Interconnectivity and Security by Satellite*, https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-programme/iriss_en (accessed 26.06.2023).

24 European Commission, *The European Quantum Communication Infrastructure (EuroQCI) Initiative*, https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci (accessed 26.06.2023).

25 *See* Regulations (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023-2027. It makes reference to the European Quantum Communication Infrastructure (EuroQCI).

26 R. Kaltenbaek et al., *Quantum Technologies in Space*, Experimental Astronomy, 51 (2021) 1677-1694.

space ecosystem – governments, space agencies[27] and industry[28] – are interested in quantum technology.

The intersection of quantum computing with the space industry allows two next-generation technologies to collide. With phenomena like quantum entanglement, quantum devices in space can enable the next stage of quantum technology: the quantum internet.[29] Currently, the quantum satellites being developed use QKD, which means that a set of keys are shared between the receiver and sender, allowing a more secure connection. Future satellite projects aim to use quantum entanglement to create an even more secure and faster link. As one commentator has noted, "The quantum-entangled link allows for the teleportation of information at the speed of light, but also means that any attempt to intercept the signal immediately severe the link, making hacking impossible".[30]

## 3. Challenges in the Use of Quantum Technology: International Law Perspectives

The use of quantum technology raises international law questions, including with respect to cybersecurity, data protection and liability. As increasingly more services and products depend on connectivity and new technologies are developed, the number of potential vulnerabilities, as well as the means of exploiting them, will increase accordingly, leading to a rise in the number of cyberattacks.[31]

27 European Space Agency, *Quantum Technologies*, https://technology.esa.int/program/quantum-technologies (accessed 07.06.2023); European Space Agency, *ESA to help develop secure quantum communications*, 23 January 2023, https://www.esa.int/Applications/Connectivity_and_Secure_Communications/ESA_to_help_develop_secure_quantum_communications (accessed 07.06.2023).

28 R. Karayan, *Airbus, Thales et Orange s'allient pour bâtir la constellation européenne de satellites IRIS²*, 2 mai 2023, https://www.usine-digitale.fr/article/airbus-thales-et-orange-s-allient-pour-batir-la-constellation-europeenne-de-satellites-iris-2.N2128916 (accessed 07.06.2023); Thales, *Thales prepares to secure european infrastructures against attacks from future quantum computers*, 14 April 2023, https://www.thalesgroup.com/en/worldwide/group/press_release/thales-prepares-secure-european-infrastructures-against-attacks (accessed 07.06.2023).

29 K. Hughes-Castleberry, *Inside Quantum Technology's Inside Scoop: Quantum and the Space Industry*, 16 December 2022, https://www.insidequantumtechnology.com/news-archive/inside-quantum-technologys-inside-scoop-quantum-and-the-space-industry/ (accessed 07.06.2023).

30 A. Herman, *The Quantum Space Race is Here*, 20 October 2022, https://www.forbes.com/sites/arthurherman/2022/10/20/the-quantum-space-race-is-here/?sh=5cd3e7874764 (accessed 07.06.2023).

31 *Digital Challenges for International Law*, White Paper, International Law Association (ILA), 2023, 73: https://www.ilaparis2023.org/wp-content/uploads/2022/08/Numerique-VHD-EN.pdf (accessed 07.06.2023).

**Cybersecurity and Quantum Threat**

The enhanced ability of quantum computing to break today's encryption standards points to the crucial role of network and information systems' cybersecurity.[32] Quantum-resistant cryptography may become increasingly necessary, and companies will need to assess the extent to which their developing systems comply with applicable cybersecurity regulations.

Moreover, *Harvest Now, Decrypt Later* (HNDL)[33] attacks are significantly increasing with the commercial evolution of quantum computing. Today, hackers are aware that stealing sensitive encrypted data using classical computers can help them decrypt powerful quantum computers in the future. Quantum computing has the potential to fundamentally alter the cybersecurity landscape and could greatly accelerate the pace of cyber innovation and also render useless some current encryption methods.[34]

With this in mind, cybersecurity regulation should be made more applicable to quantum technology, given the current lack of universal instruments.[35] Very few laws and regulations are harmonized across the world. Cyberlaw is currently composed of instruments, adopted at international, regional[36] and national levels.[37] Their common denominator is the explicit reference to the issue of cybersecurity, which is relevant for space activities and infrastructures.[38]

With regard to cyberspace, mention should be made of the 2001 Budapest Convention on Cybercrime,[39] which implements a system of international

32 S. Bonnart et al., *Cybersecurity Threats to Space: From Conception to the Aftermarths*, in: PJ Blount, Mahulena Hofmann (Eds), *Space Law in a Networked World*, Brill, Leiden, Boston, 2023, 72.

33 J.P. Mello, *Harvest Now, Decrypt Later*, 23 November 2022, https://www.insidequantumtechnology.com/news-archive/harvest-now-decrypt-later/ (accessed 07.06.2023).

34 V. Biradar, *Cybersecurity in the new era of Quantum Computing*, 10 January 2023, https://www.frost.com/frost-perspectives/digital-transformation-frost-perspectives/cybersecurity/cybersecurity-in-the-new-era-of-quantum-computing/ (accessed 07.06.2023).

35 Digital Challenges..., White Paper, ILA, *op. cit.*, 93.

36 *See* the EU 2022 Directive on measures for a high common level of cybersecurity across the Union (NIS2), 2022 Directive on the resilience of critical entities.

37 F. Delerue, *Cyber-opérations et droit international*, IRSEM, Note de Recherche n° 59, 17 juillet 2018, 1–8.

38 S. Hobe, R. Popova, *Cyber Law and Outer Space (Activities): Legal and Regulatory Challenges*, Proceedings of 61th Colloquium on the Law of the Outer Space of the International Institute for Space Law 2018, Eleven International Publishing, The Hague, (2019), 659–670.

39 *Convention on Cybercrime*, Budapest, 23 November 2001, ETS 185: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (accessed 07.06.2023); M. Keyser, *The Council of Europe Convention on Cybercrime*, Journal of Transnational Law&Policy 12, 2 (2003) 287–326.

cooperation that considers the specific requirements to fight against cybercrime and interference of data flows. The Convention addresses "data interference" and "system interference" in the case of computer operations,[40] but does not refer specifically to QT or space infrastructure.

Another instrument to consider is the 2017 Tallin Manual 2.0 on the international law applicable to cyber operations,[41] which could apply also to QT, as it considers the rules of international law governing cyber-related incidents that States may encounter. Even though a non-legally-binding instrument, it provides a restatement of international law as applied in the cyber context, addressing issues of sovereignty, due diligence, jurisdiction and international responsibility, which are also relevant for quantum technology. The Manual addresses in particular the relevance of cybersecurity law and space law,[42] containing cybersecurity rules applicable to various fields of activities, including space operations. Indeed, it clarifies the connection between cyber and space, thus linking space technology to cybersecurity.

Concepts relevant for digital security can also be found in international space law,[43] in particular the notion of "harmful interference" in Article IX of 1967 Outer Space Treaty (OST),[44] which might be linked to cyber risks to the transmission and data.[45] Given the growing need of connectivity between satellites, such risks make them vulnerable to cyber threats and the general evolution of quantum technology.

There is an agreement within the international community on the applicability of general international law, and of the various branches of international law as international human rights law, international humanitarian law, law of international responsibility in the field of digital security, but there remain unresolved issues related to the application of principles such as due diligence and sovereignty of States in cyberspace,[46] in particular the threshold at which cyber operations breach international law that need to be assessed on a case-by-case basis depending on the nature, circumstances and consequences of the cyber action.[47]

40 Articles 4, 5 and 6 of the Convention of Cybercrime.

41 E. T. Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, Georgetown Journal of International law, 48 (2017) 735-778.

42 A.S. Martin, *Outer Space, the Final Frontier of Cyberspace: Regulating Cybersecurity Issues in Two Interwoven Domains*, Astropolitics, 21 (2023) (doi.org/10.1080/14777622.2023.2195101).

43 Digital Challenges..., White Paper, ILA, *op. cit.*, 25.

44 *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, 1967, 610 U.N.T.S.205.

45 S. Kaiser, M. Mejia-Kaiser, *Cyber Security in Air and Space Law*, German Journal of Air &Space Law 64 (2015), 404.

46 Digital Challenges..., White Paper, ILA, *op. cit.*, 27.

47 D. J. B. Svantesson et al., *The Developing Concept of Sovereignty – Considerations for Defence Operations in Cyberspace and Outer Space*, Bond University, June 2021, 27 ss.

**Data protection**

The improved capabilities offered by QT are likely to substantially change the amount, manner, and speed at which data can be processed. Further, the risk of quantum computing breaking current encryption standards raises potential questions about compliance with data protection laws currently in force, such as the requirement to implement appropriate technical and organisational measures to safeguard data under the 2016 General Data Protection Regulation (GDPR) in Europe. Companies which handle personal data will need to assess whether their systems and measures to store and transfer personal data indeed do comply with such Regulation.

The GDPR applies to (i) a company or entity which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed; and (ii) a company established outside the EU and is offering goods/services or is monitoring the behaviour of individuals in the EU. In other words, the Regulation applies to the processing of personal data wholly or partly by automated means (Article 2).

> The GDPR has consequences for satellite operators,[48] which includes the improvement of the protection of personal data with quantum-secure encryption to prevent data breaches by quantum computers and developing regulatory policies to ensure personal data protection in the quantum era.[49]

In terms of information security, while quantum computing can improve encryption, it could also make current methods of encrypting data much less effective, since quantum computers can solve specific problems much faster than regular ones, thus making it possible to use them to break the encryption algorithms that currently protect sensitive data. A critical risk is the possibility to use the sophisticated algorithms of quantum computers to analyse and predict human behaviour in a way that undermines the principles of data protection law. General international law, as well as relevant areas of international law, such as international humanitarian law and international human rights law (rights to privacy, freedom of expression, access to information) apply to digital data.[50] However, with the exception of EU law, there are few binding rules of international law specifically dedicated to digital data.

48 M. Cocco, H. Correia Mendonça, *GDPR for Satellite Operators: What You Need to Know*, ViaSatellite, 8 June 2018, https://interactive.satellitetoday.com/via/july-2018/gdpr-for-satellite-operators-what-you-need-to-know/ (accessed 26.06.2023).

49 World Economic Forum, *Quantum Computing Governance Principles*, January 2022, 25.

50 Digital Challenges..., White Paper, ILA, *op. cit.*, 17.

These issues will also be of relevance to the use of QT in space applications, in particular in terms of cybersecurity, data transfers (e.g. communications, Earth observation data, GPS signals) and liability in case of damage. There is a necessity to develop international standards,[51] like in the field of AI, to address the expected behaviours in the use of QT, as well as to identify common definition and terminology (features, usage and purpose), sharing of methods, procedures, uses and purposes,[52] particularly considering all industrial sectors where QT can be used, including space activities.

**Responsibility and Liability**

The extension of the law of State responsibility to digital activities has been the subject of some conjecture, especially on issues of attribution, countermeasures, and defense.[53]

The emergence of quantum computing will likely have a bearing on contracting practices engaged with this technology, the complexity of which may make foreseeing potential losses challenging, including: (i) measuring performance (given the increased speed of quantum computing and, consequently, accurate drafting of service level agreements); and (ii) formulating liability provisions, such as for a loss of data arising out of an error which was difficult or even impossible to predict.

The question arises: 'Who is accountable for the actions of quantum computers?'. Further, who is liable when third parties use quantum computers that they don't own for unlawful purposes? What happens if data loss results from an error within the functioning of the QT?

These questions are also relevant for space activities due to the fact that damage in outer space – between space objects – is based on fault. The challenge is to determine how to prove fault due to QT in the conduct of space activities.

## 4. Relevant UN Space Treaties Provisions in the Use of Quantum Technology

The application of the UN Space Treaties to QT in space relates principally to the OST, the 1972 Liability Convention (LIAB),[54] and the 1975 Registration Convention (REG).[55]

51 International Telecommunications Union, *AI, quantum technologies and new cyber threats – are we prepared?*, 26 March 2020, https://www.itu.int/hub/2020/03/ai-quantum-technologies-and-new-cyber-threats-are-we-prepared/ (accessed 23.10.2023).

52 World Economic Forum, Quantum Computing..., *op. cit.*, 27.

53 Digital Challenges..., White Paper, ILA, *op. cit.*, 27.

54 *Convention on International Liability for Damage Caused by Space Objects* 1972, 961 U.N.T.S. 187.

55 *Convention on Registration of Objects Launched into Outer Space*, 1975, 1023 U.N.T.S. 15.

**General principles**

Subject to the development of future international regulatory frameworks, the use of QT in space missions will be subject to the relevant governance principles that currently apply to outer space activities, including:

(i) The freedom of access, exploration and use;
(ii) The peaceful exploration and use of outer space;
(iii) The conduct of space activities in accordance with international law. This calls for a consideration of the applicability of international digital law;
(iv) The principles of cooperation, mutual assistance and due regard to the corresponding interests of all other States;
(v) The international responsibility of States for national activities in outer space;
(vii) The international liability of the launching to other States or their nationals for damage caused by a space object of that launching State.

**Responsibility, Liability and Damage**

According to Article VI of the Outer Space Treaty, States Parties *inter alia* bear international responsibility for national activities in outer space, including the Moon and other celestial bodies. In relation to space activities carried out by non-governmental entities, including those incorporating QT, these must have been authorized, through an appropriate license issued under a national regulatory framework, and be subject of continuing supervision by the appropriate State.

In addition, the relevant States, agencies, organizations or private companies will have the responsibility to maintain the control and security over a spacecraft that utilizes QT.[56] Indeed, the use of QT underscores several security and transparency concerns, particularly in the case of military or dual-use satellites.

Moreover, Article VII of the OST provides that the launching State is internationally liable for damage to another State Party. Article II of the LIAB specifies that: "A launching State shall be absolutely liable to pay compensation for damage caused by its space object on the surface of the Earth or to aircraft in flight". Article III of the LIAB introduces a regime of fault-based liability in case of damage being caused elsewhere than on the surface of the Earth to a space object.

56 Government of Luxembourg grants space activity license to OQ Technology, https://www.oqtec.space/news/government-of-luxembourg-grants-space-activity-license-to-oq-technology (accessed 07.06.2023) "[...] this license authorisation will allow OQ Technology to also provide its internet of things (IoT) and machine-to-machine (M2M) connectivity services with all additional satellites [...]".

In any case, the launching State(s), as defined in the LIAB, will be liable for damage caused by a relevant space object. However, the complex issue to consider is whether, and how, the system of liability, as foreseen in the UN Space Treaties, is suitable in the context of quantum components utilized in space programmes. If something goes wrong with a satellite utilizing QT, for example, the question arises as to who is responsible, and liable, in the case of damage involving personal injury or property, or a failure to comply with national and/or international rules and regulations.

While every case will be determined in accordance with the specific circumstances, in general, the notion of damage included in the OST and LIAB corresponds to physical and direct damage, and does not expressly address the risk of intangible or non-direct damage caused by cyberspace activities,[57] in particular those linked to quantum technology. For example, if damage occurs to an object in outer space, the liability regime applicable is based on fault. But, how can we define the notion of fault? How can we prove fault?

Responsibility for actions and decisions taken by quantum components can be secured by resorting to strict or objective liability schemes, which do not require human fault, or by relocating human fault to the programmer or supervisor.

In this context, compliance with cybersecurity standards in industry is of utmost importance. In addition, a system of verification in orbit of actions conducted should be developed given the fact that new technological components are increasingly being incorporated within space systems (AI, ML, QT).

**Jurisdiction, Control and Registration**

In relation to issues of jurisdiction, Article VIII of the OST provides that the State of registry retains jurisdiction and control over such object and over any personnel, while in outer space or on an celestial body. In addition, Article II(1) of the REG provides that:

> "when a space object is launched into Earth orbit or beyond, the launching State shall register the space object by means of an entry in an appropriate registry which it shall maintain.[…] and paragraph (2) that: where there are two or more launching States in respect of any such space object, they shall jointly determine which one of them shall register the object […]".

Consequently, the State of registry retains jurisdiction and control over any space object that includes a quantum component. However, even if the concepts of State of registry and the launching State(s) are relevant, they may require further elaboration in the development of a workable and consistent legal framework for QT use in space activities, since further research may lead us

57 D. Stefoudi, *The Relevance and Applicability of Cybersecurity Laws with Regard to Data Storage on Board Satellites and on the Ground*, Air &Space Law 44 (2019): 440.

eventually to conclude that it is appropriate to alter their scope to take account of the precise applications and activities operated under the QT technology.
The use of QT (as well as AI) in future space missions challenges the current legal and policy frameworks in many ways. If QT can be used to protect both the safety and security of operations, potentially it can also be used as a tool for interference, hacking or satellite destruction. Transparency in terms of QT utilisation is of utmost importance. Even if artificial agents produce useful and reliable results, it must be openly explainable as to how these results are generated. The many uses of QT agents also raise questions regarding aspects of autonomy, privacy and freedom from manipulation.

## 5. Policy and Strategy Initiatives at National Level

Digital regulation is quite fragmented between international, regional and national framework. That said, some strategy and policy frameworks for the use of QT are now being adopted or updated by States.[58]
In the *United States*, for example, the Quantum Computing Cybersecurity Preparedness Act[59] adopted in 2022 encourages "federal government agencies to adopt technology that will protect against quantum computing attacks." This represents a milestone in the global effort to develop and implement "quantum-resilient cybersecurity".[60]
The *United States* has also adopted its National Cybersecurity Strategy in March 2023. Two of its pillars are of particular relevance are: (i) (Pillar one) "Defend critical infrastructure"; and (ii) (Pillar four) "Invest in a resilient future" which refers to a "digital ecosystem based on artificial intelligence and quantum computing".[61] It deals with cybersecurity and the protection of critical infrastructure such as space assets.

58 *Unveiling the National Quantum Strategies Worldwide – Part I*, QTI Blog, 14 November 2023, https://www.qticompany.com/unveiling-the-national-quantum-strategies-worldwide/ (accessed 16.11.2023); *Unveiling the National Quantum Strategies Worldwide – Part II*, QTI Blog, 6 December 2023, https://www.qticompany.com/unveiling-the-national-quantum-strategies-worldwide-part-ii/ (accessed 10.12.2023).

59 Public Law 117-260, *Quantum Computing Cybersecurity Preparedness Act*, 21 December 2022.

60 S. Sanzeri, *What the Quantum Computing Cybersecurity Preparedness Act Means for National Security*, 25 January 2023, https://www.forbes.com/sites/forbestechcouncil/2023/01/25/what-the-quantum-computing-cybersecurity-preparedness-act-means-for-national-security/ (accessed 07.06.2023).

61 United States, National Cybersecurity Strategy, March 2023, 23, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (accessed 26.06.2023); *see* United States, *National Quantum Initiative Supplement to the President's FY 2023 Budget*, January 2023, 26, https://www.quantum.gov/wp-content/uploads/2023/01/NQI-Annual-Report-FY2023.pdf (accessed 26 June 2023).

In particular, strategic objective n°4.3 deals with "prepare[ing] for our post-quantum future", with strong encryption of fundamental importance to cybersecurity and global commerce for the protection of online data and to certify the accuracy of information. Given that, as noted, quantum computing has the potential to break most ubiquitous encryption standards, it is important to balance the promotion and advancement of quantum computing against threats posed to digital systems. There is therefore the need to develop complementary mitigation strategies to provide cryptography agility in the face of these new risks. In this context, the National Institute of Standards and Technology (NIST) is developing quantum-resistant cryptographic algorithms.[62]

The *United Kingdom* released its National Quantum Strategy in 2023. It addresses the fact that QT can support business and, in particular, the space sector.[63] QT acts as an enabler for wider innovation across the economy, including the space sector.[64] Goal 4 of the Strategy focuses on regulation and protecting the sector, mitigating the risks associated with quantum, technical standards, and assurance of quantum technologies. It mentions the necessity to create a national and international regulatory framework that supports innovation and the ethical use of quantum technologies.[65]

*Australia* published its National Quantum Strategy[66] in 2023. It deals with 5 main themes focusing on (1) research, development and investment in the use of QT; (2) securing access to essential quantum infrastructure and materials, which refers to the space sector;[67] (3) quantum workforce; (4) standards and frameworks that support national interests; and (5) an inclusive quantum ecosystem based on trust and ethic. It also mentions the fact that quantum computers can improve Earth observation from space to more precisely observe parameters for disaster resilience and climate change.[68]

62 National Institute of Standards and Technology, *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*, 5 July 2022, https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms (accessed 07.06.2023).

63 UK, National Quantum Strategy, March 2023, 32, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1142942/national_quantum_strategy.pdf (accessed 26.06.2023).

64 *Idem*, 43.

65 *Idem*, 47.

66 Autralian Governement, Department of Industry, Science and Resources, *National Quantum Strategy, Building a thriving future with Australia's quantum advantage*, 2023, https://www.industry.gov.au/sites/default/files/2023-05/national-quantum-strategy.pdf (accessed 26.06.2023).

67 *Idem*, 31.

68 *Idem*, 50.

*France* also adopted its National Quantum Strategy in 2021. It deals in particular with the use of quantum for defense purposes, the need to develop policies for the measurement, evaluation and standardization of QT, taking account that QT communication applications are emerging as core "building blocks for connecting space and ground segments".[69]
Lastly, other countries are developing their market and strategy in the field of QF as *China*[70] and *Canada*.[71]
Policies and strategies are only first steps towards developing more comprehensive national legislation for ICTs, artificial intelligence and quantum technology. The main elements of national policy focus on critical infrastructure, resilience, national security, standards, risks mitigation. Those aspects are particularly relevant for the space sector.

## 6. Concluding Observations

QT represents transformative capabilities, but poses issues related to cybersecurity, data transfer, responsibility and liability. There is a need for standardisation, traceability, testability and predictability in the use of this technology.
Even if the industry is at a relatively early stage of 'quantum technology', in particular in space activities, it is clear that governments and industries should develop common standards, considering the applicability of international law, including digital law, and thus promote recommendations and requirements for critical infrastructure and national security systems. Soft law instrument as the Tallinn Manual constitutes an important tool and provides important elements considering cyber operations in space that could apply to QT. In addition, it is necessary to consider that non-state actors are an integral part of cyber domain and space activities, and so the establishment of standards should take into consideration their participation in the use of QT.
However, there is a trend toward the nationalization of norms and laws for the protection and security of the digital environment, which could further fragment and undermine the legal interoperability of relevant international, regional and domestic legal regimes.
Artificial intelligence, machine learning and quantum technology are changing international law. They represent a promising future in term of

69 France, *Stratégie nationale sur les technologies quantiques*, Janvier 2021, https://www.entreprises.gouv.fr/files/files/secteurs-d-activite/numerique/enjeux/quantique/dossier_de_presse_quantique.pdf (accessed 26.06.2023); see France, *National Quantum Strategy*, Annual Report, March 2023, 15.

70 *Chinese Quantum Companies and National Strategy 2023*, The Quantum Insider, 13 April 2023.

71 *Canada's National Quantum Strategy*, 2022, https://ised-isde.canada.ca/site/national-quantum-strategy/sites/default/files/attachments/2022/NQS-SQN-eng.pdf (accessed 26.06.2023).

technological advancement and innovation, but they also raise ethical, legal, social and policy questions.[72]

This paper serves simply to introduce issues related to QT and there is clearly much more detailed work required as the technology continues to develop and we see the further practical applications to space activities. This will be essential to ensure that future space activities are as much as possible consistent with the overarching governing principles related to the exploration and use of outer space for peaceful purposes.

72 M. Kop et al., *Towards Responsible Quantum Technology*, Standford Law School, 2023, 22 p.