AI & SOCIETY (2024) 39:125–137
https://doi.org/10.1007/s00146-023-01729-7

MAIN PAPER

# Digital sovereignty, digital infrastructures, and quantum horizons

Geoff Gordon[1]

Received: 31 August 2022 / Accepted: 12 July 2023 / Published online: 13 September 2023

## Abstract

This article holds that governmental investments in quantum technologies speak to the imaginable futures of digital sovereignty and digital infrastructures, two major areas of change driven by related technologies like AI and Big Data, among other things, in international law today. Under intense development today for future interpolation into digital systems that they may alter, quantum technologies occupy a sort of liminal position, rooted in existing assemblages of computational technologies while pointing to new horizons for them. The possibilities they raise are neither certain nor determinate, but active investments in them (legal, political and material investments) offer perspective on digital technology-driven influences on an international legal imagination. In contributing to visions of the future that are guiding ambitions for digital sovereignty and digital infrastructures, quantum technologies condition digital technology-driven changes to international law and legal imagination in the present. Privileging observation and description, I adapt and utilize a diffractive method with the aim to discern what emerges out of the interference among the several related things assembled for this article, including material technologies and legal institutions. In conclusion, I observe ambivalent changes to an international legal imagination, changes which promise transformation but appear nonetheless to reproduce current distributions of power and resources.

**Keywords** International law · Imagination · Transformation · Quantum technology · Digital sovereignty · Digital infrastructure · Digital decade

## 1 Introduction

This contribution to the symposium on changes to an international legal imagination addresses next generation technologies envisioned for the future of digital technologies. The technologies that I focus on are quantum technologies, which in many respects remain more notional than operational, at least at scale. My argument is that governmental investments in quantum technologies speak to the imaginable futures of digital sovereignty and digital infrastructures, two major areas of change driven by related technologies like AI and Big Data, among other things, in international law today. Quantum technologies are being developed for insertion into digital infrastructures, to surpass current limitations to those infrastructures' computational powers and processes. Under intense development today for future interpolation into digital systems that they may alter, quantum technologies occupy a sort of liminal position, rooted in existing assemblages of computational technologies while pointing to new horizons for them. The possibilities they raise are neither certain nor determinate, but active investments in them (legal, political, and material investments) offer perspective on digital technology-driven influences on an international legal imagination. The international legal imagination that I address is a hegemonic one, bound up with the contested notion of sovereignty and traced here by observation of specifically European institutions, policies and legal instruments. In contributing to visions of the future that are guiding European ambitions for digital sovereignty and digital infrastructures, quantum technologies condition digital technology-driven changes to international law and legal imagination in the present.

Broadly speaking, the most advanced quantum technologies are not yet ready for general use, but substantial public investments and policy instruments are already priming them for insertion into material networks associated with digital infrastructures and digital sovereignty (Johnson 2018). There are three pertinent classes of quantum technologies, each at a different stage of development: quantum computing, quantum sensing, and quantum communication

✉ Geoff Gordon
g.gordon@asser.nl

[1] T.M.C. Asser Institute, The Hague, The Netherlands

(Hoofnagle and Garfinkel 2022). Quantum computing, which promises the most apparently disruptive effects on existing institutions of international law (especially in the area of security, on the basis of an existential threat to current encryption technologies) is the farthest from viability. Quantum sensing is already contributing to information flows that inform international institutions, and lab results point to a new frontier in sensing capabilities. Quantum communications harness quantum mechanical phenomena to information communication, and have been achieved in limited experimental set-ups. I will present the several technologies in more (though still rudimentary) detail in Sect. 2.

The common thread for the latest innovations across all three classes of quantum technologies is their capacity actively to intervene in quantum phenomena for effects in the world at large, exploiting seemingly impossible quantum mechanical properties that are usually present only at (sub) atomic scales (Dowling and Milburn 2003). Those properties include superposition, in which a quantum system exists in multiple, otherwise-incompatible states at once; entanglement, by which multiple quantum systems correlate in ways that make the condition of the collected whole knowable, but also make the conditions of the constitutive units unknowable; and non-locality, by which stimulus to one quantum system effects an identical and perfectly simultaneous stimulus to another quantum system, though separated at distance—a property that Einstein refused to accept, famously describing it as ‘spooky action at a distance’ (Markoff 2015).

Quantum technologies have become objects of intense governmental interest, but remain at and perhaps just beyond material and conceptual horizons. While quantum technologies remain at the horizon, they are the object of global public and private investment in the tens of billions of dollars, the majority of it through governments’ defense spending (Gibney 2019). Discursively, quantum technologies have already been entered into an arms race logic, as part of a geopolitical contest organized around the US and China (Lele 2021). In short, though quantum technologies and theory remain futuristic, they are present in contemporary discourses, already driving policy and material investments. As an emerging technology that is not yet field-ready but driving substantial investments nonetheless, quantum technologies mark out a liminal space between material governmental apparatuses and speculative possibilities. The idea here is to use this situation of quantum technologies, between a complex present and an indeterminate future, for perspective on an international legal imagination today, with specific reference to digital sovereignty and digital infrastructures.

Digital sovereignty figures prominently in the current and ongoing policy of the European Commission (the Commission). In addition, observers (critical and otherwise) are increasingly adopting an analytic of digital sovereignty to explain global policies and programs of diverse actors and institutions, not limited to the Commission. To be sure, digital sovereignty is hardly limited to quantum technologies. The Commission’s program for digital sovereignty has principally been associated with interests in Big Data, AI, and the information and communication flows they rely on. In part, that is the point: the liminal position that I ascribe to quantum technologies is not yet operational but actively being developed today for inclusion in digital infrastructures as a facet of digital sovereignty. Quantum technologies feature prominently, for instance, among the Commission’s ensemble of policy aims and instruments for the so-called European Digital Decade (2020–2030), including the €1 billion European Quantum Flagship initiative (the Flagship) (EC 2021; Riedel et al. 2019). Initiatives like the Flagship are priming quantum technologies for other initiatives, such as the European Gaia-X program for a new digital infrastructure. Gaia-X and other infrastructural programs are supposed to establish a robust material foundation for digital sovereignty (Braud et al. 2021). In sum, digital infrastructures are imagined as a competitive terrain for novel assertions of digital sovereignty, and quantum technologies point to horizons for that terrain and those assertions.

This paper proceeds in three parts. The next part will review the material technologies in question, describing their peculiar quantum mechanical properties as well as their stages of current development. Although the next part will point up places where the technologies may problematize existing law and legal practice, I will mostly focus on the material condition of the technologies (including speculative investment as a material condition) to set up analysis of how they may interact with issues of international law. The part thereafter will sketch governmental frameworks bearing on the development of quantum technologies, focusing on European frameworks of digital sovereignty and digital infrastructures, and the policy instruments that lay out the European vision for the insertion of quantum technologies into the frameworks of digital sovereignty and digital infrastructures. Impatient legal readers may prefer to skip ahead to this section and the conclusion, referring back to the section describing the material basics of quantum technologies. In the final, concluding part, I will read these preceding parts diffractively, observing the properties of the devices and their material limitations in interaction with European legal frameworks, for what their interaction demonstrates about a changing international legal imagination.

Throughout, I adopt a style of situated observation. This encompasses some theorizing, but I do not mean to prioritize the theoretical register, neither with respect to quantum mechanical theory, nor quantum social theory. I do adapt a methodological technique from quantum theory, namely diffraction (about which in a moment), but not for an encompassing framework of social theory. There has been a growing body of ambitious work developing quantum social theory, prompted by Karen Barad's *Meeting the Universe Halfway* (Barad 2007), with recent books including Michelle Wright's *The Physics of Blackness* (Wright 2015), and Denise Ferreira da Silva's *Unpayable Debt* (Ferreira da Silva 2022). Likewise, there has lately been quantum-inspired work in international relations, including Alexander Wendt's *Quantum Mind and Social Science* (Wendt 2015), Laura Zanotti's *Ontological Entanglements* (Zanotti 2018), and Mark Murphy's *Quantum Social Theory for Critical International Relations Theorists* (Murphy 2020). These theoretical undertakings exceed my intent as well as the bounds of this article. In my observational register, however, I will try to be clear about the work that theory is doing throughout the rest of this piece.

In adopting a style of situated observation, I mean something loosely in keeping with Anne Orford's descriptive technique. Orford's description restrains the philosophical impulse while attending to 'relations between elements … that [are] not reducible to causal or dialectical relations', and entails 'attempting to describe practice while recognizing that the choice of what to include in such a description is always value-laden' (Orford 2012, p. 618, 624–625). My adaptation of diffraction works in this methodological vein of observation and description. The diffractive method is a common technique for experimentation in quantum physics, used to observe the result of a dynamic element as it passes through and interacts with some interference, including the active agency of the observer as well as the experiment's design in the observational outcome (Barad 2007). Diffractive method attends to patterns that emerge out of interference among multiple elements under examination, according to their arrangement. The diffractive method as I use it here has a comparative character, at least insofar as I draw conclusions out of differences and discrepancies that I describe among material technologies, policy discourses, and theoretical possibilities. But the distinction from straightforward comparative method is precisely that I am interested in what emerges from the combination of differences, and not in an evaluation or map of the divergences themselves. Though divergent, the things that I assemble and describe here are mutually occupied in the same timespace, and I attend to their differences to discern what may issue from their interaction. Equally, I employ a diffractive method in part because I am not analyzing any singular effects traceable to unique underlying elements, nor am I after a dialectical account of point and counterpoint. Rather, I am interested to envision what emerges, from my vantage point, out of the interference among several things that I assemble here, including symbolic legal discourses, governmental institutions, material technologies and infrastructures, investments, evolving policy, and vanguard theory. In conclusion, I will describe a resulting image in which cutting-edge technologies and visionary programs combine ambivalently with historical materialities and political economic conditions. The international legal imagination that this ambivalent image sustains appears to raise critical dilemmas both novel and familiar.

## 2 Quantum materialities

This section describes some basics about the quantum technologies that I use with a diffractive method to gauge an international legal imagination. Here, I largely cabin the legal and institutional analysis to which I return in the next section, except to note where the technology appears to create friction with existing legal arrangements. Following convention, I take up the technologies in the three classes of quantum computing, quantum sensing, and quantum communications.

### 2.1 Quantum computing

I start with quantum computing, because the computers remain the focal point of policy attention, the "gamechanger" in policy and investment discourses. Before I turn to the computers as integral machines, however, let me begin with the basic unit of the quantum computer, the qubit. The qubit is the quantum computer's counterpart to the classical computer's bit. The bit is readable in one of two states, 0 or 1. The qubit, by contrast, utilizes superposition, which means that it is readable in more than two states: 0, 1, or a superposition of 0 and 1. On the face of it, that would appear to mean a third possibility, which would make a quantum computer remarkably more powerful than a classical computer. If 3 bits allow 8 possible combinations of 0 and 1, 3 qubits would allow 27 possible combinations of 0, 1 and their superpositions. A difference like that would be staggering if raised to the order of gigabytes. This is why some observers mistakenly describe quantum computers as much more powerful updates on classical electronic computers. This is a mistake because working with superposition does not really allow a one-to-one comparison of qubits to classical bits. What qubits do, at least when they can be entangled one with another, is allow a quantum computer to exploit the wave function at the heart of quantum mechanics. This means that qubits allow quantum computers to take advantage mathematically of quantum mechanics' special descriptive powers—which also means that quantum computers will not necessarily be better at the things that classical physics already do quite well.

If they surpass classical computers, quantum computers will be better at parsing certain complex and multidimensional problems that strain the compute power and processes of classical electronic computers. Molecular interactions, for instance, are very hard to describe and model with classical computers, because the permutations of even limited interactions exceed the compute power of classical computers. A functioning quantum computer, on the other hand, would theoretically be able to deploy entangled qubits to model the multiple permutations. This is part of the transformative imaginary associated with quantum computers: the ability to "unlock" and ultimately thereby exploit heretofore inaccessible properties of the physical world. Presently, however, there is only a single algorithm for a universal quantum computer that demonstrably outperforms (in theory) anything a classical computer can achieve: namely, the ability to factor large numbers. This is notable because it is also the key to overcoming contemporary encryption technologies. At scale, quantum computers would overcome the encryption protocols that digital infrastructures run on today. That suggests an existential threat to global communications systems, which rely on information security. This is another key to understanding the transformative imaginary associated with quantum computers. The ability to overcome encryption would spell the end of proprietary information and confidential or secret communications transmitted electronically. While the unadorned threat appears to be overhyped and unrealistic (I will not go into the reasons here; for the argument, please see Lindsay 2020), it nonetheless is driving policy concerns and substantial investments in quantum technologies, especially from national defense units (Smith 2020).

But I am getting ahead of myself, and before getting properly to quantum computers as integral machines, let me back up to the modeling potential for things like molecular processes. That capability is being actively advanced with quantum simulators, which do what their name implies: they simulate quantum mechanical behavior. Quantum simulators are not universal computers, i.e., they are not programmable to run any calculation. Instead, they can be set up to simulate specific sorts of quantum interactions. While they cannot work on any problem put to them, they can model specific quantum behaviors. They do this by actually executing the quantum properties involved in the interactions that they simulate, deploying superposition and entanglement across qubits, thus using quantum behavior among gate-controlled quantum systems (qubits) to model the behavior of quantum systems 'in the wild'. A quantum simulator is sort of like the teapot in the teapot test, popularized by Richard Borcherds' YouTube video, in which Borcherds debunks some of the hype around quantum computers (Borcherds 2021). He points out that classical electronic computers would struggle accurately to model the scatter of pieces from a teapot dropped and smashed. He then points to the computer that would accurately model the scatter of pieces: namely, a teapot, which can be dropped and smashed. His point is leveled against persons overeager to proclaim the superiority of machines capable of doing things that classical computers cannot. But his teapot is also a useful analogy of a quantum simulator: it models the problem by behaving as the thing to be modeled. When a quantum simulator mimics behavior, it does so according to programmed instructions, roughly like a classical computer, but those instructions trigger more than formal, digital representations; they also trigger quantum mechanical properties, like superposition and entanglement, meaning that the quantum simulator recreates the problem posed to it in ways that a classical computer does not. Quantum simulators are already doing work in experimental laboratories, primarily in universities, for research purposes, and mostly as objects of study in themselves, allowing researchers to observe quantum phenomena at work. A next step in development, however, remains to make good on the promise of simulation, to model quantum phenomena that occur 'in the wild', such as chemical and biological interactions.

Moving on, universal quantum computers—quantum computers that can be programmed to solve any computational problem—are under development in several varieties. These computers, at scale, would be useful in digital infrastructures as all-purpose information processors. All-purpose, however, remains qualified, meaning all-purpose with respect to complex, and multi-dimensional problems, potentially including logistical problems or problems posing challenges intractable for classical machines, but likely not for the many problems that classical computers will continue to solve with efficacy. Most actually existing quantum computing models under development today are identified as Noisy Intermediate-Scale Quantum devices, or NISQs. The name conveys that these models, if successful, will mark an intermediary step towards still more robust quantum computing devices. They are called noisy because they are prone to error, a consequence of the difficulty and expense of maintaining, manipulating, and reading a quantum device in an entangled state (Preskill 2018). Overcoming error is one of the principal challenges for quantum computing. For NISQs, the near-term aim is to build increasingly large machines (meaning with increasing numbers of qubits) capable of performing their own error correction (thus not eliminating error, but adding enough qubits to compensate and correct). For that reason, a functioning NISQ computer requires far more qubits than would a comparably powerful quantum computer that is not noisy (though no such machine yet exists, if it ever will).

There are several sorts of universal quantum computer under development. One, under development by Google and IBM, relies on semiconducting circuits known as Josephson junctions, which involve rings that can be relatively large in size (even to the measure of a ring worn round the finger) and can carry electric current in superposition, effectively moving in two directions at once (as well as either direction individually). Another, under development by Honeywell, involves ion traps, whereby individual subatomic particles are manipulated in and out of 'traps' by a variety of possible means to exploit properties of superposition and entanglement. A third approach utilizes photons. This approach is not much developed outside of China, and there is only limited public information about its development there. Outside of China, photon-based quantum computing is generally viewed as not capable of supporting general use (Hoofnagle and Garfinkel 2022). Another wild card is topological quantum computing, which Microsoft has been developing. Topological quantum computing relies on subatomic particles that include distinct topological characteristics, which would stabilize the particles and lower the likelihood of error in quantum computing processes. But while these particles exist in theory, no such particle has yet been found for use as a qubit. Microsoft had been counting on so-called Majorana fermions, but a 2018 study funded by Microsoft and published in *Nature*, which purported to show evidence of having found exploitable Majorana fermions, was retracted in 2021 (Kouwenhoven et al. 2018; Castelvecchi 2021). The research was discovered to be fundamentally flawed, and contradictory evidence appears to have been suppressed, though outright fraud was not alleged on review (Simonite 2021).[1]

## 2.2 Quantum sensing and communications

Quantum sensing is hard to encapsulate. There is a large variety of quantum sensors which utilize diverse techniques to produce diverse measurements. All quantum sensing technologies involve measurements of time and location, but that can mean different things in practice. One sensor may be able to 'see' objects underground and through obstructions; another may be able to 'hear' a weak signal in a large, noisy field; others 'read' electronic signatures or other qualitative data about sensed objects; others produce time measurements with extraordinary precision and consistency; etc. Quantum sensors can arguably be divided in two categories. The first is a long-standing category that has exploited the knowledge that energy varies discontinuously, in discrete quanta (Dowling and Milburn 2003). The technologies in this category, while significant, are not pertinent here. They include things like magnetic resonance imaging technologies. While they were developed on the basis of knowledge associated with quantum mechanics, they do not actually rely on quantum properties like superposition and entanglement. The second category, however, does precisely that: it includes a diverse array of technologies that exploit specifically quantum mechanical properties—properties that appear to be impossible according to human understanding—to produce results that other technologies cannot. For instance, some sensors will utilize entanglement to 'see' by entangling two particles, projecting one and retaining the other, to observe with the second what the first encounters; others will detect hidden objects by utilizing measurements so precise that the smallest deviations from the norm will indicate gravitational anomalies. The former, utilizing entanglement, actively deploys the quantum property to measure its object directly; the latter group, attuned to deviations, does not deploy the quantum property to the object directly, but instead the act of measuring will take changes in the sensors' quantum properties into account to determine measurement of its object (Hoofnagle and Garfinkel 2022).

The enhanced scopic capacities of quantum sensors are imagined to be transformative in themselves, potentially disrupting everything from resource extraction to bedrock routines for defense against nuclear war (Gamberini and Rubin 2021). Moreover, quantum sensors expand measurements both in terms of what they can measure and the precision with which they can measure, and in doing so, quantum sensors are headed to market on the promise of significant new streams of qualitative measurement data. As qualitative data, the information generated by quantum sensors differs from the bread and butter of contemporary information streams, namely metadata, or data about data (as gleaned from digital communications, in contemporary context). Quantum sensors are being developed for use in everything from submarines to satellites, and, as will be seen in the next section, as parts of expansive digital infrastructures.

Quantum communications broadly include two groups of projects. One is quantum key distribution, a system that utilizes quantum properties to generate and distribute encryption keys, or keys to encrypt and decrypt communications. Quantum key distribution, if viable, might supplement or surpass classical encryption for classical computing, though the marginal utility of quantum key distribution relative to a robust but fully classical key distribution is not clear. The other group of projects aims at a fully quantum communications network or even internet, in which quantum mechanical properties are directly involved in information communication (Hoofnagle and Garfinkel 2022: 257–302). In these latter projects, entangled quantum systems carry information end to end (and thus do not merely operate to encrypt or decrypt otherwise classical information communications). The primary purpose, for both sets of projects, is security: quantum communications provide new ways to secure information. When quantum information (or an entangled quantum system) is communicated, whether as encryption key or

[1] Todd Holmdahl, who had led hardware development for Microsoft's Xbox, directed the project. In 2018, he promised a verifiable topological qubit by the end of that year. In 2019 he left the project, reportedly due to missed internal deadlines, including the failure to produce the topological qubit. Kees Kouwenhoven was running the lab for Microsoft at Delft Technical University, in the Netherlands, and was the primary author on the 2018 article. He left the lab and the university shortly after it was retracted (Simonite 2021).

the body of a communication, any attempt to read or copy it will alter it—for the same reason that measuring a quantum system ineluctably alters it—and, thanks to entanglement, the tampering will be immediately observable to whomever transmitted the original. Further, in the case of a properly quantum network or internet, the window for tampering will potentially be narrowed: using nonlocality, information can be "teleported" from one entangled system to another, without traveling a path over space and time between them (Castelvecchi 2018). As a result, there would be no metadata trail to eavesdrop (Hoofnagle and Garfinkel 2022: 258).

The foregoing features of quantum communications derive from the unitary character of entangled systems: stimulus to one is immediately measurable on the other. But this is also the condition that makes quantum computers noisy, as it is difficult under the best conditions to maintain quantum systems in an entangled state. Similarly, actually existing quantum communications systems remain in the experimental stage, and scaling remains a challenge. China has been a leader in the field; having apparently developed a quantum communication system capable of transmissions from a low earth orbit satellite to select points on earth (Chen et al. 2021). Outside of China, the Netherlands has been a leading site of development, with Delft University recently announcing successful communication of entangled quantum systems along a network with three nodal points (two end-point quantum processors communicating through an intermediary) (Pompili et al. 2021). The promise of these systems at scale is information security, and the ability to ensure confidentiality of proprietary information, potentially countering the threat to encryption posed by quantum computers at scale. Given the perceived threat that quantum computing poses to standard encryption of digital communications infrastructures, the promise of quantum communications is of reciprocal interest for the future viability of secret and secure communications. This security interest appears to be the primary driver behind public and private investment in quantum communications development (Hoofnagle and Garfinkel 2022). There is, however, an interesting twist here to the transformative potential associated with quantum communications: though much of their promise is conservative in nature, associated with preserving secrecy and proprietary or confidential communications, the possibility of a communications network that eliminates metadata would portend enormous change to the pervasive, metadata-based surveillance routines that have developed with contemporary information systems (Zuboff 2019). Combined (speculatively) with increasing qualitative data from quantum sensors, the imaginary promises a transformed global information ecosystem. But the challenges of harnessing quantum phenomena for communications at scale are extreme, and mundane challenges also remain. A secure communication system, for instance, is only as good as its weakest link, and there remain points of access beyond targeting the transmission of entangled quantum systems.

## 3 European digital sovereignty, digital infrastructures, and quantum visions

Having described the state of contemporary quantum technologies, as well as the potentials ascribed to them, I turn now to international legal frameworks with which they interact, focusing on digital sovereignty, the contemporary expression of sovereignty in networked environments, and digital infrastructures. In this section, I describe unsettled doctrine and novel institutional initiatives, much as the last section described technologies in early stages of development. And where in the last section I largely cabined the legal analysis, in this section I refrain from what the material state of quantum technologies may say about the legal and policy aims. I bring them together in the conclusion, to observe the figure of contemporary international legal imagination as it emerges from their interaction.

### 3.1 Digital sovereignty

In Europe, existing and proposed legislation has been expressly linked by the European Commission and other EU bodies to digital sovereignty (or to technological sovereignty, which is regularly used interchangeably with digital sovereignty by European bodies). They include: the proposed European Chips Act; the proposed European Artificial Intelligence Act; the Open Data Directive; the Single Digital Gateway Regulation; the Regulation on the Free Flow of Non-Personal Data; and the General Data Protection Regulation. Ursula von der Leyen and Charles Michel have each foregrounded digital sovereignty as a policy imperative, at the European Commission and European Council, respectively (von der Leyen 2020, 2021; Michel 2021). Likewise Thierry Breton, the Internal Market Commissioner, who, like von der Leyen and Michel, expressly includes strategic protection of European power and European values as a main part of the rationale (Breton 2020).

Digital sovereignty remains a big basket for policy initiatives and material investments. It does not represent just one thing (Herlo et al. 2021). Beyond European government, the formula is variously used by policy-makers, civil society participants, and observers, public and private. Especially across usages by public institutional figures, however, digital sovereignty appears to signal at least two things: an enduring ideal of individual self-supremacy, as associated with sovereignty; and an ambition to transpose prerogatives associated with sovereignty under international law into domains featuring digital technologies. Thus, digital sovereignty appears intended to reconstruct 'the notion of sovereignty in the context of the digital ecosystem' (Celeste 2021, p. 7). There is something dissonant about the notion of digital sovereignty, captured by Couture and Toupin: 'In the case of the digital, current uses of the notion of sovereignty should also be situated following years of technological determinist discourses claiming the erasure of the nation-state with the emergence of the Internet and the network society' (Couture and Toupin 2019, pp. 2318–2319). Perhaps for that reason, the emergence of digital sovereignty is regularly described as a reactive development, for instance by Bratton, who, in his work popularizing 'The Stack' as a techno-political construct, contextualizes digital sovereignty as a response to breakdowns in political aspirations associated with classical sovereignty, breakdowns occasioned by digital infrastructures (Bratton 2016). Despite the reactive ascription, however, digital sovereignty is also associated with something new. Thus, Couture and Toupin expand on Bratton's framing: 'Whereas the Westphalian system can be understood as creating a horizontal relationship among territorially bounded nation-states, The Stack provides a new global governing logic through which sovereignty operates' (Couture & Toupin, p. 2311). Bratton's Stack, in this analysis, is proxy for the complex ecosystem supported by digital infrastructures, to which digital sovereignty applies as a reconfigured governmental logic. Observers describe twinned characteristics of interconnectedness and plurality in this new ecosystem: 'digital sovereignty may contemplate the co-existence of a plurality of sovereignties within the same physical space' (Celeste 2021, p. 15). More than that, recent research observes changes in which physical spaces, too, are 'newly articulated' in the debates and stratagems that go forward under the banner of digital sovereignty (Glasze et al. 2022, p. 3).

There apparently remains, however, a classical governmental ambition behind assertions of digital sovereignty, namely 'the idea that states should "reaffirm" their authority over the Internet and protect their citizens, institutions, and businesses from the multiple challenges to their nation's self-determination in the digital sphere' (Musiani 2021, p. 1). The overlay of entanglement, post-Westphalian pluralism, and new articulations of spaces and other things points in emerging governmental practices not to an emancipatory condition but an expanded competitive terrain. An ambition to reaffirm authority with a security-driven character is apparent, not least in European mobilizations of the concept: 'What is traditionally defined as 'external' sovereignty, the capability of a state to exercise its power without interference of other entities, is perceived under threat in the European digital society' (Celeste 2021, p. 8). Likewise, European policy initiatives have linked assertions of digital sovereignty with another policy formula emphasizing the need for strategy to safeguard autonomy, namely, strategic autonomy (EC 2020; Moerel & Timmers 2021). In this vein, European policy in the name of digital sovereignty aims to consolidate control over digital infrastructures and the information that flows through them, as part of a fight 'for the control of the digital' (Floridi 2020, p. 371). This has been linked to the exertion of control over data flows and digital infrastructures: 'Measures invoked in the name of digital sovereignty share the exercise of a centripetal force on data and digital infrastructures by states or supranational organizations' (Celeste 2021, p. 10). The emphasis on security and the projection of control support the preservation of historically consolidated prerogatives internationally, but Couture and Toupin point out that those dynamics and their discontents remain relatively suppressed at the level of policy discourse: 'many of the issues discussed are usually addressed without reference to colonialism, imperialism, and a critique of sovereignty itself' (Couture and Toupin 2019, p. 2319).

Imperialism and colonialism play multiple roles in the discourse of digital sovereignty. Digital sovereignty was also (and arguably first) developed outside of the traditional imperial power centers of Europe and the US, as an anti-imperial and anti-colonial program to resist powerful states and private firms in the global north, especially the US and US-based enterprises (Belli 2021; Pinto 2018). The rhetoric of resistance, however, has been adopted for domestic politics by states within the traditional imperial power centers of Europe and the US, as a sort of public push back against ascendant private powers attributed to giant tech firms such as Google and Facebook (Christakis 2020; Pohle and Thiel 2020). Thus, despite a mixed history, the resurgence of sovereignty in the digital domain by geopolitical power centers seems to raise renewed possibilities of imperial and neo-colonial international relations, whether emanating from the US, Europe, or other power centers, including China.

### 3.2 Digital infrastructures

The contests that the digital sovereignty discourse presupposes go forward materially over digital infrastructures. In this light, Musiani observes a relative neglect: 'the study of digital sovereignty as a set of infrastructures and socio-material practices has been largely neglected [and] the concept of (digital) sovereignty should also be studied via the infrastructure-embedded "situated practices" of various political and economic projects which aim to establish autonomous digital infrastructures in a hyperconnected world' (Musiani 2021, p. 1). The embodiment of digital sovereignty is in the infrastructure, which comprises material and semantic elements as well as practical routines organized for directed information flows. The embodiment of digital sovereignty in digital infrastructures underscores what has already been raised in recent research: global infrastructures are of special interest to international law (Gordon 2021; Kingsbury 2019; Donaldson and Kingsbury 2013). The interest includes a recognition that ‘infrastructures act like laws. They create both opportunities and limits; they promote some interests at the expense of others’ (Edwards 2002, p. 191). Kingsbury and Maisley go farther: ‘A common trait of laws and infrastructures is that each can create, shape, or prevent the emergence of social relations of particular kinds’ (Kingsbury and Maisley 2021, p. 357). As I have argued elsewhere, these several infrastructural possibilities—creative, conditioning, and foreclosing—are not the product of a static, transparent law, nor do they effect law as a function of technological determinism alone. Rather, law and infrastructure exist in a complex relationship, sometimes complementary and sometimes conflictual, but in each case co-constituting normative relations (Gordon 2021; Kingsbury and Maisley 2021, p. 357).

The European Commission’s European data strategy is clear about privileging new relations, namely ‘a thriving ecosystem of private actors to create economic and societal value from data’ (EC 2018). The infrastructure for that ecosystem is being developed with initiatives like Gaia-X, which I will focus on now briefly for the example it provides. Described as a ‘sovereign digital infrastructure’ for Europe, Gaia-X was officially proposed by Germany and France in 2019 for the whole of the EU. The title of its launch document described Gaia-X as ‘the Cradle of a Vibrant European Ecosystem’ (BMWi 2019). Other documents are equally clear about the aim to establish new ‘European ecosystems’ (BMWi 2020a). References to digital sovereignty are sprinkled throughout the documentation of Gaia-X, and one of the primary documents produced by the German government to describe and explain the Gaia-X initiative begins with a text box dedicated to digital sovereignty (BMWi 2020b). The notion of digital sovereignty at work in Gaia-X documentation, however, is not identical with usages in other European policy documents. Digital sovereignty for Gaia-X appears both more limited and more expansive: more expansive for not merely encompassing private actors but actively developing digital sovereignty in their name; more limited by identifying digital sovereignty with a specific aim of data sovereignty:

> GAIA-X’s mission is to strengthen digital sovereignty for business, science, government, and society by empowering the development of innovation ecosystems. Digital sovereignty means that these individuals, organizations, and communities stay in complete control over stored and processed data and are enabled to decide independently who is permitted to have access to it (BMWi 2020b, p. 2).

While Gaia-X tailors digital sovereignty to data sovereignty, the project as a whole is replete with the language of values—economic value and European values—as well as other ambitions associated by the Commission with digital sovereignty, such as the creation of a robust digital ecosystem, flagged above. With respect to values, however, close reading shows Gaia-X’s pluralism to be relatively thin: throughout all of the policy documents, economic value is by far the more developed, while social and cultural values appear to function as placeholders at best. Further, in addition to the register of values, Gaia-X is organized according to seven principles, which incorporate from social, technical, and normative registers, to articulate interrelated political, economic, and governmental ambitions. Gaia-X’s seven guiding principles are: European data protection; openness and transparency; authenticity and trust; digital sovereignty and self-determination; free market access and European value creation; modularity and interoperability; and user-friendliness (BMWi 2019). Beyond Gaia-X, in the language of other European institutional initiatives, digital infrastructure has been constructed along three interrelated lines: as a key security arena, as a source of economic value creation, and as a site of social values preservation (Van den Meerssche and Gordon 2023; EC 2018). These themes demonstrate the discursive global framework against the background of which the European project goes forward: digital infrastructures are securitized domains constructed with multiple adversarial relationships—geopolitical, private–public, and private-private—in turn organized around multiple socio-technical axes, economic, political, legal, and cultural. The ongoing controversy around Huawei has been exemplary, exhibiting the high stakes of securitized interests in global digital infrastructure, with diverse legal and political devices applied to intervene in market practices for control over information flows (Madiega 2020).

### 3.3 Quantum visions

Quantum technologies have been raised in numerous policy statements under the European Digital Decade initiative, most recently in the proposed Chips Act, applying to computer chips and nanotechnologies. Some of those references are on the order of placeholders, pointing to the future significance of quantum technologies and prospectively establishing readiness for their incorporation into a European digital ecosystem. The development of quantum technologies for incorporation into the European digital ecosystem has been concentrated by the European Commission under the European Quantum Flagship. The Flagship, launched in 2018, is ‘one of the largest and most ambitious research initiatives of the European Union.’ (EQF website) The Flagship will operate for at least 10 years with a budget of at least a €1 billion. I canvass here the issues and questions raised specifically in the Flagship’s Strategic Research Agenda, for what that document points up about the development of quantum technologies for the European digital ecosystem.

The Strategic Research Agenda begins with a premise not limited to quantum technologies, namely, that 'the mastery of deep [digital] technologies will determine the future prosperity of countries and regions across the world' (EQF 2020, p. 8). Specific to quantum technologies, use cases are identified 'in the fields of: medicine; physics; chemistry; biology; geo-physics; climate science; environmental sciences; mobility; defense, and data storage and processing' (EQF 2020, p. 60). Among other things, 'Defence systems and autonomous mobility and navigation will profit from long-term stable rotation and acceleration sensors based on quantum technologies' (EQF 2020, p. 60). On these bases, documentation for the Flagship characterizes QITs as 'essential building block[s] for Europe's technological sovereignty' (EQF 2020, p. 12). Just as technological or digital sovereignty marks a discursive transposition from classical state sovereignty to 'a new global governing logic through which sovereignty operates' (Couture and Toupin 2019, p. 2311), QITs further alter horizons of political self-sufficiency: 'quantum technologies can also raise issues of sovereignty that can change the reasoning about international collaborations' (EQF 2020, p. 93). An overlap between digital sovereignty and more traditional usage, however, remains clear: 'a robust and secure communication infrastructure based on quantum security will be essential to protect European sovereignty and its economy in the face of increasing cybersecurity challenges' (EQF 2020, p. 23). Security is also an economic priority, expressed in terms of intellectual property: 'To build a flourishing quantum industry, Europe needs to protect its ideas and strategically build up intellectual property to compete with other regions' (EQF 2020, p. 17). The Strategic Research Agenda envisages a hypercompetitive economic terrain, in which '[t]he ability to process data fast will be a key driver for the future economy, where even marginal technological differences lead to valuable competitive advantages' (EQF 2020, p. 39). In this vision of competitiveness, the possibility of disruption—and the possibility of exploiting disruption—is a key dynamic:

> Quantum technologies have a huge potential for innovation that may revolutionise the information economy. Europe can play a leading role through strategic international cooperation to develop competitive collaborations…. Quantum technologies are one of the most disruptive R&D sectors as they present a gamechanger for the entire information and data value chain from sensing, to communication, sorting, simulating, predicting and computing (EQF 2020, p. 91-2).

Despite celebrating disruptive potential, however, the document also aims at continuity, with quantum technologies inserted into contemporary infrastructures to develop on an already-existing architecture: 'The long-term vision is to develop a Europewide quantum network that complements and expands the current digital infrastructure, laying the foundations for a quantum internet' (EQF 2020, p. 22).

## 4 Conclusion

I suggested in the introduction that current investments in not-yet-scaled quantum technologies give those technologies a liminal position vis-à-vis the governmental frameworks of digital sovereignty and digital infrastructures, into which quantum technologies are to be inserted in the future. Here in conclusion, I propose to put that perspective to work with the diffractive method that I have been setting up, to observe what emerges from the combination of factors and phenomena assembled and described to this point. If a genealogical analysis offers a "history of the present", I use the diffractive method here for a sort of futurist twist, or a future of the present. If a history of the present is a way of 'using history as a means of critical engagement with the present', then my ambition here is to use the institutional vision of quantum technologies as a means to the same (Garland 2014, p. 367). In doing so, I am describing attributes of a contemporary international legal imagination, identified here principally with reference to European institutions, concerned with digital sovereignty, and cutting-edge information-technologies.

To start, I return to the vision described by the European Quantum Flagship's Strategic Research Agenda, reading it with the materiality of the quantum technologies to which the Strategic Research Agenda applies, and the governmental frameworks of digital sovereignty and digital infrastructures which they may develop or disrupt. What horizons become visible through their cross-combination? I believe at least two images of ambivalent futures for international legal practice (such as I know it) become visible. One image of ambivalent futures concerns international law as an ordering mechanism in socio-technical context, and the relative concentration or distributions of power and resources that digital infrastructures will support and digital sovereignty will entail under international law. Another concerns the ways in which international legal practices participate in the world, including the sorts of technologies that mediate access between the international legal system and the world, and the sorts of socio-technical architectures that sustain the international legal system in the world.

To sketch the first ambivalent image, let me start with a crude binary, individualistic versus relational. While there is no one authoritative understanding of quantum mechanics, interpretations of quantum mechanics consistently express deeply relational dynamics. Though particles exist in quantum mechanics, they hardly exist as coherent, discrete unities, at least not until the moment of waveform collapse, when the effects of superposition, entanglement, and nonlocality all cease to manifest. Prior to that point, the individual contains multitudes, such as in superposition, in which multiple incompatible states are viable, or entanglement, in which constituent parts form a whole, but the constituent parts cannot be measured as individual units while in the entangled state. History suggests that the growing appreciation for these relational properties could support generative models for social order, much as Newtonian physics once established revolutionary new principles for enlightened government (Ferreira da Silva 2022). As noted, Karen Barad has recently popularized the exploration of quantum mechanics for social theory, and there is the recent work by international relations theorists attempting to mine quantum theory for new directions in global relations (Barad 2007; Wendt 2015; Zanotti 2018; Murphy 2020; see also the recent forum in Global Studies Quarterly, introduced by Voelkner and Zanotti 2022).

But to read the theory diffractively, together with the material situation of quantum computing technologies, points to another possibility as well. The machines, as described, are wildly complex and astronomically expensive to develop. Under current political-economic conditions, the state of the industry shows increasing consolidation in favor of a handful of privileged agents. The computers especially are dominated by IBM, Google, Honeywell and a small handful of others, with Microsoft among the club though with a particularly unproven technology. Both the history and the future of this consolidation is inauspicious. Historically, this consolidation tracks something that Mariana Mazzucato has called out in other contexts: public money has funded advances in the technology, and continues to do so, but ultimately the product is auctioned off to a high bidder (Mazzucato 2018). With respect to the future, quantum technologies appear likely to continue a trend already apparent with platforms featuring artificial intelligence technologies. The costs of the expertise and compute power to run a scalable program are high, and the competitive incentives to dominate are extreme, leading to a remarkably small club of global providers, who leverage their programs through cloud-based platform distribution (Rieder et al. 2021). But while the cloud allows relatively wide-spread access, that access is controlled by the owner of the platform. Applied to quantum computing, this trend may well be exacerbated, as the costs and expertise point to still more exclusive control over the technology and access to it. In addition, one other factor points up the possibility of more consolidation. Securitization of quantum technologies and the digital infrastructures into which they may be inserted is ringfencing their development. Considerable international legal activity today is aimed at restricting access to the technologies, blocking their distribution and communication, with tools like import/export controls, dual use restrictions, and blacklists barring distribution of the technologies (van Daalen 2022; USDC 2021). These tools favor a paranoid security apparatus that rewards the consolidation of power.

To sketch the second ambivalent image, another crude binary: digital versus analog. Quantum technologies are being primed for insertion into contemporary digital systems, but they differ materially in notable ways from the classical digital devices with which they will interact and perhaps replace. Take sensors, as touched on above: much of the global scopic apparatus behind contemporary surveillance generates signals intelligence, or SIGINT, which yields metadata, communications and electronic signals that reveal contextual markers about the thing under surveillance. Quantum sensors, on the other hand, typically generate measurement and signature intelligence, or MASINT, which yields qualitative data about the thing under surveillance, whether that be mass, wavelength, shape, etc. (Hoofnagle and Garfinkel 2022) MASINT demands different processing, and supports different technical, socio-technical, and governmental systems. As mentioned above, the potential difference becomes still more radical in combination with a future quantum communications network.

There is also a stark divide between quantum computers and classical computers. I referred to this in the introduction, when speaking of the wave function. Here in conclusion, the difference between quantum and classical computing can be put in terms of a question: what does it mean to let the thing itself solve problems? The classical electronic computer relies on the formal languages of math and code to represent the problem to be solved. The computation is formal, likewise its solution, the product of math and semantic code, the endpoint of a representation, never an act of the thing itself. Though they also involve mathematical language and code, quantum computers are different. This is clearest with quantum simulators, which by design are limited to enacting specific quantum properties for observation. Universal quantum computers, if they are ever built at scale, rely on semantic code just as classical computers, but the code quantum computers computational process ultimately also relies on something more than formal abstraction: it relies on the wave function itself, as it manifests in an actual enactment of superposition and entanglement. This is not a formal rendering, and there is no adequate explanation for how these properties work, only after-the-fact confirmation that they do. The quantum computer harnesses quantum phenomena to 'solve' problems. Karen Barad's Bohrian interpretation of quantum mechanics for social theory proposes to meet the universe halfway, and perhaps the quantum computer does just that, solving problems by bringing together formal code with the fabric of the universe (Barad 2007). To adapt an argument made in another context by David Chandler, however, governmental technologies that come ever closer to the Real begin to take on a homeostatic character, for instance in related probabilistic decision systems that exploit the Real to optimize command and control routines—harnessing the Real to reproduce what is (Chandler 2018). In short, radical properties of quantum theory and technology plausibly support reproduction as well as disruption. Just as with the first binary, one possibility points to radical transformation; another points to a deepening of already-existing socio-technical conditions, including divisions of access and power.

Finally, consider in this light Barad's brittlestar, which also features prominently towards the conclusion of *Meeting the Universe Halfway* (Barad 2007, 2014). Though eyeless and brainless, the brittlestar can be described to see and know its environment, including predators, which it apparently observes and evades, despite the lack of brain and eyes. It can do this because the brittlestar's body is covered in a web of crystalline lenses linked to a complex nervous system. That nervous system includes feedback loops that trigger homeostatic responses, such as inducing bodily color changes, to optimize the optics of the constellated lenses. This system allows the brittlestar to observe and avoid predators. Furthermore, it epitomizes Barad's mobilization of quantum mechanics for social theory, as an organism the agency of which can neither be denied nor separated from its environment. In the sense, Barad's brittlestar points to a radical horizon in which naïve individualism may be overcome and agency transformed without being sacrificed (Barad 2007, 2014). For Barad, a key characteristic of the brittlestar is that there is no separation between it and its environment; it has no brain to think itself apart from the world it observes. But still it observes that world and differentiates between those parts of it that constitute a threat from those that don't. Accordingly, Barad writes that 'The brittlestar lives agential separability, the possibilities for differentiation without individuation' (Barad 2007, p. 378). This possibility for differentiation without individuation makes clear a powerful horizon that quantum theory may support for social systems.

Against that transformative possibility, however, there is a troubling correspondence between the body of the brittlestar and the latest instantiations of cybernetic systems theory, whether in legal practice or in legal-security assemblages that feature sensors and information processors in global array. With respect to legal practice, the brittlestar's existence—sustained by feedback loops without the intervention of any one mind—approximates Marianne Constable's related indictment of the contemporary legal imagination:

> Today's dream is that of a system or set of systems – perhaps even of a world system – that would run of itself. In this dream, institutions require continuous administration or processes of management, even as management seeks to efface its own presence. Governance of and through institutions comes to depend more and more on increasingly recursive communicative systems of technology and personnel. Systems form circuits of information, which in turn manage the functioning of the system, generating further information, which in turn manage… (Constable 2017).

The same characteristics of the brittlestar are also reminiscent of the scopic assemblages that allow contemporary weapons systems to observe and hunt human prey (Liljefors et al. 2019). These assemblages lack a locatable mind but are covered in lenses linked by electronic pulses, constantly reconstituting information flows to differentiate threat and nonthreat—or target and not-target. Thus, the way in which the brittlestar maintains, as a nervous system continuously responding to a complex and changing topography, sounds close Allen Feldman's description of cutting-edge military technologies, when he writes that 'omnivoyant warfare is the tactical mastering of the differentia of the world through the latter's optical compression and vectoring by commensurable topological profiles' (Feldman 2019). It bears noting that quantum technologies are now envisaged for inclusion in such assemblages (AARC 2020).

Alongside the mundane dynamics of legal practice generally and the violent assemblages of international security, there is another correspondence worth noting, with the cybernetic architectures of sensory power lately described by Isin and Ruppert. Isin and Ruppert describe sensory power as a technology of governance that dispenses with the traditional individual subject. Instead, sensory power relies on pattern recognition processes reiteratively applied to information flows, thereby producing clusters, units of constant and changing differentiation in which individuation is eclipsed by transient associations (Isin and Ruppert 2020). Governance of the cluster does not rely on the production of a subject, nor on the management of a population, but something more topological, namely the iteration of—and control over—transient units constituted by patterns that are legible and susceptive to government. Isin and Ruppert hold that the cluster is a novel development. Unlike Barad's brittlestar, however, Isin and Ruppert identify sensory power as a profoundly disempowering governmental innovation (Isin and Ruppert 2020).

To conclude, let me raise one last ambivalent possibility: while much of the foregoing appears novel in nature, the diffractive reading also points to aspects of historical continuity. The security dynamics traced here are bound up with sovereign authority, though updated as digital sovereignty. The quantum technologies that are promoted under the banner of digital sovereignty promise radically new possibilities, but are envisioned as an extension of already-existing communications infrastructures. My point is not to favor one or the other, the 'new' or the 'old', but to observe what about the present moment can be gleaned from their combination. Each of the ambivalent images above—possibly transformative, possibly dystopian—can be traced to existing antecedents even as they promise disruptive change. My intuition is that most of the antecedents and continuities are anchored in competitive logics vested in proprietary control over information, which finds a historical framework in competitive relations among modern states (Foucault 2003, 2007, 2008). Investments in quantum computers may be driven by competitive aims to intervene in secure communications infrastructures, but not to dismantle them, while investments in quantum communications are predicated on the possibility of reinforcing them. And while quantum sensors may produce a different sort of information from that produced by other sensors, their cutting edge is being honed by industries for defense and resource extraction, among the very few for whom the cost of developing and deploying quantum sensors is worth the surplus they may yield. The information flows that these technologies are intended to enable may ultimately support new modes of governance, and the imaginary may support the demise of the classical legal subject, among other radical possibilities; but that does not equate to emancipatory transformation, which is not yet apparent in the international legal imagination that I have tried here to draw out with the help of quantum systems.

**Data availability** Not applicable.

## References

Australian Army Research Centre (AARC) (2020) Quantum technology: the defence imperative (5 May 2020). https://researchcentre.army.gov.au/library/land-power-forum/quantum-technology-defence-imperative

BMWi (2019) Project GAIA-X: A federated data infrastructure as the cradle of a vibrant European ecosystem. Federal Ministry of Economic Affairs and Energy, Berlin

BMWi (German Federal Ministry For Economic Affairs and Energy) (2020a) GAIA-X: a Pitch Towards Europe, status report on user ecosystems and requirements. Federal Ministry of Economic Affairs and Energy, Berlin

BMWi (2020b) GAIA-X: Driver of digital innovation in Europe, Featuring the next generation of data infrastructure. Federal Ministry of Economic Affairs and Energy, Berlin

Barad K (2007) Meeting the universe halfway. Duke University Press, Durham

Barad K (2014) Invertebrate visions: diffractions of the brittlestar. In: Kirkesy E (ed) The multispecies salon. Duke University Press, Durham, pp 221–241

Belli L (2021) BRICS countries to build digital sovereignty. In: Belli L (ed) CyberBRICS. Springer, Cham, pp 271–280

Borcherds R (2021) The teapot test for quantum computing. https://www.youtube.com/watch?v=sFhhQRxWTIM

Bratton B (2016) The stack: on software and sovereignty. MIT Press, Cambridge

Braud A, Fromentoux G, Radier B, Le Grand O (2021) The road to European digital sovereignty with Gaia-X and IDSA. IEEE Network 35(2):4–5

Breton T (2020) Europe: the keys to sovereignty. European Commission. https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en

Castelvecchi D (2018) The quantum internet has arrived (and it hasn't). Nature 554(7690):289–293

Castelvecchi D (2021) Evidence of elusive Majorana particle dies with retraction. Nature 591(7850):354–355

Celeste E (2021) Digital sovereignty in the EU: challenges and future perspectives. In: Data protection beyond borders: transatlantic perspectives on extraterritoriality and sovereignty, pp 211–228

Chandler D (2018) Ontopolitics in the Anthropocene: an introduction to mapping, sensing and hacking. Routledge, London

Chen YA, Zhang Q, Chen TY, Cai WQ, Liao SK, Zhang J, Chen K, Yin J, Ren J-G, Chen Z, Han S-L, Yu Q, Liang K, Zhou F, Yuan X, Zhao M-S, Wang T-Y, Jiang X, Zhang L, Liu W-Y, Li Y, Shen Q, Cao Y, Lu C-Y, Shu R, Wang J-Y, Li L, Liu N-L, Xu F, Wang X-B, Peng C-Z, Pan J-W (2021) An integrated space-to-ground quantum communication network over 4600 kilometres. Nature 589(7841):214–219

Christakis T (2020) 'European Digital Sovereignty': successfully navigating between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy. SSRN 3748098

Couture S, Toupin S (2019) What does the notion of "sovereignty" mean when referring to the digital. New Media Soc 21(10):2305–2322

Donaldson M, Kingsbury B (2013) Ersatz normativity or public law in global governance: the hard case of international prescriptions for national infrastructure regulation. Chic J Int Law 14:1

Dowling JP, Milburn GJ (2003) Quantum technology: the second quantum revolution. Philos Trans R Soc Lond Ser A Math Phys Eng Sci 361(1809):1655–1674

Edwards P (2002) Infrastructure and modernity: force, time, and social organization in the history of sociotechnical systems. In: Philip B, Arie R, Andrew F (eds) Technology and modernity: the empirical turn

European Commission (2021) 2030 Digital Compass: the European way for the digital decade. COM (2021) 118 final

European Commission (2018) European Commission Digital strategy, C(2018) 7118 final (21.11.2018)

EQF (European Quantum Flagship). https://qt.eu/

EQF (2020) Strategic research agenda. https://qt.eu//app/uploads/2020/04/Strategic_Research-_Agenda_d_FINAL.pdf

Feldman A (2019) Of the pointless view: from the ecotechnology to the echotheology of omnivoyant war. In: Liljefors M, Noll G, Steuer D (eds) War and algorithm. Littlefield, London, pp 165–190

Ferreira da Silva D (2022) Unpayable debt. Sternberg Press, London

Floridi L (2020) The fight for digital sovereignty: what it is, and why it matters, especially for the EU. Philos Technol 33(3):369–378

Foucault M (2003) "Society must be defended": Lectures at the Collège de France, 1975–1976. Picador

Foucault M (2007) Security, territory, population: lectures at the Collège de France, 1977–78. Picador

Foucault, M (2008) The birth of biopolitics: lectures at the Collège de France, 1978–1979. Picador

Gamberini SJ, Rubin L (2021) Quantum sensing's potential impacts on strategic deterrence and modern warfare. Orbis 65(2):354–368

Garland D (2014) What is a "history of the present"? On Foucault's genealogies and their critical preconditions. Punishment Soc 16(4):365–384

Gibney E (2019) The quantum gold rush. Nature 574(7776):22–24

Glasze G, Cattaruzza A, Douzet F, Dammann F, Bertran MG, Bômont C, Zanin C (2022) Contested spatialities of digital sovereignty. Geopolitics, 28(2):1–40

Gordon G (2021) Engaging an infrastructure of time production with international law. Lond Rev Int Law 9(3):319–349

Herlo B, Irrgang D, Joost G, Unteidig A (2021) Practicing sovereignty: digital involvement in times of crises. Verlag, Bielefeld

Hoofnagle C, Garfinkel S (2022) Law and policy for the quantum age. Cambridge University Press

Isin E, Ruppert E (2020) The birth of sensory power: how a pandemic made it visible? Big Data Soc 7(2):2059

Johnson WG (2018) Governance tools for the second quantum revolution. Jurimetrics 59:487

Kingsbury B (2019) Infrastructure and InfraReg: on rousing the international law 'Wizards of Is.' Cambr Int Law J 8(2):171–186

Kingsbury B, Maisley N (2021) Infrastructures and laws: publics and publicness. Annu Rev Law Soc Sci 17:353–373

Kouwenhoven LP et al (2018) Retracted article: quantized Majorana conductance. Nature 556(7699):74–79

Lele A (2021) Quantum technologies and military strategy. Springer, Cham

Liljefors M, Noll G, Steuer D (2019) War and algorithm. Rowman & Littlefield, London

Lindsay JR (2020) Surviving the quantum cryptocalypse. Strategic Stud Quart 14(2):49–73

Madiega TA (2020) Digital sovereignty for Europe. European Parliament Research Series 651

Markoff J (2015) Sorry, Einstein. Quantum study suggests 'spooky action' is real. *The New York Times*, 21

Mazzucato M (2018) The value of everything: making and taking in the global economy. Hachette, London

Michel C (2021) Digital sovereignty is central to European strategic autonomy–Speech by President Charles Michel at 'Masters of digital 2021' online event. Council of the EU and the European Council, February, 3

Moerel L, Timmers P (2021) Reflections on digital sovereignty. EU Cyber Direct, Research in Focus series

Murphy M (2020) Quantum social theory for critical international relations theorists: quantizing critique. Springer Nature, Cham

Musiani F (2021) Towards an infrastructure-based sociology of digital sovereignty practices: the 'pilot case' of Russia. AoIR Selected Papers of Internet Research

Orford A (2012) In praise of description. Leiden J Int Law 25(3):609–625

Pinto RA (2018) Digital sovereignty or digital colonialism. SUR-Int J Hum Rights 15:15

Pohle J, Thiel T (2020) Digital sovereignty. Internet Policy Rev. https://doi.org/10.14763/2020.4.1532

Pompili M, Hermans SL, Baier S, Beukers HK, Humphreys PC, Schouten RN, Vermeulen RFL, Tiggelman MJ, dos Santos ML, Dirkse B, Wehner S, Hanson R (2021) Realization of a multinode quantum network of remote solid-state qubits. Science 372(6539):259–264

Preskill J (2018) Quantum computing in the NISQ era and beyond. Quantum 2:79

Riedel M, Kovacs M, Zoller P, Mlynek J, Calarco T (2019) Europe's quantum flagship initiative. Quantum Sci Technol. https://doi.org/10.1088/2058-9565/ab042d

Rieder B, Sileno G, Gordon G (2021) A New AI Lexicon: monopolization: concentrated power and economic embeddings in ML & AI. A New AI Lexicon. https://medium.com/a-new-ai-lexicon/a-new-ai-lexicon-monopolization-c43f136981ab

Simonite T (2021) Microsoft's big win in Quantum Computing Was an 'Error' After All. Wired. https://www.wired.com/story/microsoft-win-quantum-computing-error/

Smith FL III (2020) Quantum technology hype and national security. Secur Dialogue 51(5):499–516

United States Dept. of Commerce (USDC) (2021) Commerce Lists Entities Involved in the Support of PRC Military Quantum Computing Applications, Pakistani Nuclear and Missile Proliferation. https://www.commerce.gov/news/press-releases/2021/11/commerce-lists-entities-involved-support-prc-military-quantum-computing

van Daalen O (2022) Making and breaking with science and conscience: the human rights-compatibility of information security governance in the context of quantum computing and encryption. PhD dissertation, University of Amsterdam

van den Meerssche D, Gordon G (2023) The contemporary values of operadiction regimes. In: Feichtner I, Gordon G (eds) Constitutions of value: Law, governance, and political ecology. Routledge, Abingdon

Voelkner N, Zanotti L (2022) Ethics in a quantum world. Glob Stud Quart 2(3):ksac044. https://doi.org/10.1093/isagsq/ksac044

von der Leyen U (2020) State of the Union. Building the world we want to live in: a Union of vitality in a world of fragility. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

von der Leyen U (2021) State of the Union Address by President von der Leyen. European Commission, Brussels

Wendt A (2015) Quantum mind and social science. Cambridge University Press, Cambridge

Wright MM (2015) Physics of blackness: beyond the middle passage epistemology. University of Minnesota Press, Minneapolis

Zanotti L (2018) Ontological entanglements, agency and ethics in international relations: exploring the crossroads. Routledge, Abingdon

Zuboff S (2019) The age of surveillance capitalism: the fight for a human future at the new frontier of power. Profile Books, London