Stanford Law School | Stanford Center for Responsible Quantum Technology

QUANTUM INFORMATION TECHNOLOGIES AND PUBLIC INTERNATIONAL LAW: A STRATEGIC PERSPECTIVE

Elija Perrier[*]

ABSTRACT

The use of computational technologies by nation States and other actors for offensive and defensive purposes represents a major element of international strategic relations. Quantum information technologies, encompassing quantum computing, quantum sensing and quantum communication, have considerable potential to affect geopolitical dynamics among States due to their impact upon cybersecurity, encryption, data processing and strategic planning. The extent to which international law permits and governs the use of computational technologies, both classical and quantum, for strategic competition and conflict is an area of emerging importance in international law. In this article, we review the use of quantum information technologies by States for strategic purposes and the consequences arising under public international law. We present novel analyses of legal implications arising from unique characteristics of quantum systems and supplement our analysis with game theoretic models of quantum-driven State interaction.

INTRODUCTION

A. Overview

A major motivation of research into and technological development of quantum information technologies (QIT), including quantum computing, quantum communication and quantum sensing, is their potential use by State actors in offensive and/or defensive geopolitical contexts. Over the last several decades, public international law jurisprudence has developed an increasing focus on the rules, laws and norms that do - or ought to - govern the conduct of cyber activities by States. Exactly what constitutes 'cyber operations, cyber space and cyber activities' is itself the subject of analysis and debate within the literature and public international law fora. The focus of this article is on the question of what changes with respect to the laws governing the use of cyber technologies when those technologies are quantum in nature. As we discuss below, while there is not yet a

[*]Stanford Center for Responsible Quantum Technology, Stanford University; Centre for Quantum Software and Information, University of Technology, Sydney; Australian National University

formal international treaty instrument specifically devoted to regulating the adversarial use of cyber technologies among States, the use of such technologies is already framed within the existing jurisprudence governing international law generally and the use of force and adversarial action in particular.

The question posed is thus germane and important. In an era in which the critical infrastructure of States upon which they rely for effective actualisation of their sovereignty is informational, digital and cybernetic in nature, the use of such technology for adversarial means and the risk of such technology becoming a target for the adversarial activities of other States is becoming an even more central issue for State strategic planning than ever. Compounded by the rapid acceleration of information technologies in the form of artificial intelligence, automated systems and communication systems all of which rely upon layered classical digital communications infrastructure, the potential disruptive impact of QIT is, should it be realised, profound. What is new about QIT depends on context and the specific technologies in question, but intuitively it is the fact that the uniquely quantum mechanical characteristics of quantum computing, quantum sensing and quantum computing give rise to new avenues of action that are in principle or practice unavailable to States under classical computing technologies that gives rise to the need to consider how and by what means these new forms of activity ought to be regulated. International law is classical. Quantum mechanics is non-classical. Thus integrating each requires a careful analysis of how quantum-specific dynamics and effects propagate through to unique capabilities for action and decision-making, such as the capacity for decryption of classically encrypted data, solving higher-order complexity class problems, or more efficient information processing to afford an information asymmetry advantage for a State.

B. Structure of article

Our article is structured as follows. Section I (*What is Sui Generis about QIT?*) provides motivation for the study of the international law implications of the strategic use of QIT, focusing on the need for technological specificity, strategic certainty and dual use clarity. Section II (*Strategic Quantum Information Technology*) introduces a taxonomy of QIT in a strategic context via the three sectors of quantum information processing, those of quantum computing, quantum sensing and quantum communication. It summarises key principles of quantum mechanics relevant to understanding QIT affordances, with detailed focus on quantum computing and cryptography, quantum networking, quantum communication protocols and quantum sensing techniques. It provides a synopsis of quantum infrastructure stacks and makes a number of observations regarding the use of QIT, such as its embedding within classical information processing architecture.

Section III (*Geopolitical Impact of Quantum Technologies*) discusses the geopolitical impacts of specific QIT applications, including machine learning and optimisation, quantum cryptography, quantum simulation and quantum communication. It examines

literature on the geopolitical implications of quantum sensing. Section IV (*Technical Factors Affecting Strategic QIT*) provides a classical and quantum strategic taxonomy whereby strategic behaviour of States can be considered in terms of a number of channels such as classical-to-classical, classical-to-quantum, quantum-to-classical and quantum-to-quantum. It continues discussion on the embedding of QIT within classical systems, noting that direct quantum-to-quantum interaction is difficult, albeit possible and considers other factors such as local constraints on action by States and the use of QIT to enhance cyber attack strategies. It concludes with a brief note on quantum game theory and its relevance to strategic studies of QIT use.

Section V (*Geopolitical Scenarios*) sets out a number of geopolitical scenarios for the analysis of QIT use. It adopts a taxonomy that fits within the framework of international jurisprudence and strategic behaviour, namely considering cooperative and adversarial activities in peacetime and conflict scenarios. The section sets out two working scenarios whose implications are revisited in the analysis of international law applicable to QIT cyber operations. Section VI (*International Law and Quantum Information Technologies*) presents an overview of relevant international law applicable to the strategic use of QIT by States, with a focus on the application of principles set out in the Tallinn Manual. Section VIII (*Conclusion*) discusses prospective research directions into international law governance instruments for QIT.

I. What is Sui Generis about QIT?

As with any new technological development, the important and necessary question arises as to what is, from a jurisprudential perspective, *sui generis* about its governance [112, 111]. Is there anything *new* from a governance perspective that arises when technology changes, including information processing technology in general and quantum information processing technologies in particular? Is not the application of QIT simply another form of information processing technology already captured by the broad jurisprudence on the use of computational, cybertechnological and information processing technology in general (of which QIT is merely a subset)? This question is often debated within jurisprudential and technology governance under auspices of the 'technology neutrality' of regulation. This includes emerging scholarship on the governance and ethics of QIT [86, 88, 89, 90, 91, 87]. The answers to these questions depend in part on the operating theory of jurisprudence - its rationale and the justification of governance itself - that one adopts. We answer this question in the affirmative on the following bases.

A. *Technology governance requires technological specificity*

Firstly, we argue that while quantum information technologies *qua* information technologies already fall within the abstract ambit of information technology regulation [26, 81, 80,

60, 106], including instrumental or normative prescriptions and proscriptions applicable thereto, the purpose and function of legal principles, laws and governance instruments is not merely to specify abstract general principles. Rather, details matter, including details as to how, where and under what conditions technology is to be operated, used, monitored, stored and deployed. Specificity is an important feature of the implementation of the law itself and indeed is a hallmark of the logic of all legal systems which rely upon hierarchies of classification in order to determine rights, obligations and interests. And specificity is already a feature of how almost all technology is governed: legislation, regulations, rules, precedents and guidance specifically set out the *how* of technology governance as it applies to a specific technology.

B. Strategic technologies require certainty

Secondly, *strategic* technologies, such as those with particular impact on State strategic behaviour, require common rules and certainty in order to regulate and motivate rule-following by State actors and solve the coordination problems, often studied and the subject of game theoretical analyses, of how State actors whose interests do not necessarily align may act cooperatively. The canonical case here in a State sovereignty and national security context is the regulation of nuclear weapons, such as via test-ban, non-proliferation and other international instruments [110, 38, 37]. The monitoring and verification regimes encoded within such instruments play an important role in motivating State behaviour to adhere to the terms of such instruments. Thus when it comes to the use of advanced information technologies, such as artificial intelligence of quantum computing, by States for potentially adversarial means, it is reasonable to expect that similar requirements for specificity ought to apply (consider, for example, proposals for regulation of compute levels in respect of artificial intelligence technologies [33]).

C. Dual use of technology requires clarity

A third, but related, rationale why technological specificity regarding the governance of QIT at international law is well-motivated is the *dual use* [74, **?**] characteristic of such technologies. Dual use technologies are those which have application both in civilian and adversarial contexts, giving rise to the dilemma of how to regulate the use of and trade in such technologies to afford beneficial utility on the one hand, while limiting their use for adversarial or harmful means by an adversary on the other [73]. Clarity of permitted and proscribed uses is essential in the case of dual use regimes in order to provide certainty for stakeholders, actors and users of such technology, especially where the transition from civilian to military use of a technology is relatively frictionless or straight-forward.

II. Strategic Quantum Information Technology

A. *Taxonomy of QIT*

The primary impacts of QIT can be categorised by way of a typical QIT taxonomy that partitions QIT into its three primary divisions of quantum computing, quantum communication and quantum sensing. We consider each application and its geopolitical implications from the perspective of public international law in more detail below. The quantum characteristics of all QIT stems from their reliance upon and utilisation of properties of quantum mechanical systems. Comprehensive reviews of quantum mechanics and quantum information processing may be found throughout the literature [109, 134, 124, 23], including literature on quantum governance [**?**, 90, 86, 91, 87, 74]. However we set out briefly the key concepts behind quantum information processing below before summarising the major subsectors of QIT, being quantum computing, quantum communication and quantum sensing.

B. *Principles of Quantum Information*

Quantum computing, quantum sensing and quantum communication are three interrelated divisions of quantum information [109, 134]. Each is united by the fact that the properties and dynamics of the systems in question, be they computational, mechanical or communicative, satisfy the postulates of quantum mechanics. Quantum information processing represents a means of abstractly reasoning about such systems via axioms and theorems which in turn satisfy the postulates of quantum mechanics. Thus quantum information processing as a discipline draws upon physics, formal theories of computation and information theory. The key characteristic underpinning of all quantum information technology that we assess below in the context of State governance and that which renders such technology distinct from its classical analogue is that such technology leverages the unique properties of quantum mechanics. In formal theoretical terms, this means that such quantum systems respect the postulates of quantum mechanics. These include the following:

1. *Stateful*. Quantum systems are stateful, being described by *quantum states* $|\psi\rangle$ belonging to a Hilbert (vector) space $|\psi\rangle \in \mathscr{H}$ which may exist as linear superpositions of basis states $|\psi\rangle = a|0\rangle + b|1\rangle$ for amplitudes $a, b \in \mathbb{C}$ which subsists in state $|0\rangle$ with probability $|a|^2$ and $|1\rangle$ with probability $|b|^2$. Where the quantum state is two-dimensional, it is denoted a *qubit* (short for 'quantum bit'). Quantum states are also represented by density operators ρ which are analogous to operator representations of probability distributions over states. Quantum systems may subsist as composite systems $|\psi\rangle = |\psi\rangle_a \otimes |\psi\rangle_b$ (product states), otherwise they are said to be *entangled*. Entangled states are a unique feature of quantum mechanical systems and are a central resource for QIT. They include for example two-qubit Bell states

$|\psi\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$ where, as can be seen, measurement outcomes for each qubit are correlated (measuring $|0\rangle$ on the first means it is certain that the second qubit is also in $|0\rangle$, and similarly for $|1\rangle$).

2. *Measurement and encoding*. Information is input into quantum states via encoding protocols [123, 124] (such as via encoding in basis states, relative phases or other forms). Information is extracted from quantum systems via quantum measurement [138], whereby a measuring apparatus interacts with the system. The statistics obtained by repeated measurements of identically-prepared copies of quantum systems are then used to reconstruct the properties of the system. Measurement is framed as a quantum-to-classical channel [134] which collapses (or in the case of partial measurements, partially collapses) the quantum system into a normalised eigenstate corresponding to an observed eigenvalue.

3. *Evolution*. Closed quantum systems $|\psi\rangle$ evolve according to the Schrödinger equation $d|\psi\rangle / |\psi\rangle = -iHdt$ whose solutions are wavefunctions representative of quantum states. The dynamics of quantum evolution are encoded in the Hamiltonian operator H whose description (such as in terms of operators, generators or circuit gates in a quantum algorithm etc) characterises the system. Control of quantum systems occurs via control functions (realised via for example electromagnetic pulses to instantiate logic gates etc) which steer the quantum system towards a desired state, such as via controlled application of quantum logic gates [54].

4. *Open and Closed Quantum Systems*. Quantum systems interact with the environment (such as measurement apparatuses) which may be quantum or classical in nature and which may be represented as its own Hamiltonian coupled to that of the quantum system. Environmental effects decohere and affect quantum state evolution. This is often represented formally using stochastic master equations which model the effects of, for example, environmental noise on quantum systems. Quantum systems are highly sensitive to noise [138] and thus require error correction (such as in the form of error-correcting codes) in order to achieve sufficient fault-tolerance, such as fault tolerant quantum computing [115, 116, 23].

The fundamental properties of quantum mechanical systems above form the basis for the unique capabilities of quantum computing, quantum communication and quantum sensing. We explore each of these in more detail below and in later sections link such unique features to capabilities State actors may leverage strategically. The postulates of quantum theory listed above also give rise to a number of important consequences which distinguish QIT from classical information processing. These include (i) the *no cloning* theorem [139] (that quantum states cannot be copied), (ii) the fundamental requirement for error correction [66] in order for QIT to function (due to the sensitivity of quantum systems) in

fault-tolerant [65] ways, (iii) measurement protocols [138] (requiring identical state preparation or multiple copies produced by an identical quantum process in order to generate measurement statistics rather than having a single quantum state that is repeatedly measured), (iv) quantum ontological phenomena [28], manifest in contextuality [72] (order of measurement giving rise to different statistics), uncertainty principles and non-local action [32] and (v) that entanglement is a resource. Although we do not focus in-depth on these consequences, they are both profound and fundamentally distinguish quantum physics from its classical counterpart. It is also not uncommon to compare classical and quantum information processing from an information-theoretic perspective, including comparisons between classical and quantum models of computation, the relationship between classical information theory [125] and its quantum counterpart. We direct the reader to technical discussions in the literature for more detail (see [134]). Moreover, the extreme sensitivity of quantum systems and the fact that interaction with quantum systems via measurement can effectively decohere or demolish their quantum properties means that verification, auditing and control of such systems varies from classical analogues, a factor relevant to proposals for technical control of such systems and governance regimes (such as international legal standards and protocols). We now summarise a number of technical features each of the three sectors of quantum computing, quantum communication and quantum sensing.

C. Quantum Computing and Quantum Simulation

1. Quantum Computation

Quantum computing [109] is a computational paradigm whereby computation and information processing leverages and is constrained by quantum mechanics. Quantum computing is distinguished from its classical counterpart by way of the existence of properties of superposition and entanglement noted above. Algorithms which utilise such characteristics, denoted *quantum algorithms*, give rise to computational procedures which are effectively unique and distinct from classical computation (or more formally, which may be simulated by classical computation but only with super-polynomial resource cost). Quantum algorithms vary considerably, but are often classified into three broad types based upon the underlying quantum subroutines they leverage. These include (i) *quantum Fourier transforms*, a class of algorithms applying a quantum version of classical Fourier transforms, into which Shor's algorithm [126, 127] falls; (ii) *quantum search algorithms* such as Grover's algorithm [68] for $\sqrt{n}$ speedup of search based on amplitude amplification and (iii) *quantum simulation* which we discuss in more detail below, and which is sometimes classified as an effective use-case of quantum systems rather than a specific subclass of quantum computational methods. The effect of these quantum algo-

rithmic subroutines and methods is to facilitate more efficient computational processes, such as faster or more accurate search and quicker optimisation.

2. Quantum Simulation

Quantum simulation [62, 119, 70, 96] represents a major prospective use of quantum information systems and computation of strategic relevance to States. Quantum simulation involves utilising controllable quantum systems to emulate and study the behaviour of other, often less accessible or highly complex quantum systems. This approach is particularly valuable in fields such as condensed matter physics, high-energy physics, atomic physics, quantum chemistry, and cosmology, where understanding complex quantum interactions is essential. For States, the potential synthesis of chemicals and materials may provide it with a competitive advantage in both peacetime and conflict. Quantum simulations regarding strategic behaviour are speculative, but could in principle also provide advantages for States (e.g. enabling speed-up of currently infeasible simulations).

D. Quantum Communication and Quantum Cryptography

1. Quantum Communication

Quantum communication [29, 48, 64, 94] leverages the principles of quantum mechanics to enable secure and efficient transfer of information. It is fundamentally distinct from classical communication as it uses quantum states, such as qubits, to encode and transmit data. Key technologies within quantum communication include quantum key distribution (QKD) [34, 99], quantum networks, and entanglement-based communication protocols [57], each of which addresses specific challenges and opportunities in secure communication and information sharing. QKD provides a protocol for the secure exchange of cryptographic keys by utilising features of quantum systems, specifically the no-cloning theorem and the Heisenberg uncertainty principle to detect eavesdropping attempts. Protocols like BB84 [34] and E91 [57] utilise either discrete quantum states (e.g., polarised photons) or entangled particles to securely generate a shared key between two parties, even in non-idealised settings [120]. Any interception of the quantum channel alters the quantum state of the transmitted particles, making eavesdropping detectable. The exchanged key is used in symmetric encryption schemes, such as AES, for secure communication. Entanglement-based regimes for communication via quantum teleportation are particularly important for distributed quantum systems relevant to State strategic interests. Quantum teleportation [35, 40, 118] enables communication without measurement of an unknown quantum state from one quantum system to another via the use of entanglement, Bell state measurements and EPR channels [42].

2. Quantum Networking

Quantum networking is a major prospective application of quantum communication technologies [102] that utilises quantum teleportation to enable communication among multiple users across long distances without the need for inter-mediating local networks (albeit quantum repeaters are usually a feature of such systems). Quantum networking [128] and quantum teleportation [46] have particular strategic implications for State as a result of the prospect of a *quantum internet* [135, 85], representing a network of coupled and linked quantum computational and communication (and even sensing) devices enabling, in the communication context, high-volume and fast information distribution [114] via quantum states transmitted securely and robustly [47]. Such quantum internet proposals are expected to provide enhanced means of using quantum technologies relevant to State activity, including: performing QKD, quantum secure direct communication (allowing confidential information to be distributed without separate key distribution), distributed and used for distributed quantum computing, clock synchronisation, and quantum-enhanced communication.

3. Post-Quantum Cryptography

Post-quantum cryptography (PQC) [24, 36, 50] is a set of cryptographic protocols intended to be secure against adversarial attacks and decryption by adversaries equipped with scalable fault-tolerant quantum computers. PQC is motivated as a way of addressing the strategic threats faced by States and other actors [82] arising from the decryption capabilities of quantum computers identified above which can in principle decrypt public-key systems like RSA, Diffie-Hellman, and elliptic curve cryptography. Classical encryption schemes often rely upon standardised classes algorithm, such as integer factoring or discrete logarithm algorithms [95]. PQC algorithms, by contrast, leverage algorithms and encodings whose decryption is in a higher complexity class i.e. it is hard or intractable for even quantum computers, including lattice-based methods [107], learning-error based methods [39], multivariate polynomial systems, or isogeny problems on elliptic curves [92]. In general PCQ algorithms typically generate larger key and ciphertext sizes which exceed resources feasibly decode.

E. Quantum Sensing and Quantum Metrology

Quantum sensing [52] in its theoretical and applied forms examines how certain quantum mechanical properties of systems give rise to new and highly sensitive ways of measuring environments, collecting data. Doing so gives rise to finer-grained information about measurement statistics and probability distributions of environmental systems. Quantum sensing also has been shown to improve quantum metrology, often utilising quantum-

specific properties of superposition and entanglement, enabling more precise parameter estimation (quantum metrology) [63, 131]. One of the more advance forms of quantum sensing technology are *quantum dots* [79, 45, 31], types of quantum circuits engineered to confine electrons (or cavities) in particular constrained environments. Quantum dots have a variety of applications, and indeed are a candidate component of technology for quantum computational substrates themselves. The underlying concept of quantum dots is the confinement of single electrons within electromagnetic potentials such that their quantum mechanical state can be effectively tuned or adjusted, such as by way of control architecture involving microwave pulses, magnetic resonance of other methods. By doing so, quantum dots represent a controllable subsystem which may be coupled to an environment in ways that allow *both* for fine-grained control of quantum states (enabling, for example, the implementation of quantum circuit gates) but also enabling their use as a measurement instrument (or apparatus). Intuitively, this is because measurement and control are both interactions with the quantum system: measurement of quantum systems, particular POVM measurements which completely characterise a system, require that the particular eigenstates and eigenvalues of the measurement device are sufficiently well-defined in order that measurement outcomes are distinguishable and intelligible. Existing quantum sensing devices utilise the sensitivity of quantum systems realised via atomic, ion, photonic, or solid state systems for precision measurement. They tend to be classified according to either the quantum system or the target of measurement, with various physical characteristics such as sensitivity, weight, size, power and cost factoring into their use. Quantum sensor technology follows a protocol whereby sensors (i) are initialised, (2) are transformed into a quantum state (e.g. superposition), (3) interact with the environment via coupled evolution, (4) transformation into a measurable state (e.g. eigenstate), (5) measured. This process is then repeated sufficiently for measurement statistics to be gathered. For States, quantum sensors have application a range of applications that we mention below.

F. Quantum Infrastructure Stack

Quantum information technologies can be considered in the abstract, as a form of computational technology with particular unique effects unavailable to classical technology, or even more abstractly, as an affordance of States whose effects, rather than technical specificity, is what matters for normative and jurisprudential consideration. Yet such coarse-grained analysis overlooks important technical detail regarding how *quantum infrastructure stack*, within which quantum information systems are and will be necessarily embedded, affects strategic and jurisprudential factors. It is useful to assess this stack both *vertically*, in terms of how layers of classical and quantum architecture are integrated; and *horizontally*, in terms of how quantum and classical infrastructure are distributed and networked. Understanding the technical features of quantum infrastructure stacks can provide greater clarity on how and where States may actually act (where it the site or locus of

their action, at what layer in the stack, its degree of directness and so on) and, as a result, the consequences for the application of international law principles as a result. The two examples we adopt for the purposes of illustrating these technical considerations are (i) a single quantum computer and (ii) a quantum internet, comprising quantum computing nodes networked by either classical or quantum information channels (which might be for example a candidate quantum internet architecture).

1. Quantum Computing Stack

The typical qubit-based quantum computing stack can be represented via a layering of features as set out in Table 1. At the base of any quantum computing device is the *physical layer* upon which the quantum computational substrate is constituted, such as photonic, superconducting, trapped ion, topological and other systems. Overlaying the physical layer is the *measurement and control layer* comprising physical infrastructure for exerting fine-grained control over the quantum system, including that required for measurement, such as in the form of microwave pulses and laser signalling. The next layer is the *error correction layer* which encodes quantum error correction protocols, such as the surface code [66]. The *logical qubit layer* is way of abstracting the logical qubits formed via clusters and interactions of physical qubits (mediated via error correction protocols) and may include quantum memory structures. Foreshadowing our discussion of the Tallinn Manual below, logical qubits constitute an element of the logical layer of quantum infrastructure. From the logical qubit layer, there are then effective language and programming layers, such as (i) the *quantum assembly layer*, analogous to assembly code layers in classical computers; (ii) *quantum compilers* [61] which enable compilation of development environments and programs; (iii) *quantum intermediate representations* which are ontological representations that mediate between compilers and programming languages; (iv) *quantum programming languages* which are high-level interpretive languages with considerable expressive capacity; (v) the *application layer* for applications and user interfaces and where practically, for example, human interface for the application of quantum computing would apply. In addition, we can also specify a *classical interface layer* such as where quantum systems are encapsulated in classical components, such as classical registers or databases to store measurement statistics, classical specification of algorithms and the like. Each layer in the stack represents both a capability (quantum, classical or hybrid) and also a potential vulnerability which may be targeted by a State adversary.

Layer	Description
Physical Quantum Layer	The quantum computational substrate, which includes physical qubits realised using technologies such as photonic systems, superconducting circuits, trapped ions, or topological qubits. This layer involves the physical realisation of quantum states and their manipulation.
Measurement & Control Layer	Hardware control systems responsible for interacting with the physical quantum layer generating precise signals to manipulate qubits, such as microwave pulses or laser systems. These systems ensure the implementation of quantum gates and readout operations.
Error Correction Layer	Quantum error correction protocols, such as surface codes or concatenated codes, which detect and correct errors arising from decoherence and noise in the quantum system.
Logical Qubit Layer	Logical qubits formed from physical qubits through error correction, enabling more robust quantum computations by abstracting away the noise at the physical layer.
Quantum Assembly Language	Low-level programming languages designed for quantum computers, specifying quantum operations and circuits in a hardware-specific manner (e.g., OpenQASM [137]).
Quantum Compiler	Software tools that translate high-level quantum algorithms into executable instructions for the quantum hardware, optimising for specific hardware constraints and minimising error rates.
Quantum Intermediate Representation	Intermediate representations used by compilers to bridge high-level code and hardware-specific assembly instructions, allowing optimisations across different hardware platforms.
Quantum Programming Language	High-level languages used to write quantum algorithms, such as Qiskit and Cirq. These provide abstractions that simplify quantum programming for researchers and developers.
Applications Layer	End-user applications leveraging quantum algorithms, such as quantum cryptography, optimisation, machine learning, and simulation of quantum systems. This layer focuses on domain-specific problems addressed using quantum computing.
Classical Interface Layer	The interface between classical and quantum systems, managing hybrid computations, data input/output, and pre- and post-processing of results. This includes classical hardware and software integrated with quantum processors.

Table 1: A typical quantum computing stack, from the physical quantum computational substrate up through programming languages, compilers, and applications.

2. Quantum Network Stack

Quantum networks, whereby QIT systems form distributed systems, are an important prospective QIT use case for States as noted above. A quantum network in simpliciter involves quantum computers as nodes with message passing channels and is thus repre-

sentable as a graph. The infrastructure requirements for quantum networks are considerable: they include all the required infrastructure for a single quantum computing device, in addition to the complex infrastructure required to support distributed computing and messaging. In Table 2, we set out a number of key features of the quantum network stack. Doing so assists in our analysis in later sections regarding where and how States may interact (cooperatively and adversarially). Our taxonomy is generic but is based upon proposals for a quantum internet [135, 78]. Quantum networks [136] are comprised via *quantum nodes*, being quantum computers or processors that perform information processing and store quantum information. The nodes are connected via *quantum channels* that link each node and enable information transfer between them. Although these channels may be classical, to leverage the benefits of networked quantum systems, they are quantum channels. Overlaid on top of this core architecture are mechanisms for *entanglement distribution*. These may include a *quantum repeater* layer which extends the range of quantum communication via correcting for errors and amplifying entanglement. Quantum networks also require their own *classical control layer* for managing the network elements of the system (distinct from those at the node level), together with network-specific *quantum memory* for buffering and delayed operations. *Network protocols* represent an abstraction layer over the quantum network setting out how QKD, quantum teleportation and entanglement are managed. There may also be *classical nodes* themselves and a separate network *quantum application* layer for implementation of applications at the network level (such as for distributed quantum sensing) together with additional *security infrastructure* to secure the distributed physical infrastructure, *routing and topology management* and other distributed systems optimisation processes and of course error correction.

Component	**Description**
Quantum Nodes	Quantum computers or quantum processors that serve as the computational units in the network. These nodes perform quantum computations and store quantum information using qubits.
Quantum Channels	Communication links enabling the transfer of quantum states between nodes. Typically implemented using fiber optics, free-space photonics, or satellite-based systems to preserve quantum entanglement.
Entanglement Distribution	Mechanisms for generating and distributing entangled states across the network, forming the backbone of quantum communication protocols. Examples include entanglement swapping and quantum repeaters.
Quantum Repeaters	Devices that extend the range of quantum communication by correcting errors and amplifying entanglement across long distances. These are essential for large-scale quantum networks.
Classical Control Layer	Classical communication and synchronisation layer for coordinating quantum operations, transmitting measurement outcomes, and enabling error correction protocols.
Quantum Memory	Storage units for preserving quantum states during communication or computation. Quantum memories are critical for buffering entanglement and supporting delayed quantum operations.
Network Protocols	Protocols governing the operation of the quantum network, including quantum key distribution (QKD), quantum teleportation, and entanglement distribution protocols. These also include hybrid quantum-classical protocols.
Classical Nodes	Classical systems that interface with quantum nodes to manage control tasks, perform pre- and post-processing, and handle non-quantum computational tasks.
Quantum Applications	High-level applications running on the network, such as secure communication, distributed quantum computing, clock synchronisation, and quantum-enhanced sensing.
Security Infrastructure	Mechanisms ensuring the security of quantum communication, including QKD systems, eavesdropping detection, and classical cryptographic support for hybrid protocols.
Routing and Topology Management	Management systems that determine the optimal pathways for quantum and classical information, considering the unique constraints of quantum communication such as no-cloning and decoherence.
Error Correction Layer	Quantum error correction protocols to mitigate noise and decoherence in quantum channels, ensuring reliable transmission and storage of quantum states.

Table 2: Elements of a distributed quantum network detailing components and features of a quantum internet, where quantum computers act as network nodes.

G. QIT is embedded within classical information infrastructure

As we noted in a number of sections below, QIT is inevitably situated within classical infrastructure which forms an integral part of the operation and support of QIT. We include a taxonomy of such infrastructure in Table 3. A major and important element are classical control systems, including signal generators and pulse sequence controllers, which are essential for manipulating qubits and executing quantum operations, such as measurement, encoding of information within quantum systems and classical-quantum hybrid protocols, such as many quantum machine learning systems. Classical computing interfaces are also central to handling data processing, setting initialisation specifications, and overall management of QIT. In quantum communication, networking equipment such as classical routers and switches are essential to quantum devices being integrated into larger network architectures, enabling communication across quantum-to-classical and classical-to-quantum channels to subsist. Classical databases and registers are essential to retaining quantum experiment results, measurement statistics and computational datasets [113]. Power supply systems and cooling mechanisms are essential requirements of all candidate physical realisations of quantum systems, including cryogenic refrigerators, in order to ensure the stable operation of quantum hardware under precise, low-noise, environmental conditions.

In addition to surrounding physical infrastructure, classical processors are important components in quantum error correction, implementing syndrome measurements to detect and mitigate errors that arise during quantum computation. Classical systems are also essential to security architecture for QIT, protecting quantum infrastructure through firewalls and intrusion detection, safeguarding sensitive quantum operations. They are also critical to monitoring and diagnostic tools used to evaluate the performance of quantum systems, providing real-time insights into noise levels, stability, and efficiency. The classical-quantum interface acts as middleware, translating classical instructions into quantum commands and processing quantum results for classical interpretation. Together, these components form a comprehensive classical infrastructure that supports and enhances the functionality of quantum technologies.

Type of Classical Infrastructure	Description
Control Systems	Classical control hardware and software used to manipulate qubits, such as signal generators, microwave control systems, and pulse sequence controllers.
Classical Computing Interfaces	Classical computers and servers that interface with quantum computers, managing data processing, initialisation, and interaction with quantum systems.
Data Storage Systems	Classical storage solutions for retaining quantum experiment results, intermediate calculations, and large datasets required for hybrid quantum-classical computations.
Networking Equipment	Classical networking devices like routers, switches, and hubs that form the backbone for integrating quantum systems into broader networks, including quantum networks.
Error Correction Systems	Classical processors that implement error detection and correction algorithms for stabilizing quantum computations and communication.
Cooling Systems	Cryogenic systems required to maintain the operational environment for quantum hardware, such as dilution refrigerators for superconducting qubits.
Power Supply Systems	Reliable power infrastructure ensuring stable and uninterrupted operation of quantum and classical subsystems.
Monitoring and Diagnostics Tools	Classical systems for monitoring the status of quantum systems, including diagnostic tools for noise, stability, and performance analysis.
Security Systems	Firewalls, intrusion detection systems, and other classical cybersecurity measures to protect quantum infrastructure from unauthorised access.
Classical-Quantum Interface	Middleware that translates classical commands into quantum instructions and vice versa, enabling seamless operation between classical and quantum systems.

Table 3: Classical Infrastructure Surrounding Quantum Computers and Quantum Networks. This table outlines the classical systems that support and interface with quantum technologies.

III. Geopolitical Impact of Quantum Technologies

A. *Overview*

The growing capabilities of QIT, especially advancements towards fault-tolerant quantum computational devices potentially capable of facilitating decryption of classically encrypted information has motivated increased consideration of the impact of QIT on national security, national infrastructure, economic competitive advantage and information ecosystems within and among States [93, 108]. In this section, we survey the primary impact of QIT as they pertain to key characteristics of public international law and the law of conflict. As we discuss throughout, national security is an integral hallmark of the jurisprudential principle of State sovereignty at the heart of public international law. To study the geopolitical impacts of QIT, we map State behaviour to its classification in terms of quantum computing, quantum communication and quantum sensing. Later in this article, we consider three strategic scenarios involving States and its effect on strategic behaviour.

B. *Quantum Computing Impacts*

Quantum computing has extensive potential application in strategic contexts. Impacts of quantum computing capabilities derive from the unique aspects of quantum computing itself, such as simulation of physical systems, including chemical and biological systems, materials synthesis and more efficient composite materials, in ways not technically possible on classical computers. But perhaps the primary application of quantum computers in State adversarial contexts lies in their ability to solving complex optimisation problems and decryption. The use of quantum algorithms to solve optimisation, search and decryption problems rapidly in ways that that are infeasible on classical computers is central to their strategic impact. Of particular note is the ability to, in principle, solve certain classes of intractable problems (requiring exponential computational resources to solve) outside the reach of classical computing to solve due to being in a higher complexity class (and which could never be solved on a classical computer without exponential resource cost). We explore a few of these below:

1. *Optimisation and Machine Learning.* Quantum algorithms offer potential for solving certain complex optimisation problems, such as logistics and resource allocation, supply chain management and mission planning (pre- and during conflict scenarios for command and control systems), which are critical in military operations. Other more general applications include better or quicker decision-making, predictive analytics or verification procedures, though the extent to which quantum systems provide a practical advantage is yet unknown in general. An extension of such methods is the use of quantum algorithms (in concert in most cases with classical algorithms)

for quantum machine learning. Example prospective applications include quantum-enhanced (hybrid) algorithms for rapid classification of data, such as for example satellite imagery, or processing large-scale datasets more quickly.

2. *Simulations.* Quantum systems may be used in principle to more efficiently simulate certain classical systems faster than classical computers (and to incorporate more fine-grained information), relevant to for example scenario modelling, central to military planning. Quantum computers are also in principle able to more efficiently simulate other quantum systems themselves, a process essential for understanding complex materials and chemistry. Such simulations may help design better armour, explosives, and energy systems or model the use of for example biological agents by a State (or non-State) actor, enabling better preparedness against bioterrorism or chemical warfare. For example, the simulation of molecular interactions could help design antidotes or protective materials against chemical weapons.

3. *Cryptography*. Quantum algorithms techniques (such as those based on quantum Fourier transforms and Shor's algorithm) for decrypting existing public-key cryptographic systems, such as RSA, Diffie-Hellman, and Elliptic Curve Cryptography represent what is generally considered the primary application of quantum computing in adversarial strategic scenarios among States, both in peacetime and during conflicts. Quantum cryptographic capabilities are (if realised) also anticipated to be critical for State intelligence agencies, enabling both decryption of intercepted communications from adversaries and the ability to test the resilience of a State's own (or its allies') cryptographic encryption regimes to adversarial attack. Because encryption is central to the functioning of modern States, the strategic benefits from even moderate capacities for such decryption are considered strategically significant. Defensively, post-quantum cryptographic protocols which aim to secure information and communications systems from quantum adversarial attack is already a major focus of research efforts among States.

As we note below, quantum computing systems are necessarily embedded within classical computational architecture. Practically speaking, this means that State quantum computing infrastructure is likely to be cloud-based and distributed across quantum communication networks where fixed quantum computer edifices are interfaced via classical communication channels. Furthermore, as noted in our discussion of international law governing the application of QIT, strategic cyber operations and QIT-related activities among States will, as with their classical counterparts, occur in both peacetime and conflict scenarios.

C. *Quantum Communication, Quantum Networks and Quantum Cryptography Impacts*

Quantum communication, quantum networks and quantum cryptography (which we examine in a communication context here specifically) have significant strategic implications for States. From a strategic perspective, quantum communication provides both opportunities and challenges for state actors. Nations with advanced quantum communication capabilities can secure critical infrastructure, military communications, and financial systems against quantum and classical cyber threats. At the same time, quantum communication intensifies geopolitical rivalries as States compete to develop superior quantum technologies, including quantum cryptoanalysis to decrypt adversaries' communications. Quantum communication combines QKD, entanglement-based protocols, quantum networks, and QRNGs to offer unparalleled security and functionality. It is a cornerstone of the emerging quantum internet and has transformative implications for secure communication, distributed computing, and international strategic dynamics. However, its implementation poses significant technological and geopolitical challenges:

1. *Quantum networks*. One of the attractive potentials of quantum network technology is in overcoming limitations of (including attenuation) and risks of intervention in terrestrial fiber optics via the use of satellite-based quantum communication methods [97]. Examples include China's quantum experimental science satellite, Micius [100], enabling satellite-based QKD and entanglement distribution.

2. *Quantum Key Distribution (QKD)*. Recall that QKD is a secure communication protocol that enables two parties to generate and share a secret cryptographic key with the assurance that any eavesdropping attempt will be detected. QKD ensures ultra-secure communication by leveraging quantum mechanics to detect eavesdropping. States can use QKD for critical communication infrastructure, such as diplomatic, military, and intelligence channels of States, ensuring confidentiality and integrity in sensitive operations.

3. *Quantum Internet and Strategic Infrastructure*. Quantum communication networks, including quantum communication satellite-based systems, represent a prospective important form of peacetime and conflict QIT use. Such networks have particular dual use capabilities, especially in connecting national defense systems and critical industries securely and prospectively in conflict scenarios.

4. *Post-Quantum Cryptography*. Post-quantum cryptography has been a major focus of research efforts by States seeking to secure their networks against potential adversarial interference, interception and espionage. This is manifest in the long-term PQC programme of NIST in the United States leading to a PQC standardisation regime [25, 24]. PQC is a major priority for quantum-capable nation states because of the

information security affordances it potentially offers against an adversary using QIT, such as for espionage or during conflict.

D. Quantum Sensing

A number of prospective use-cases of quantum sensing have potential strategic impact.

1. *Submarine detection*. Submarine detection holds significant consequences for strategic relationships among nuclear States due to the consequences for a State's second-strike capability in the event of nuclear armed conflict. Existing methods of submarine detection rely upon magnetic anomaly detection, which measures disturbances in the Earth's magnetic field caused by a metallic substances within a submarine's hull. The prospective application of quantum sensors lies in their potential to improve sensitivity to these disturbances, enabling detection at greater distances. There are, however, significant technical challenges hindering the use of quantum sensors for submarine detection [117]. These include ocean noise (where magnetic disturbances from sources like ocean currents and mineral deposits, interfere with a submarine's magnetic signature), proximity requirements (all sensors, including, quantum sensors perform better closer to submarines), limited range (quantum magnetometers such as those utilising nitrogen vacancy have limited operational range), target variability (where submarines may vary their signatures via methods such as degaussing) and the movement of submarines themselves. Empirical analysis of current quantum sensing technology (and nascent technologies such as quantum gravimetry and synthetic aperture radar) suggest that near-term submarine tracking is unlikely.

2. *Missile tracking*. Quantum sensors also have potential application missile tracking via improving the accuracy of inertial navigation systems used in ballistic missiles. Inertial navigation relies on accelerometers and gyroscopes to track an object's motion without external references. Quantum sensors could increase the precision of such instruments and thus enable finer-grained targeting. The technology could also provide an in principle advantage by reducing initial alignment errors, mitigating gyroscopic drift due to other noise sources (such as heat or kinetic energy), albeit doing so requires overcoming specific technical challenges to ensure they remain robust.

3. *Quantum sensor networks*. Quantum sensor networks maybe also be networked in order to created highly-sensitive quantum communication architectures. Quantum sensor and communication networks leverage the physical characteristics of quantum sensor technology and quantum communication protocols to create distributed networks of quantum sensors across wider geospatial distances while retaining the

benefits of quantum communication security features. Quantum systems being used as quantum sensors are entangled with other quantum systems in long-range networks. An example candidate protocol theoretically explored is integrating quantum sensing and communication via entanglement. A number of protocols exploring quantum sensor networks have emerged recently, including the QISAC protocol [98] leveraging Bell states for simultaneous quantum sensing and communication. In this case, Alice prepares and transmits entangled photon pairs to Bob via a quantum channel. Both parties perform randomised measurements on subsets of particles to confirm channel security with the remaining particles being encoded with information and used in sensing operations by Alice (such as for parameter estimation). Bob measures the received states, decodes the messages and retrieves the measurements statistics in question. Other proposals include cavity-based multipartite entanglement [43], distributed quantum sensing systems using spin-squeezed atomic states leveraging non-local entanglement for improved scaling effects [101]. Challenges include technical design and engineering issues especially at the NISQ stage [116], but also more broadly the fact that quantum entanglement diminishes after each use (or measurement) of the quantum network itself. In quantum information science parlance, quantum entanglement is a resource [140] (meaning it is both a necessary resource for certain types of computation or information not otherwise possible and that it diminishes once used).

IV. Technical Factors Affecting Strategic QIT

A. *Classical and Quantum Strategic Taxonomy*

In this section, we briefly examine a number of technical factors regarding strategic QIT use. As with the comparison between quantum and classical information processing itself (as is common in information sciences when describing classical and quantum channels [134]), strategic behaviour of States related to QIT can be taxonomically classified in terms of quantum and classical relations:

1. *Classical-to-classical*, covering the use of classical information processing with respect to classical information technology (e.g. conventional cyberattacks).

2. *Classical-to-quantum*, covering the use of classical information processing to act in relation to QIT.

3. *Quantum-to-classical*, covering the use of quantum resources and QIT to act upon classical information (or information processing systems), as exemplified by for example quantum algorithms for decrypting classically encrypted information.

4. *Quantum-to-quantum*, involving the direct use of quantum-specific processes on quantum resources.

This taxonomy is a useful way to situate the interrelationships between quantum and classical technology in the context strategic behaviour. There is also the added complexity of hybrid systems that leverage both classical and quantum (QIT will always be integrated within classical information systems infrastructure). We note both this and summarise this taxonomy in Table 4 below. We utilise this taxonomy in scenario modelling of strategic State behaviour in section V and our analysis of the implications under public international law in section VI below.

Information Processing	Infrastructure		
	Classical Infrastructure	Hybrid Infrastructure	Quantum Infrastructure
Classical Processing	State-sponsored cyberattacks targeting classical systems (e.g., hacking government databases, disrupting power grids).	Use of classical methods to infiltrate hybrid systems (e.g., exploiting weaknesses in hybrid cryptographic schemes).	Espionage on quantum research facilities using classical surveillance and analysis techniques.
Hybrid Processing	Quantum-informed attacks on classical systems (e.g., using quantum-inspired optimisation to identify vulnerabilities in infrastructure).	State-backed operations combining classical and quantum methods to breach hybrid networks (e.g., intercepting classical-quantum communication).	Manipulation of quantum components in hybrid systems to disrupt or disable functionality.
Quantum Processing	Quantum cryptographic attacks on classical communication channels (e.g., breaking classical encryption using quantum computing).	Quantum-based interference in hybrid systems (e.g., using quantum simulations to disrupt hybrid networks).	State adversaries directly attacking quantum networks or systems (e.g., disrupting quantum entanglement or intercepting quantum communication).

Table 4: Comparison of adversarial State classical, hybrid, and quantum information processing actions applied to classical, hybrid and quantum infrastructure. *Classical-to-classical* attacks represent classical adversarial action against classical infrastructure; *classical-to-quantum* represents targeting quantum infrastructure using classical methods; *quantum-to-classical* attacks utilise QIP against classical infrastructure or information (e.g. decryption); *quantum-to-quantum* represents the use of QIP to target quantum infrastructure.

B. Quantum Systems are Classically Embedded

An important fact of QIT from a governance and strategic perspective is that all QIT is necessarily embedded within classical information processing architecture. The ontolog-

ically [28] quantum characteristics of quantum information systems - quantum states in superposition or entangled quantum states - cannot be directly observed. Rather, their representation is reconstructed via the results of classical measurement statistics arising from repeated measurements upon identically-prepared copies of the quantum system in question. These measurement statistics are in turn used to reconstruct, for example, quantum states via state or process tomography [67, 104]. The inherently non-classical nature of quantum systems is represented classically by way of non-deterministic paradigms such as probability. In the language of quantum information, measurement is a quantum-to-classical channel. The manner in which quantum systems are controlled is also classically based: quantum control, such as the control required to have a quantum computer undertake a quantum computation, ultimately relies upon translating instructions and information from classical systems (the controlling system or human input channel) to quantum systems. This is an important point to bear in mind. In cyber attacks, such as penetration of an adversary State's cyber infrastructure, the actual computational processes underpinning that penetration within an adversary's classical network will be classical. It is not the case that for example a quantum algorithm could be deployed onto an adversary's classical network (to afford quantum advantage offered by such algorithms for example). For a State adversary with a quantum computer, in principle it may be possible to, for example, hack the classical infrastructure surrounding the quantum device to embed a copy of a particular algorithm by way of for example interfering with the classical description of quantum compilation [84] protocols, but this potential (which would in any foreseeable future be remote) in turn relies upon mediating information between classical and quantum systems.

C. Direct quantum-to-quantum offence is difficult but possible

In principle it is of course possible for two quantum systems to interact in ways that are 'directly quantum' in that the proximity of those systems causes them to be coupled in a quantum-specific way, such as via entanglement. However, engineered pure 'quantum-to-quantum' cyber operations would be at current technology levels incredibly challenging, if not impossible, to effect. This is because the *direct* interaction between two States' quantum systems without classical mediation requires networking of those quantum computers which physically means coupling of all or part of those systems to each other. While quantum computers - as with classical computers - are always coupled to their environment to some degree, the technical challenges to such coupling in an adversarial context are formidable. Thus the prospect of mobile QIT devices being utilised by State adversaries for espionage activities within a rival State are remote if not impossible due to the fundamental conditions required for quantum systems to remain robust, controllable and stable.

The exception to this scenario, which we explore further below, is where two States' quantum systems are entangled. It may seem fanciful that two State actors would willingly

entangle their QIT resources despite being adversaries, but plenty of instances of adversaries sharing resources during competitive and even conflict scenarios about throughout history. In the quantum case, a primary example would be the sharing of QIT by way of quantum networks. As discussed above, the networking of quantum computing can significantly affect the computational power and capabilities. The whole of a quantum internet is literally greater than the sum of its parts. This can be seen in elementary fashion by the fact that the number of computational states (and dimension of the Hilbert space) of an n qubit system is 2^n. Thus as n increases, the dimensionality - and thus its computational expressiveness - increases exponentially. In peacetime, States would thus be motivated to network their quantum devices in order to leverage the computational gains from such cooperative coordination of shared resources. States may subsequently become adversaries - but may also decide to share resources during conflict. Thus the prospect of shared QIT resources, such as entangled quantum systems, is not completely implausible. In this scenario, in principle we have something resembling 'direct' quantum means of each State affecting the other via quantum actions which affect the mutually entangled quantum system. It should be noted that actually controlling such an attack would itself in most cases require classical inputs (i.e. classical inputs into the control regimes). Such quantum-to-quantum interference could take the form, in principle, of interfering with both quantum data and QIT processes themselves, such as how computation unfolds or how communication occurs.

D. Classical-to-quantum cyberattacks can interfere with QIT and quantum infrastructure

While the prospect of a State actor interfering with another State adversary by way of direct quantum-to-quantum interaction may seem remote, classical-to-quantum adversarial behaviour by States is possible. Such behaviour is constituted by the use of classical information processing, such as conventional classical cyberattack strategies, directed towards a State adversary's quantum infrastructure. Because any QIT infrastructure is necessarily embedded within classical information systems - those which transmit information from the quantum system (e.g. via recording and storing the results of measurement) and into the system (via classical control signals, or classically-described protocols for state distillation or preparation) - those classical channels can be leveraged for adversarial activity.

E. Most adversarial quantum activity will be locally constrained

The consequences of the foregoing are that, at least based on current and near-term forecasts, any use of QIT for State adversarial action is likely to be limited to mostly immobile QIT devices, or QIT devices whose mobility is constrained (such as those integrated into other mobile platforms such as vehicles). The most plausible *offensive* use cases are to

do with quantum cryptography and quantum sensing where for example immobile networks of quantum computers are used to decrypt intercepted classical communications, or stationary quantum sensor networks are used to detect a State adversary's activities. The exception, once more, is where adversarial action involves entangled quantum systems which are geographically remote, but which can be acted upon non-locally by one State's interaction with its own entangled quantum system. Such a scenario certainly would involve non-locality as a principle, but the actual action of a State (say which might seek to interfere with a joint quantum network in that way) would still require that they act locally upon their own local quantum system. This is because the physical substrate, such as the qubits of an entangled system, are for most intents and purposes local themselves. While they exhibit a degree of non-locality (via measurement uncertainty in their position or momentum degrees of freedom for example), the concentration of probability (measure) is in almost all realistic cases going to be within very narrow spatial bounds (in part because such systems need to be localised to be instantiated and controlled in the first place). The element of control remains, in this sense, local. The consequences of the foregoing are that, at least based on current and near-term forecasts, any use of QIT for State adversarial action is likely to be limited to mostly immobile QIT devices, or QIT devices whose mobility is constrained (such as those integrated into other mobile platforms such as vehicles). Table 5 sets out some speculative examples of how classical information processing and cyber activities by one State could adversarially target and act against another State's quantum infrastructure.

Type of Adversarial Activity	**Examples**
Disruption of Classical Control Systems	Interfering with the classical hardware or software responsible for controlling quantum systems, such as modifying pulse sequences or disrupting signal generators used in quantum gate implementation.
Hacking Classical Infrastructure Supporting Quantum Systems	Targeting classical systems that support quantum computers, such as data centers, control servers, or networks that transmit classical instructions to quantum systems.
Manipulation of Classical Instructions	Altering classical instructions used to initialise or operate quantum systems, such as tampering with qubit initialisation parameters or gate sequences in quantum programs.
Classical Interference with Quantum Algorithms	Embedding malicious classical descriptions of quantum algorithms or Hamiltonians into the quantum system prior to quantum compilation, causing the quantum system to behave incorrectly.
Cyberattacks on Quantum Network Nodes	Launching classical cyberattacks on quantum network nodes to disrupt entanglement generation or transmission of quantum states.
Intercepting Classical Communications in Quantum Protocols	Intercepting or tampering with classical communication channels used in quantum key distribution or error correction protocols.
Physical Disruption of Quantum Systems	Using classical tools to physically disrupt the environment of a quantum system, such as inducing electromagnetic interference or modifying temperature controls.
Classical Malware in Quantum Systems	Embedding classical malware into the classical-quantum interface, such as corrupting firmware updates for quantum devices or injecting malicious code into classical simulators of quantum systems.
Disrupting Quantum Compilation Processes	Targeting classical compilers that translate high-level quantum algorithms into executable instructions for specific quantum hardware, causing errors in the generated quantum circuits.
Classical Attacks on Quantum Sensor Networks	Using classical computational or signal-jamming methods to disrupt the operation of quantum sensors, such as quantum radar or magnetometers, by interfering with their classical data processing layers.

Table 5: Taxonomy of classical-to-quantum adversarial actions by States including examples of how classical information processing can be used to disrupt or interfere with another State's quantum infrastructure.

F. QIT can enhance cyberattack strategies

As noted above, one of the major motivations for the use of quantum computing is the existence of certain algorithms which enable, in principle, the decryption of classically encrypted communications and data. The most celebrated of such algorithms is *Shor's algorithm*, a quantum algorithm based upon the class of quantum Fourier transforms which in principle provides a means of classically (within at most polynomial time) decrypting information encoded using classical encryption protocols such as RSA. While the practi-

calities of decryption using a quantum computer executing such an algorithm are complex (see [74] for a discussion of constraints), it is this potential impact which is of considerable, indeed major, focus of States, motivating much of the funding envelope driving research into quantum computing and QIT. Information confidentiality and encryption has a rich provenance throughout State conflict and interactions [30]. The celebrated example of Turing's involvement in the decryption of the Third Reich's *Enigma* encryption device [130] is a practical case in point. All modern national security apparatuses rely upon modern encryption protocols for their communication and data integrity. Data confidentiality is also critical to fundamental strategic imperatives such as nuclear stances and doctrines that shape and define modern State geopolitics. In analogy with nuclear and other dual use technology, the fact dual use of such technology shapes governance approaches to it. In practice, the use of QIT, such as quantum computing devices to execute variants of Shor's algorithm to break classical code represents a hybrid approach that would leverage both classical-to-classical eavesdropping and espionage techniques in order to gather data (we set aside the use of quantum sensing for this objective) and then quantum information processing techniques to decrypt and return the decrypted information to a classical register.

1. Quantum decryption does not afford omniscience

We consider in more detail the technical aspects of the likely use of quantum information systems for decryption in sections below. However, it is important to note the practical constraints upon QIT used in cyberattacks, for example in cryptoanalysis, data gathering (eavesdropping) of deception attacks. QIT is not some sort of omniscient oracle. Thus even the application of Shor's algorithm to gathered and stored data will take considerable time across each possibility. Classical controls and constraints will continue to apply. Nevertheless, the use and combination of QIT in cyber offensive activities related to decryption is a significant consequence of the technologies that is shaping governmental and institutional responses to quantum technology.

2. Quantum decryption and classical infrastructure

Offensive use of QIT can also be classified in ways that borrow from classical cybersecurity literature. Quantum-based offensive cyberattacks against classical information systems exploit weaknesses of those systems to enable and amplify their impact. They must also engage with classical systems and infrastructure. Examples include:

1. *Data gathering*, where classical data is stored in advance until quantum cryptoanalysis is possible;

2. *Data processing*, where information gathered in side-channel attacks can be more efficiently searched (e.g. using Grover-style algorithms noted above), or where the search for trajectories through complex networks may be optimised on a quantum computer;

3. *Quantum simulation* may enable, for example, scenario modelling by States to plot effective cyber attack strategies;

4. *Entanglement* which can enable untraceable coordination among cooperating adversaries.

Such cryptoanalysis based attacks relying upon analysing data gathered or stored in registers include a classical component. Quantum-based methods, such as the application of Shor's algorithm and related decryption quantum protocols involve classical activities as well. Thus *store-now, decrypt-later* (SNDL) attacks may involve classical interception of classically-encoded communications for later decryption. Cryptoanalysis can also interfere with classical key distribution, such as Diffie-Hellman exchange protocols, allowing interception or impersonation.

3. Quantum sensing

Quantum sensing also has application in adversarial and defensive cyber activities. We set out a few examples below:

1. *Enhanced Side-Channel Attacks*. The sensitivity of quantum sensors to electromagnetic spectra and acoustic emission disturbances may allow collection of finer-grained or higher-resolution data as part of a broader cyber attack strategy.

2. *Attack detection*. Quantum sensing devices may be able to detect the use of interception devices themselves, e.g. where low-power signals or perturbances indicative of interception technology or the equivalent of wire-taps are being used by an adversary. Other proposals of a more speculative variety include augmented quantum sensing used in radar systems [93].

G. QIT effects on strategic behaviour

The unique features of quantum information technology have implications for how States utilising such technologies strategically behave in response to each other in ways that in principle differ from classical strategic behaviour. We can assess this via studying scenarios involving quantum resources (such as quantum communication resources) along with considering how States may act in cooperative or non-cooperative ways during peacetime

or conflict. The strategic impact of quantum technology is modelled theoretically by quantum game theory [71, 41, 56] representing a subset of research into quantum strategies which considers differential effects of decision-making involving quantum information processing [103] (see [69] for a still-relevant summary). Because multi-agent games and behaviour, including those of States, can be viewed in terms of distributed systems (and even modelled in part using distributed algorithms), quantum game theory has specific relation to circuit architecture and distributed quantum systems frameworks (see [41] and [51] for a discussion). Implications of and results of quantum game theory include:

1. *Different equilibria*. Quantum variations of classical games enable players to share entangled quantum states giving rise to equilibrium strategies where both players may achieve higher payoffs than in the classical Nash equilibrium context, such as in quantum versions of the Prisoner's dilemma which enable cooperative outcomes. These strategic outcomes are not feasible classically.

2. *Strict Dilemmas*. So-called 'strict dilemmas' where incentives and rational agency of players can lead to suboptimal and non-Pareto outcomes can in certain cases be supplanted where quantum resources are available (again the Prisoner's dilemma is the canonical case).

Intuitively, quantum resource availability alters classical cooperation and defection strategies. Classically, cooperation usually relies upon (i) external enforcement mechanisms such as treaties, third-party oversight or reputational considerations to motivate State behaviour or (ii) repeated interactions among States to build trust or (iii) mutually shared resources or interests which are at risk if cooperation is not undertaken. The availability of quantum resources provides an effective self-enforcing mechanism. This is for two reasons. First, shared entanglement motivates honest behaviour to reduce the chances of a State secretly changing its strategy or deceiving in communications due to the no-cloning theory and measurement constraints. Thus State communication may be encoded using entanglement methods or encrypted in ways that can detect changes in strategy and decision making (e.g. the decision to defect or not), motivating States to act honestly by the fact that their decisions are detectable or verifiable (the idea being that requiring State communication through quantum channels - because only communications via that channel were valid- say in prisoner dilemma contexts would give rise to such dynamics that are distinct from the classical case). Secondly, quantum protocols can verify randomness and therefore strategic behaviour dependent upon randomness, such as where distribution of outcomes depends on an agreed procedure involving random sampling, thus providing a means of enforcing agreed upon outcomes via cryptographic protocols. Entanglement-based protocols require, however, some degree of cooperation and are conditional on a number of assumptions including:

(a) *Cooperation on quantum resource use*. States must at some stage have agreed to share quantum resources (inadvertent entanglement is unlikely) e.g. such as via quantum communication networks (albeit States may later become adversarial) in order that entangled quantum states may be accessible by both.

(b) *Technical capabilities*. States must have the resources and technical expertise to utilise quantum resources (we touch upon this below in the context of strategic computational umbrellas where certain nation states have access to computational - AI or quantum - resources and others to not, affecting their strategic choices).

(c) *Rationality*. States are assumed to be rational or mostly rational in order to recognise the benefits of cooperation over defection.

Another source of content for State economic strategic behaviour is that of quantum economic behaviour among States. This includes quantum analogues of classical economic behaviour [75], such as contracting, principal-agency theory, exchange of commodities and market design, along with information asymmetry principles [76, 77]. States engaging in peacetime cooperative and competitive behaviour often do so through economic channels and the availability of quantum resources via which to conduct economic activity thus gives rise to novel forms of strategic behaviour. We consider the strategic behavioural activity of States with respect to QIT in more detail in section V below.

H. Prospective Strategic Quantum Technology & AI Umbrellas

Another possible effect of QIT technology is on the behaviour of nation States who do not and cannot obtain QIT advantage, but may experience harm from State adversaries using QIT (e.g. via decryption in conflict scenarios). Where such non-QIT equipped States have the means to intervene, such as via conventional or unconventional (e.g. nuclear) means, they may consider whether to do so early prior to States obtaining an runaway advantage in QIT technology. These dynamics are not restricted to QIT per se, but they speak to how emergent new technologies that may provide acute asymmetric advantages could be responded to. They also speak to broader questions of strategic State alliances akin to *computational alliances* (or information-processing alliances), where, in analogy with nuclear alliances or umbrellas, States cooperate and coordinate alliances for the mutual use, benefit and strategic deployment of quantum information processing and computational resources.

V. GEOPOLITICAL SCENARIOS

A. Overview

The foregoing technical analysis of QIT gives rise to questions about the practical and applied scenarios in which QIT would give rise to strategic State behaviour. Is the use of QIT give rise to unique geopolitical effects distinct from other computational and informational technologies? And what consequences might these effects have for international law? To consider how the technical prospects for use of QIT have consequences within the framework of international law discussed in the previous section, we consider strategic behaviours along different dimensions. Firstly, whether States are in *peacetime* (defined as the absence of State armed conflict) or in *conflict* (defined as the presence of State conflict, which may be binary between States or between alliances). For each such scenario, we consider whether States act *cooperatively* (such as trade partners in peacetime or allies in conflicts) or *adversarially* (such as economic competitors in peacetime or adversaries in war). Using this taxonomy, scenario modelling can then consider how different classes of QIT use may apply. To give a flavour for the types of activities, we set out some prospective examples in Table 6. These include: (i) *optimisation problems*, such as logistical activities or strategic planning; (ii) *quantum simulations*, for materials discovery or strategic simulation; (iii) *cryptoanalysis*, including post-quantum cryptography cooperation or adversarial decryption; (iv) *machine learning and AI* enhanced using QIT; (v) *searching* and data mining using QIT (e.g. Grover-based algorithms); (vi) *quantum cloud computing* to enable wider interface among States to distributed QIT; (vii) *post-quantum cryptography* to strengthen State information security. We draw upon this taxonomy in the next section to develop scenarios used in our analysis of public international law implications of strategic QIT use further on.

Quantum Technology in International Relations				
Category	**Peacetime**		**Conflict**	
	Cooperative	**Adversarial**	**Cooperative**	**Adversarial**
Optimisation Problems	Collaboration on logistics optimisation for disaster relief or development of mutual infrastructure.	Monitoring adversarial advancements in logistics optimisation or competitive trade strategy.	Joint optimisation of logistics and planning for allied military operations.	Disrupting adversarial military planning or interfering with supply chains or predicting strategic behaviour of adversaries.
Quantum Simulations	Joint research on quantum chemistry products, pharmaceuticals.	Simulating competitive markets or negotiations.	Development of advanced materials and defense strategies.	Weaponising simulations to gain battlefield advantage.
Cryptoanalysis	Collaborative development of post-quantum cryptography.	Intercepting adversarial encrypted communications for market intelligence.	Testing secure communication systems among allies.	Decrypting adversarial communication networks during conflict.
Machine Learning and AI	Quantum enhanced shared civilian AI infrastructure for public benefit (e.g., smart cities).	Monitoring adversarial AI activities for potential military applications.	Using quantum computing with AI for battlefield intelligence and decision-making.	Using QIT with AI for autonomous military systems and cyber warfare.
Searching	Quantum data mining for global humanitarian purposes.	Data mining of market competitor communications.	Quantum sensing to track and search enemy troop movements using.	System search routing using to assist in cyberattacks on adversaries.
Quantum Cloud Computing	Shared quantum cloud for collaborative global research.	Quantum sensor networks for detection.	Secure quantum networks for inter-allied military coordination.	Enabling distributed use of QIT during conflict.
Post-Quantum Cryptography	Global collaboration to establish resilient cryptographic standards.	Developing countermeasures against adversarial cryptographic advancements.	Implementing quantum-resistant communications among allies.	Exploiting vulnerabilities in adversarial cryptographic systems.

Table 6: Strategic uses of QIT, highlighting the use of quantum technologies in peacetime and conflict, divided into cooperative and adversarial contexts.

B. Strategic scenario modelling

To study the implications of State strategic the use QIT (and its implications under international law) we consider simple scenarios of State strategic behaviour related to QIT. The scenarios we use are designed to deliberately highlight the application of public international law principles to cyber activities primarily set out in the Tallinn Manual. Each scenario is constructed to focus upon the unique or *sui generis* aspects of QIT as they relate to State behaviour, concentrating on the unique affordances that QIT enables which classical cannot. Our focus in this paper is primarily upon adversarial behaviour during peacetime and conflict, but we note the raft of international regulatory frameworks that would also apply to cooperative behaviour in peacetime and during conflicts. For each scenario, we consider adversarial State behaviour: in peacetime, we consider adversarial behaviour as *competitive*; while in conflict situations, we consider such behaviour as *offensive*. These can be itemised as follows:

1. *Peacetime / Cooperative*: where each State seeks to coordinate their use of quantum resources to act cooperatively in order to achieve an objective, which may be the construction, or expansion, of distributed quantum infrastructure, global research initiatives and so on;

2. *Peacetime / Adversarial*: where one or more States seeks to use quantum resources act adversarially to obtain an advantage over other States, such as by way of economic competitive advantage, or cyber espionage;

3. *Conflict / Cooperative*: covering where States may enter into alliances or coalitions during conflicts affecting how they may use their quantum resources; and

4. *Conflict / Adversarial*: where States use their quantum resources to seek to obtain a military advantage.

We also discuss briefly the consequences of asymmetric possession of QIT capabilities as asymmetries in technology can motivate State behaviour, such as striking or acting (e.g. in anticipatory self defence) to obtain an advantage before a technology gap becomes too great. In an elementary sense in which possession of QIT affords a comparative advantage with respect to a strategic decision, such as in conflict or negotiation, each scenario above represents a simple game whose structure, such as potential Nash equilibria, may be studied to inform toy models of strategic behaviour. A game-theoretical approach to modelling impact e.g. the strength of inclination to take a particular action being reflection of a the weight or importance a State places on that action (such as a response to a cyber attack, or the use of QIT adversarially) is of independent research interest and able to draw upon the developing body of work on quantum games mentioned in section G (*QIT effects on strategic behaviour*) above. However, our focus is instead on using these scenarios to draw

out their international legal implications. To this end, two main scenarios and variations on them.

1. Scenario 1: Asymmetric Quantum Infrastructure

In Scenario 1 (Table 7), State A has access to QIT while State B does not. We then consider two examples where State A utilises its QIT adversarially: in peacetime to conduct industrial espionage and in conflict situations to decrypt military communications. We consider how this QIT asymmetry affects their strategic behaviour and study consequences under international law in the next section.

Item	Description
States	State A (with QIT) and State B (no QIT).
Technology	State A has access to an idealised quantum computer and quantum sensor network (comprising quantum sensors located within and outside its territory) connected by a quantum internet (within its territory)
Peacetime	State A conducts espionage via an SNDL decryption attack against State B, intercepting or conducting espionage to obtain data about State B's industrial production, storing it and decrypting it using its quantum computer. The interception occurs both within and outside its territory. The decrypted information is used to obtain economic competitive advantages.
Conflict	State A decrypts strategically sensitive military communications and uses its quantum sensor network to eavesdrop on State B and decrypt its communications. State A utilises its ability to decrypt classical communications in order to determine classical private keys and protocols use by State B to encrypt its network. It uses that information to launch a cyber operation that disables State B's military surveillance network and to obtain strategic military advantage.

Table 7: Scenario 1: Asymmetric Quantum Infrastructure

2. Scenario 2: Entangled Quantum Networks

In Scenario 2 (Table 8), we add more complexity and variation. State A and State B both share access to a single quantum resource, quantum internet e.g. distributed quantum network where both their quantum resources (e.g. qubit resources) are entangled. The quantum internet stack is taken to be that set out in section 2 (*Quantum Network Stack*) and set out in Table 2 above.

Item	Description
States	State A (with QIT) and State B (with QIT).
Technology	State A and State B share entangled quantum resources in the form of entangled qubit-based quantum computers and an entanglement-based quantum internet. State A and B initially entangled their quantum resources and participated in the establishment of a quantum internet across their jurisdictions. The quantum internet is used within each State and by each State internationally.
Peacetime	State A exploits the shared entangled resources to solve complex problems such as factoring large integers for cryptanalysis or simulating intricate molecular structures—tasks enhanced by quantum correlations. While both States use the quantum internet for secure scientific exchanges, State A covertly measures certain entangled qubits, subtly extracting sensitive patterns from State B's quantum data without triggering obvious alarms.
Conflict	State A intercepts or manipulates entangled qubits carrying State B's classified directives, thus undermining secure quantum key distribution and real-time strategic coordination. By exploiting its QIT, State A disrupts State B's critical communications and decision-making processes. The quantum network—once a cooperative computational platform—now amplifies State A's offensive capabilities, granting it intelligence and control over State B's most sensitive military operations.

Table 8: Scenario 2: Entangled Quantum Networks

VI. International Law and Quantum Information Technologies

A. Overview

Having surveyed the QIT technology landscape, we now examine the sources of international law governing such strategic uses of quantum information technologies by States. As a set of information technologies, we consider how the use of quantum information technologies is situated within broader international law governing classical information systems, what are often denoted by the term 'cyber technologies'. We examine the main conventions, customs and other sources of international jurisprudence on information systems usage by States generally. There are no treaties at international law specifically designed to regulate the use of information technology or cyber activities by States. We rely upon key principles of international law and cyber activities of States as set out in the Tallinn Manual. We then provide scenario analysis of State adversarial interaction using QIT described above in order to identify any unique consequences or dilemmas arising under international jurisprudence from the use of such QIT.

The conceptual framing we adopt is that of typical international law analysis. Specifically (and as we discuss below), this ranks normative and legal imperatives according to the canonical principle of State sovereignty as set out in treaties, customary law and jurisprudence. State sovereignty sets out the justification for rights, obligations and interests of States under international law, including definitions of territorial and other sovereignty, actions which infringe upon sovereignty and actions by States justified in terms of preservation of State sovereignty. In practical terms, this situates QIT in instrumental terms, be it as infrastructure, a tool of State maintenance, or as an offensive or defensive technology.

B. Tallinn Manual

The leading international law resource dealing with the application of international law to cybertechnology and computational technology for state-based conflicts is the Tallinn Manual (the *Manual*) [121]. The *Manual* represents probably the most comprehensive analysis to date of how existing international law applies to cyber operations. Developed by a committee of international law experts, the *Manual* examines international law doctrine as applicable cyber activities occurring both during peacetime and conflict scenarios. Given its leading status within jurisprudential scholarship on international cyber activities, we focus on the content *Manual* as a means of analysing the consequences of State use of QIT. In later sections, we consider the extent to which international cyber jurisprudence may benefit from supplementary concepts to handle any unique consequences of QIT together with consideration of the types of international legal instruments that may be contemplated as a means of regulating (actively and pre-emptively) State strategic use of QIT. Thus in practice, the distinctly *quantum* nature of, for example, cyber operations may be

contained and limited to improving classical capacities or classical outcomes. QSuantum computation used for decryption only (rather than say interception using quantum devices) will rely in most cases on classically gathering or intercepting information, inputting that information into a quantum computer executing a quantum algorithm to decrypt such information whose outputs will be rendered classically. Any action consequent upon this will be classical in nature. One way to frame this is by comparison with classical artificial intelligence technologies. The impact of AI can be framed as (i) *epistemic*, enabling more accurate prediction or greater information asymmetries whose actions are merely communication and messaging (e.g. responses to queries, outputs of computational processes) and (ii) *agentic*, where AI systems, such as AI-based agents (be they traditional or language model agents) may interact with the environment and world via *acting*, causally effecting some change. Quantum information systems may utilise quantum algorithms - or forms of quantum advantage - to obtain advantages epistemically, but the specifically *quantum* actions which may be performed are limited (e.g. to where for example some uniquely quantum effect, such as entanglement, causes some change in environmental state). Simplifying, classical computation (e.g. classical AI) thinks and acts classically, while quantum computation thinks quantumly but (in the scenarios with which we are concerned) acts classically. To refine our analysis further, we continue with the classical-quantum strategic taxonomy set out above.

C. Key jurisprudential concepts and QIT

Before setting out a more fulsome analysis of key concepts from the *Manual* in relation to QIT, we include below discussion of a few recurring conceptual themes that arise when considering the effect and application of QIT. As we note above, QIT is anchored in the phenomena and laws of quantum mechanics. The unique features of quantum information processing systems as distinct from classical give rise to specific ontological and epistemic differences which have consequences for a number of ordinary, but relatively fundamental, concepts underpinning public international law jurisprudence. We list out a number below in advance of considering select sections of the *Manual* in detail. The primary phenomena we concentrate on are those of quantum superposition and quantum entanglement.

1. Quantum systems are stochastic

While great care goes into theoretical and applied means of governing quantum evolution via Hamiltonian specification, the outcomes of measurements of the evolved quantum states are stochastic. Jurisprudence on cyber activities in international relations as set out in the *Manual* distinguishes between physical, logical and social layers of cyberspace. This is premised upon a classical conception of the underlying physical substrate of information systems behaving classically, whose properties are in principle known or measureable and

consistent and where uncertainty is in effect epistemic. As noted above, however, quantum systems are inherently, ontologically uncertain across their properties. This includes uncertainty with regard to position and momentum and is represented specifically by the existence of superposition states $|\psi\rangle = \bigoplus_i a_i |i\rangle$ for amplitudes $a_i \in \mathbb{C}$ and basis states $|i\rangle$. When a quantum state $|\psi\rangle$ is measured, the measurement postulate provides that it collapses into a relevant eigenstate. The superposition of a quantum state is thus not directly observable in the way that we can directly observe its representation. It is represented as an artefact of measurement statistics. In practice what this means is that multiple - many - identical copies of the quantum system are prepared via state preparation procedures and measured. This jars somewhat with governance and law which is used to classical fundamental principles of persistence, continuity, identifiability and unity so that the object the subject of governance is ascertainable and definite. Understandably these classical assumptions permeate international (and even classical [**?**]) law (which is akin to a classical system), including the treatment of cyber objects and activities in the *Manual* below. The inherent ontological uncertainty of quantum systems does not, however, mean that quantum systems are somehow magical, unknowable, uncontrollable and so on. Rather, it is important to recognise the differences, such as the fact that there is not one single continuous quantum system that remains in superposition as it is measured over and over, but that governance must reckon with the essential multiplicity of quantum systems in practice.

2. Jurisdiction

The inherent ontological uncertainty of quantum states gives rise to in principle uncertainty in their position descriptions. Quantum state positions, such as the state of for example an electron, are described by reference to probabilities (measures) over a range of positions. For example the 'position' of an electron is described by a probability mass or density function such that repeated measurements allow that distribution to be estimate (subject to noise and so on). This is exemplified by simple but illuminating 'particle-in-a-box' paradigms [129] which show how the distribution of an electron's position is not classical, but actually extends vastly just with asymptotically zero probability of being found outside the box. In practice, while uncertainty in quantum properties is a central feature, this sort of uncertainty doesn't particularly impact jurisdictional issues such as the territorial location of a single or multi-qubit system. Almost all of its probability measure is concentrated within very narrow intervals such that in practice the tails of the distribution can be essentially ignored from a jurisdictional perspective. In the case of entanglement, the question is more subtle because the combination of the ontological status of superposition and entanglement give rise, at least by many arguments in quantum mechanics and quantum foundations, to the fact that the physical position of the say entangled is construed as non-local. However, as we note below, proxy concepts such as the locus of control provide a means to conform to ideas in the jurisprudence of State jurisdiction.

3. Control

Classical jurisprudence for technology governance and cyber security is premised upon classical notions of control. Implicit, for example, in discussion of State responsibility to control its own use of cyber technology, or those of actors within its jurisdiction, is an idea of controllability of the cyber system itself: that it can be directed to evolve, function and perform in a particular way. Obligations of due diligence or obligations to take precautionary measures when utilising cyber operations in armed conflict, for example, emphasise control to greater or lesser degrees. The law does countenance uncertainty and a lack of control over cyber systems - such as (discussed below) when a cyber attack otherwise lawful becomes unlawful because a failure to control it has led to unjustifiable collateral damage. There is also recognition that cyber systems are highly complex, such that it is often difficult to exert full control over them. Yet QIT is to a certain technical degree incongruous with these assumptions. Quantum state measurement outcomes are not controlled. At best the level of control over measurement statistics is managed via reliable engineering such that the measurement statistics may be predicted with sufficient confidence.

a. Control in an entanglement scenario is complicated

When two States share entangled resources, which can be said to control that entangled system? And what does it mean to control such a system? In practice States sharing such resources would share an enormous number of identically prepared and entangled quantum states. By sharing this means that each physical qubit (which in aggregate would constitute a set of logical qubits) is physically located within the jurisdiction of a State (or otherwise controlled by it) such that the State can control how it interacts with its qubit. By measuring (or some other equivalent interaction), the State causes its own qubit and that of the other State to collapse into the measurement state with a given probability. Each State cannot control per se the outcome of the quantum measurement (and thus cyber operations e.g. subsequent computations contingent upon them). Application of force in a conventional sense occurs by way of a State interacting with its own entangled qubits and this in essence causes, by virtue of entanglement, the measurement statistics of the other State to be correlated. Stochasticity aside, to the extent to which one State's measurements can be said to cause measurement statistics of the other State to be so correlated, then in effect the measuring State has exerted what the law would regard as some degree of control over the qubits of the other State.

4. Knowledge and Error Correction

Many State obligations relating to cyber activity are conditional to a greater or lesser degree on the knowledge of a State about that cyber activity. This includes customary laws regarding State due diligence, precautionary assessments by States about the impact of cyber operations and standards regarding reasonable foreseeableness of consequences. International law does countenance uncertainty in a State's knowledge or epistemic state. As noted in section II B (*Principles of Quantum Information*), quantum information is derived via measurement statistics which are used to tomographically reconstruct the quantum state or process (Hamiltonian). This is usually (given current technology) infeasible for anything other than small multi-qubit systems. So what is and even can be known of the quantum system is subject to a heightened-degree of practical uncertainty viz-a-viz classical systems along with the fundamental differences that quantum systems are not in definitive states. In general international law already has mechanisms for dealing with technological or consequential uncertainty, but it is a noteworthy distinction to make to the extent that technical specificity may be a requirement under various rules or customs. Moreover, all quantum information processing requires error correction due to the sensitivity of quantum substrates upon which QIT is engineered. The requirement for error correction means the types of control regimes applicable to them are distinct and made more complex. Error correction has important implications for the control of quantum systems because control regimes must account for the layering and encoding of, for example, error correction codes. They must also be directed in such a way that they do not undermine or interfere with the requirement for fault-tolerant error correction [115, 116, 65]. Error correction further limits the extent to which a quantum system may be diagnosed or surveilled.

5. Force

As we detail at some length below, the concept of force is central to the law of armed conflict and also cyber activities by States during peacetime. The *Manual* acknowledges that force for the purposes of cyber operations encompasses more than kinetic force, or even other physical catalysts, noting the central role that concepts of causality play in public international cyber law. Thus the application of force is framed usually in causal terms, where a cyber event has certain consequences. The application of force in a quantum setting is described by complex mathematical formalism and paradigms. Quantum paradigms of force differ in ways described by quantum causality [44, 53]. Mostly this is not going to be directly relevant for State activities using QIT. However, in the case of entanglement, it is worth noting how the application of 'force' occurs: one State interacts - measures - its own qubits and, owing the ontological entanglement those qubits with the qubits of another State, this is deemed to cause wavefunctional collapse in that other State's qubits.

Force is not, however, propagated through intermediate space in the usual way of say a wave propagating through the electromagnetic field. Nevertheless, the framing of force in terms of causality does provide a means by which the usual jurisprudence may apply, noting however that the stochastic nature of quantum outcomes means that a State may not necessarily control the measurement outcome, so the classical description of causality remains distinct. In this sense quantum causality is conditioned by way of a certain probability of an effect rather than a certainty of outcome.

One of the other challenges in the case of quantum information technology and jurisprudence is the fact that tests for causality in the law tend to be counterfactual in nature. This means that the law seeks to examine what would likely have happened but for the intervention in question as a way of ascertaining its causal impact . However in the case of quantum mechanical systems, one can at best assert a different outcome with a certain or estimated probability. While uncertainty regarding counterfactual analysis is quite common in the law in the quantum case this uncertainty is irreducible . Even with all the information in the world, the type of counterfactual analysis that the law engages in is is problematised by the fact that quantum measurements are inherently random meaning their measurement outcomes are inherently uncertain .

VII. Overview of the Tallinn Manual

The *Manual* is divided into four Parts, each containing jurisprudential analysis and normative claims regarding the application of international law to cyberspace, computational and information technology in offensive and defensive contexts and communications protocols. Each Part is further decomposed into Sections comprising rules (conventional and customary) of public international law relevant to cyberspace activities and operations. The scope of the *Manual* is broad and has been subject to considerable scholarship since its publication [55, 49, 59, 133, 83]. Its focus is upon two fundamental principles of international laws of conflict. The first is that of *jus ad bellum*, the principle governing when and whether a State is permitted to use force. The second is the principle of *jus in bello* governing the use of force and the conduct of military operations by a State during conflict, including constraints designed to protect specific persons, objects, and activities. The *Manual* also sets out extensive analysis on the public international law governing cyber operations in during peacetime. Below we examine how the principles of international law set out in the *Manual* that are applicable to cyberspace carry over to *quantum cyberspace* which we define broadly as quantum information technologies canvassed above. In many cases, usual principles of cyberspace law are equally applicable and inherited in the case of quantum cyberspace scenarios by virtue of them being generically classifiable as cyber activities, cyber assets and so on. But in other cases, especially where the unusual prop-

erties of quantum mechanics are essential to the functioning, use or distribution of QIT, there are, we argue, specific differences (especially with regard to entanglement).

A. Applicability of Tallinn Manual information system definitions to QIT

1. Cyberspace and QIT

Before examining a number of key provisions of the *Manual* and the implications of QIT for the jurisprudential analysis therein, we consider threshold issues of the extent to which QIT fits within established definitions of information processing and the subject matter of the *Manual* at all. We consider relevant definitions in the Glossary which relate to QIT. The term *cyber* is defined to connote a relationship with information technology which clearly countenances QIT detailed in earlier sections. *Cyber infrastructure* (also synonymous with 'hardware') is defined as the communications, storage, and computing devices upon which information systems are built and operate. Cyber infrastructure would thus naturally encompass QIT infrastructure, both quantum-specific infrastructure and the classical infrastructure within which QIT is necessarily embedded. *Cyberspace* is defined to include the environment formed by physical and non-physical components to store, modify, and exchange data using computer networks. A *cyber activity* is defined as any activity that involves the use of cyber infrastructure or employs cyber means to affect the operation of such infrastructure. Such activities include, but are not limited to, cyber operations. This latter term, *cyber operations* is defined to include the employment of cyber capabilities to achieve objectives in or through cyberspace. It is used in a predominantly operational context. Other relevant terms include *cyber reconnaissance*, including the use of cyber capabilities to obtain information about activities, information resources, or system capabilities. Clearly each of these terms covers within its meaning quantum information technology equivalence.

Cyber system is defined in terms of *computer system*. The definition of 'computer' itself is not included but would assume its ordinary meaning. *Computer system* is defined to include one or more interconnected computers with associated software and peripheral devices, including sensors and/or (programmable logic) controllers, connected over a computer network. Computer systems can be general purpose (e.g. a laptop) or specialised (e.g. the 'blue force tracking system'). Computer system thus includes single QIT devices, including quantum sensing and each node of a quantum. Although the foregoing definition incorporates connected (and thus distributed) computation in the classical distributed networks sense, the *Manual* also contains a definition of *computer network*, being a form of infrastructure of interconnected devices or nodes that enables the exchange of data. The data exchange medium may be wired (e.g., Ethernet over twisted pair, fibre-optic, etc.), wireless (e.g., Wi-Fi, Bluetooth), or a combination of the two. Computer networks would thus include networked quantum computers and, arguably, quantum communication net-

work devices e.g. relying upon entanglement as a wireless technology. Similarly the definition of *internet*, being a global system of interconnected computer networks that use the Internet Protocol suite and a clearly defined routing policy, would cover in the main proposals for quantum internets and distributed quantum networks in general (albeit with some subtle, but immaterial, differences regarding what constitutes, for example, routing on a quantum network).

2. Quantum data terms

Other key definitions would also be likely to encompass QIT and quantum analogues of classical information processing concepts. For example, *data* is defined to mean the basic element that can be processed or produced by a computer to convey information with the fundamental digital data measurement identified as a byte. Although the qubits are usually distinguished from bits, qubits (and by extension quantum bytes) can be seen as a classical form of information subject to a quantum ontology: qubits, for example, remain representable (and usually are represented) in terms of bits assuming values of 0 or 1 (e.g. $|\psi\rangle = a|0\rangle + b|1\rangle$) albeit in probabilistic fashion. Quantum data infrastructure (such as quantum memory and even simply the encoded data within a quantum system) would similarly fall within the concept of *data centres*, being defined as a physical facility used for the storage and processing of large volumes of data. A *database* is defined to include a collection of interrelated data stored together in one or more computerised files which would include storage of quantum data. The slight wrinkle here from a quantum perspective relate to superposition states and entanglement. Where data is in a superposition state, the concept of being stored together or stored is technically somewhat distinct from a quantum information perspective. Recalling, unlike classical computers, most quantum computing is premised upon the ability to initialise identical states, measure a sufficiently large number of them to enable measurement statistics to be obtained (the whole process being denoted an experiment in some contexts). Thus a state initialised in superposition contains probabilistic data and each experiment, once measured, collapses the relevant superposition (we use a simplistic non-multistate example here). One cannot simply access the data stored, that is, encoded, in a quantum system (such as a qubit) directly in the way that is possible with classical data, where measurement of the system does not interfere with it. Thus data in the quantum sense more closely refers to an abstraction which is effectively reconstructed via repeated experiments and interactions, rather than being identical to classical conceptions of storage.

Similarly, where data is encoded within entangled quantum systems (which by construction must be in a superposition state) that are distributed across the physical jurisdictional bounds of States (see below), the data within a quantum system controlled by a State can be affected by the measurement actions of another State on the entangled sys-

tem. Thus again the classical conception of data has slightly different features to that of quantum data because as soon as one State measures the system, the data encoded within it changes due to the ontological collapse of superposition (and any decohering interactions). However, in practice identical preparation and measurement requirements could and would likely just be seen as a procedural element such that superposition state and entangled state quantum systems would meet definitions of data and other related terms, thus falling within classical definitions for the purpose of the *Manual*. The definition of data includes the use of data centres in distributed networks, stipulating that a data centre can be used solely by users belonging to a single enterprise or shared among multiple enterprises, as in 'cloud computing' (see above) data centres. A data centre can be stationary or mobile (e.g., housed in a cargo container transported via ship, truck, or aircraft). Once again, each of these definitions categorically encompasses QIT equivalents.

3. Cyberspace definitions

There are a host of other technical terms defined in the *Manual* which the quantum analogues of which would likely fall within without much controversy. One particularly relevant definition given the offensive and defensive motivations for QIT use is that of *electronic warfare* being the use of electromagnetic (EM) or directed energy to exploit the electromagnetic spectrum. Electronic warfare covers the interception or identification of EM emissions (relevant to store-now decrypt-later quantum offensive strategies) and broadly put the employment of EM energy, prevention of hostile use of the EM spectrum by an adversary, and actions to ensure efficient employment of that spectrum by the user-State. As discussed above, the use of QIT is not equivalent in action to that of classical information systems. Although all QIT systems rely upon the electromagnetic spectrum in some form or another, the 'action' of a quantum system is not, for example, a causal electromagnetic wave propagated locally through electro-magnetic fields in the same way that say an electromagnetic pulse or even simple communication or signalling is in a classical context. So the intended meaning of electronic warfare under this definition differs in a material sense. The use of QIT for offensive actions is still captured by other definitions, such as cyber activities, but quantum systems do not act in the same way as classical ones. For example, even in the case of State adversaries sharing entangled resources, the classical notion of one State acting on another by way of measuring an entangled set of qubits is not one of local (classical) action. Rather it is sometimes described as 'spooky' action at a distance.

The terms *cyber attack* and *cyber espionage* are defined by way of reference to Rules 92 and 32 respectively. Rule 92 defines a cyber attack as a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects. As the *Manual* notes, non-violent operations, such as psychological cyber operations and cyber espionage, do not qualify as attacks under the

definition (which draws upon Article 49(1) of Additional Protocol I in its consequentialist requirement for the application of force or violence or other forms of causal interaction with similar effect). As with other jurisprudential conceptions of causality, proximity and effective causality is an issue when it comes to indirect actions that can be said to cause effects such as harm. For convenience, Table 9 in Appendix A sets out a comparison of how these important definitions apply to QIP and classical information.

4. Ontological cyberspace stack

The *Manual* adopts a stacked or layer-wise hierarchical framing of cyberspace, defining it in terms of three layers (Rule 1.4, p12): (i) the *physical layer*, comprising the physical network components (hardware), (ii) the *logical layer*, corresponding of the connections that exist between network components, comprising higher-level abstractions such as applications, data and protocols for exchange of data across the physical layer and (iii) the *social layer*, comprising the stakeholders (individuals and groups) engaged in cyberactivities. This hierarchy is important because certain rights, duties and obligations arising under the jurisprudential analysis of the *Manual* are cast in terms of distinct layers. Thus (as we note in more detail below) foundational principles of State sovereignty are construed according to all three layers of cyberspace. And further, as we analyse below, this has implications for the application of such principles. Thus while all QIT is physically embedded and relatively locally, the logical space exhibits different properties. Thus for example, the application of principles of jurisdiction, sovereignty and control to entangled qubits arguably minimally must reckon with their non-locality in position space because, for example, the probability measure over such physical space that specifies the location of say an electron used as a qubit is almost entirely concentrated in what the law would regard as the physical site of the qubit. Yet when that physical qubit is entangled and/or forms part of a logical qubit via entanglement across jurisdictions, the logical layer of the logical qubit (and entangled system as a whole) is less easily specified in terms of simple geometric coordinates.

B. General International Law and Cyberspace

Part I *General International Law and Cyberspace* of the *Manual* sets out foundational principles of international law applicable cyberspace, noting that public international law already applies to States with respect to cyberspace activities. This principle that the law as it is, *lex lata*, already applies to cyberspace carries over to QIT in most respects. We examine the specifics of existing international law cyber principles, tracking the structure of the *Manual* and canvassing how and whether the application of the same to QIT-based cyber classifications varies in any material way.

1. Sovereignty

a. Sovereign jurisdiction

Section 1 (*Sovereignty*) covers the canonical application of principles of State sovereignty (Rule 1), stipulating how this principle grants States exclusive authority over their cyber infrastructure. Despite abstractions of cyberspace as virtual, the situatedness and jurisdictional locality of cyberspace, that it is constituted by objects and involves activities conducted by persons and entities over which State sovereignty and jurisdiction applies (with no State sovereign over global cyberspace due to its partial location within other States). Cyberspace activities internally within a State's territory (Rule 2) are deemed subject to State sovereignty straightforward applications of sovereignty. This principle applies to both public (State) and private cyber assets for example, the determinative fact being whether a State may exercise sovereignty over the same rather than domestic configurations of ownership. Such internal sovereignty is related to a State's *domaine réservé* (Rule 66), those areas of activity that are considered to fall exclusively within the domestic jurisdiction of a sovereign state, meaning they are not subject to interference or regulation by international law or external entities (where unlawful intervention is regarded as a breach of sovereignty). The physical layer of cyberspace is considered to be self-evidently subject to State sovereignty. The *Manual* suggests that sovereignty extends to a principle of control over aspects of the logical layer of cyberspace within a State's territory, giving the example of State legislation mandating interoperability protocols. This question of the relationship of *control* and sovereignty is something we examine below in the context of entanglement-based quantum communication networks shared among States where the actions of each State measuring its own entangled qubits has both a physical and logical effect on the quantum network and consequences for its use.

Rule 3 discusses the principle of *external sovereignty*, enabling conduct of cyber activities in international relations subject to constraints imposed by international law. The principle is considered to derive from the sovereign equality of States (as noted in, for example, article 2(1) of the UN Charter). That is, there is no supreme singular sovereignty of one State over another. States are thus free to enter into arrangements e.g. cyber treaties or issue *opinio juris* on customary law and practice relating to cyber operations.

In Scenario 1, the sovereignty of each State extends to its classical and cyber infrastructure within its jurisdiction, with both the classical and quantum cyber infrastructure of each State constituting an instrumental extension of its sovereignty. In Scenario 2, the sovereignty of each State over the entangled quantum system is more complex than in Scenario 1. The entangled quantum system exhibits non-local characteristics that do not directly fit into territorial or extra-territorial jurisdiction. Each State's sovereignty extends to control over the qubits physically located within its jurisdiction. However, this fact ren-

ders each State's exclusive control over its qubits is problematic (as noted above). The highly correlated nature of the entangled resource could possibly constitute a *de jure* and *de facto* object which is (to the extent of entanglement) subject to the joint sovereignty of each State.

b. Joint sovereignty

Although not addressed in the *Manual*, the international law principle of condominium (or coimperium) may provide a source according to which jointly shared sovereignty, such as over entangled resources, may be analysed. In international law, a condominium occurs when two or more States share and exercise governing authority over a particular territory without any single State enjoying exclusive sovereignty [122, 27, 105]. This concept has its roots in Roman and civil law traditions, where shared ownership and joint sovereignty were recognised legal constructs. Historically, such arrangements involved the joint exercise of sovereign powers, as seen in European border territories or colonial holdings, while more recent examples often reflect limited forms of administration or regulatory oversight rather than full sovereignty. In a condominium, the States involved must manage and control their joint authority through carefully negotiated treaties or agreements, which set out principles that preserve the sovereignty of the other, such as those of non-discrimination, the free movement of persons and goods, the limits on military deployments, and the mechanisms for decision-making and dispute resolution. These arrangements are guided by principles of international law but have largely been supplanted by modern institutional regimes such as treaties and international bilateral and multilateral organisations.

c. Violations of sovereignty

Rule 4 sets out the cyber equivalent principle that States are not permitted to conduct cyber operations that violate the sovereignty of another State, subject to exceptions recognised at international law (such as authorised by the UN Security Council) (see Rule 76) or pursuant to a State's right of self-defence. The obligation is owed only among States, not by States towards non-State actors. Thus while States have avenues to respond to non-State actor cyber attacks for example, the right to respond is not considered to subsist under the auspices of responses to violations of sovereignty (albeit a State may contravene their due diligence obligations by recklessly permitting such activity). The extension of the principle of sovereignty to private cyber infrastructure would similarly apply to QIT as a subset. Violations conducted against an adversary State within that adversary's own jurisdiction would constitute a violation of sovereignty regardless. The *Manual* notes that unlawful cyber operations against State cyber infrastructure may constitute violation of

State sovereignty (Rule 4) while setting out principles of sovereign immunity and inviolability (Rule 5).

Rule 4 sets out a number of criteria. The mere interception of a target State's signals from outside that State's territory does not violate State sovereignty because the cyber operation does not manifest within the target State's cyber infrastructure (subject to some qualifications regarding privacy). The three levels of violation include (i) physical damage, (ii) loss of functionality and (iii) infringement upon territorial integrity. Thus in Scenario 1, State A's interception of classical signals outside the territory of State B, and their decryption, would not constitute a violation of State B's sovereignty per se. Cyber espionage has no legal significance with respect to violations of sovereignty per se. In the Scenario 1 conflict case, State A's interference via disabling of State B's military surveillance network would constitute a loss of functionality amounting to a violation of sovereignty (but see below for whether unlawful or not). This may also constitute interference with the governmental functions of State B.

In Scenario 2, the complicating factor is the entangled nature of the shared quantum resources. Merely utilising entanglement resources is not of itself a form of damage per se is proscribed as even cooperative activities may do so. But in a technical sense it may constitute a loss of functionality because of as noted before quantum entanglement is a resource. Whether the opportunity cost would equate to a loss of functionality (such as where States had previously agreed otherwise) is an unclear issue, but it does speak to the somewhat unusual legal implications that arise from entangled shared resources. Nevertheless, the use of such entangled resources in a way that both constitutes espionage and undermines functionality may constitute a violation if something like purpose or intent is factored into the cyber operation.

2. Due diligence

Section 2 (*Due Diligence*) covers the general principle of due diligence, the obligation of States to exert due diligence in order to control activities (primarily of private actors) within their territory regarding objects over which it exercises sovereignty from harming other States (Rule 6) (the *Corfu Rule* [1]). The duty is not considered *lex lata* and even as a custom is not considered to be a positive obligation to prevent the use of cyber infrastructure (so not in the form of a guarantee to ensure this not occur, or even to take action such that it would be unlikely to occur), but rather is one addressed to not knowingly allowing such activities, something akin to a best endeavours obligation. The question of knowledge of a State is further dealt with below. The jurisprudence considers whether transit (intermediate) States through which adversarial cyber activities were conducted bear responsibility. Rule 7 sets out considerations regarding State burdens and duties for compliance with the due diligence principle. As noted therein, there is in general no strict liability obligation upon States to prevent cyber activities within their jurisdiction

that would contravene international law. However, to the extent the general duty applies, it is considered to extend naturally to cyber operations and activities within a State's borders, which would encompass QIT as a subset thereof. A State's responsibility to act or mitigate such activities is qualified by their degree of actual or constructive knowledge. Scenarios 1 and 2 above only involve State actors, thus we eschew consideration of them in this context. However, we consider a few jurisprudential issues arising in the context of QIT use:

1. *Knowledge*. Obligations of due diligence rely upon jurisprudential standards of knowledge of States. As noted above and as is often the case with classical cyber operations, it can be difficult to identify specific activities or cyber operations per se, or challenging to establish causality. Such operations are often identified via their effects rather than, for example, surveillance of information processing itself. Similar challenges apply in the QIT case where, for example, surveilling a quantum computer that may be used to decrypt another State's classically encrypted information cannot be undertaken directly by observing quantum processes unfolding (albeit there may be alternative means of identifying the intent to, for example, implement Shor's algorithm).

2. *Adverse consequences*. What constitutes "serious adverse consequences" for the purposes of Rule 2 is a matter of degree. Certainly in principle decryption strategies compromise another State's information security or significant espionage (such as, for example, cyber espionage enabling a weapon of mass destruction to be built) could arguably meet this threshold. To the extent that qualitatively such decryption would only be possible via using QIT (as part of a SNDL attack) would then, in principle, constitute the type of use of QIT that would form a causal factor in serious adverse consequences. However, the jurisprudential logic as encapsulated in the *Manual* on this first due diligence point is at a level of abstraction that the fact QIT was used for such purposes would not, arguably, materially change the legal analysis.

3. *Control and jurisdiction*. A somewhat more interesting, albeit remote edge case, is the second consideration in the principle of State obligations regarding due diligence, namely that States must exercise due diligence over its instrumental (government) cyber infrastructure that it *controls*. Returning to our ongoing scenario where two States share entangled resources, it is conceivable that the principle ought to extent to control decisions by one State when interacting with its own entangled qubits, for example, with direct impact on the other State (such as acting on the entangled system in a way that adversely impacts the other State's ability to use the quantum system in some way). Again this toy model seems remote, but as we have noted above, it is entirely conceivable that States may share resources in competitive and

even conflict scenarios. The jurisprudential distinction drawn between *jurisdiction* and *control* is germane. Although the discussion in respect of due diligence distinguishes between control exercised by a State versus non-State actors, the distinction is useful in the case of non-local quantum resources such as entangled QIT. It might be said, echoing our point above that the control of quantum resources is ultimately a local operation (even if it allows non-local action to occur), that when it comes to non-locality, control is 9/10ths of jurisdiction.

3. Jurisdiction

Section 3 (*Jurisdiction*) sets out general jurisprudential principles regarding the State exercising jurisdiction (derived from is sovereign status). *Jurisdiction* refers, jurisprudentially, to the competence of a State to regulate persons, objects and conducts under that State's municipal law, within international law limits, territorially (within its territory) or extra-territorially. Jurisdictional competence is parsed into three forms (Rule 8) (i) prescriptive (legislative); (ii) enforcement, covering State authority to enforce laws via executive and administrative action; and (iii) judicial (adjudicatory), having to do with the competence of a State's judicial bodies (courts) to regulate disputes over which they have jurisdiction. Rule 8 provides that subject to limitations, States may exercise territorial and extra territorial jurisdiction over cyber activities. In this latter case, the use of classical and quantum information infrastructure for extra-territorial cyber activities such as cyber attacks or cyber espionage will often - as it is currently - be targeted extra-territorially. It should be noted that extra-territorial enforcement jurisdiction is more limited that the prescriptive jurisdiction, i.e. States may pass laws within the bounds of their prescriptive jurisdiction (e.g. with respect to activities outside their territory), yet the enforcement of them is limited primarily to within the State's territory. Rule 9 specifies that territorial jurisdiction applies to cyber infrastructure, cyber activities and so on with such a territorial nexus. In particular Rule 9 (c) covers cyber activities having a substantial effect in a State's territory, while extra-territorial enforcement of jurisdiction is covered by Rules 10-12. As is the case with cyber activities, QIT-related activities (such as those integrated into classical cyber infrastructure) can in principle emanate from multiple States, across multiple States leading to contested jurisdiction over particular cyber activities.

In Scenario 2, multiple States sharing distributed quantum network infrastructure face novel and interesting jurisdictional challenges which we discuss above. In principle a State could legislate how quantum resources are to be used by virtue of its jurisdictional prerogatives. If State B were to utilise those entangle resources in a way consistent with State B's jurisdictional remit, then in dilemmas would obviously arise. The key point is again one of joint jurisdiction of correlated non-local resources distinct from the classical case.

4. Law of international responsibility

Section 4 (*Law of international responsibility*) details primarily customary international law set out in the International Law Commission's Articles on State Responsibility [2] on State responsibility. State responsibility law sets out the legal criteria for attributing a cyber operation to a State (the *responsible State*) and the circumstances in which that act constitutes the use of force by the responsible State against another State (the *injured State*). It covers rules of evidence and how responsibility is attributed. As with classical cyber attacks, a State the recipient of cyber activities may have little time within which to respond under (*ex ante*) uncertainty.

In such cases States are under a duty to act and respond reasonably. Factors going to reasonableness include the nature scope and extent of a response, the reliability of information and the severity of the action. More severe responses generally impose a greater evidentiary burden. This can be problematic in the case of QIT: does decryption of military secrets, which may tip the balance in a conflict, constitute a highly severe use of QIT that would occasion more immediate reaction? And how would a State know? Moreover what counts as evidence subject of any disclosure obligation is problematic in the case of QIT e.g. is it measurement statistics, or algorithm specifications etc? Rule 14 sets out that States bear responsibility for cyber activities attributable to them which constitute a breach of international legal obligations. The principle of responsibility is well established such that responsibility of a State is for *internationally wrongful acts* (including violation of its international law obligations). Those obligations differ in peacetime and during conflict and are not limited to adversarial rules, they can include a raft of other governing instruments. The definition is not sourced in international law itself and involves an intent to cause harm. The internationally wrongful character of a cyber attack does not depend upon its geographic source per se. Our scenarios above assume State responsibility for the use of QIT, but it may be that attribution of responsibility is unclear when shared or dual-use QIT resources are being used.

5. Cyber operations not regulated *per se*

Section 5 (*Cyber operations not regulated per se by international law*) covers cyber activities by States which, while not the subject of specific regulation or *lex specialis*, may be subject to international law indirectly. The example given in Rule 32 (*Peacetime cyber espionage*) is of cyber attacks and espionage conducted outside State armed conflict. *Cyber espionage* is defined by the *Manual* to mean "any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather, or attempt to gather, information" (Rule 32) and may include cyber activities of surveillance, monitoring, capture, exfiltration of data or other information. Cyber espionage can be directed at all three layers of the cyberspace stack (physical, logical and social). Physically this may include embedding

code during a manufacturing process which can be later activated or utilised. Logically this may include quantum algorithmic malware for example.

The view espoused in the *Manual* is that customary international law does not per se proscribe espionage due to the lack of State practice and *opinio juris*, but it may be conducted in a way or have effects that are unlawful under international law, such as where it constituted some other class of proscribed activity such as an unlawful cyber attack. In Scenario 1, the utilisation of a quantum sensor network for espionage and eavesdropping can give rise to questions about the lawfulness of such activities. Thus while cyber espionage is not itself proscribed by law, the purposive or causal-style analysis preferred in the literature would provide that if the effects of such activities prejudiced another State's rights, e.g. putting them at military risk, then such activities may fall foul of other provisions.

C. Use of QIT during peacetime

Consistent with our partitioning of State activity between peacetime and conflict situations framed by cooperative or adversarial behaviour, we consider specific consequences of QIT during peacetime. Part III (*International peace and security and cyber activities*) of the *Manual* covers the adversarial use of cyber technology during peacetime, focusing on a gradation of cyber activities which, while adversarial, fall short of the threshold for conflict scenarios. Rules 65 to 80 cover a variety of jurisprudential principles applicable to our scenarios above. We focus on a few of them related primarily to cyber espionage and, in particular, our second scenario and entangled resources. As with other parts of the *Manual*, the jurisprudential discussion concentrates upon generally applicable laws and principles.

1. Prohibition of intervention

Sub-Part 13 (*Peaceful settlement*) deals with cyber activities during peacetime. Rule 65 covers the principles that States ought to engage in realistic attempts to settle their disputes involving cyber activities peacefully so as to not endanger peace and international security. Rule 66 of the *Manual* covers the principle of non-intervention (derived from the fundamental principle of sovereignty) that a State may not intervene, including using cyber activities, in the internal or external affairs of another State. The rule is considered a customary law of international law, often set out in State dicta and *opinio juris* [1]. Internal affairs are related to the *domaine réservé* of a State, this includes political, economic and social configurations of a state [3]. Coercion through cyber activities is not sufficient on its own to constitute a breach of the prohibition of intervention: the rule is purposive, that is, the coercion must be directed to target State's rights, duties or obligations (including its positions or actions), albeit there is debate as to whether depriving a state of control or

resources may constitute a form of intervention. Cyber espionage is not considered using force because of the lack of a coercive element (Rule 32). Scenarios 1 and 2 above bears upon the question of intervention, in the former case, hacking into an adversary's critical cyber infrastructure; in the latter, the intervening act arises because of the entangled nature of the shared quantum resource among States in those scenarios.

In Scenario 2, because the measurement by one state (or other such interaction) of its own qubits has a physical (and logical) effect on the qubits of the other States, then those acts by the first State would reasonably be considered causally influencing the State in question. Using computational stateful paradigms, the state of the qubits is changed causally and thus the question would be whether such change of state constitutes breaches the prohibition. This causal influence on its face may satisfy a breach of the prohibition. Clearly there is a need to distinguish between cooperative and competitive (adversarial) behaviour in peacetime scenarios. Cooperative behaviour by extension is that consented to by each State in question by virtue of its sovereign rights, which would and could encompass another State's use of entangled resources in a way that affects the first-mentioned State. In competitive scenarios, the situation is somewhat more complex. There is a jurisprudential question about the extent to which a State can be said to have consented to changes in the states of its entangled resources where such state changes lead to a competitive disadvantage.

2. The use of force and QIT

Part 14 (*The use of force*) of the *Manual* covers international law and jurisprudence regarding the use of force, focusing on the general prohibition on the use of force and exceptions such as Security Council authorised force (see Rule 76 below) and customary laws of State self-defence (Article 51 of the UN Charter, see Rule 71 below). The circumstances in which the use of force is constituted by cyber activities and, if so, is justified (*jus ad bellum*) remains an evolving area of international jurisprudence. Rule 68 encapsulates the prohibition in a cyberspace context, asserting that a cyber operation which constitutes a threat or use of force against the territorial integrity or political independence of any State (or is otherwise inconsistent with the purposes of the United Nations) is unlawful under international law. The principle derives from both customary international law (such as Article 2(4) of the UN Charter [4]). The thresholds that must be met by QIT are that (i) it is causally connected to the use of force, (ii) that it is a threat or use of force and that (iii) as a threat of use of force it undermines the territorial integrity or political independence (we leave questions of inconsistency with the purposes of the UN to one side). The application of the principle is purposive, not instrumental. It is not the use of cyber infrastructure, by one State, or even that it is the cyber infrastructure of another State which is *per se* affected, but rather the effects of such cyber activity. As to whether a cyber activity is attributable to a State, see the discussion on attribution earlier.

In the case of the use of QIT, there are a number of questions including as to the nature of the use and whether that may constitute the application of force which we discuss above. The use of QIT as an informational measure is addressed by considering its causal implications rather than any kinetic or physical application of force. This is somewhat complicated, as we note above, in the case of entangled resources because the use by a State of entangled resources may constitute in effect the application of force upon the entangled resources of another State. Thus in Scenario 2, in principle either State could interact with their own qubits in a way to affect the qubits of the other, thus constituting a physical (rather than simply indirect causal) connection between State action and effect. But as we note above whether this interaction would have led to a different outcome is precisely what makes quantum systems different: the same act by the same State on the same entangled qubit or qubit itself can give rise to different outcomes, such that any sense of determinism between a State's actions and the outcomes is different to the classical case.

3. Prohibition on the use of force

Rule 69 (*Prohibition of threat or use of force*) sets out a definition of when cyber operations constitute a use of force, namely when its *scale* and *effects* are comparable to non-cyber operations rising to the level of a use of force. The principle is drawn from jurisprudence, especially the *Nicaragua* judgment of the ICJ [3]. The threshold of the use of force is considered lower than that of "armed attack", the latter being a necessary condition to lawfully response in self defence. The use of force with more serious consequences is considered a use that is "most grave" [3]. There is debate on this point with the United States arguing any unlawful use of force constitutes an armed attack. The *Manual* sets out a taxonomy for considering whether a cyber operation constitutes a use of force:

1. *Severity*. Severity of the cyber operation indicated by scope, duration and the intensity of consequences is the most significant factor, the more severe, the more likely it meets the use of force threshold. Thus physical harm or damage would constitute the use of force (such as hacking into an information infrastructure in order to cause physical harm).

2. *Immediacy*. The immediacy of the cyber operation is a second factor to consider. The more immediate, rapid, cyber operations affording less chance to respond peacefully also contribute. The more immediate, the more the operation may constitute the use of force.

3. *Directness (proximate cause)*. A closer causal proximity between the initial cyber operation and its effects is also important. The closer in temporal proximity, the more the operation may have the character of the use of force.

4. *Invasiveness*. The degree to which the cyber operation intrudes into another State's information infrastructure, with penetration of more critical infrastructure more likely to contribute to meeting the use of force threshold.

In general, as is usually the case in law, the more ascertainable the effects of a cyber operation are, the greater the evidence that can be adduced to justify the designation of a cyber operation as a use of force. Other factors include: (i) whether the operation has a *military character* (such as caused by military institutions of a State, or targeting those of another); and (ii) *State involvement*, whether States and their governmental instrumentalities execute the cyber operation, or whether other actors are involved. The *threat* of force (Rule 70) is similarly defined in terms of the threat of a cyber operation constituting an unlawful use of force.

The use of QIT could in principle meet the type of cyber operation (albeit in concert with classical infrastructure) that met severity, immediacy, directness or invasiveness constraints. For example, in the event that quantum sensing technology could effectively decloak nuclear-armed submarines (noting the current unlikeliness of this occurring, see section V D (*Quantum Sensing*) above), then the severity of this cyber operation would be considerable, potentially altering geopolitical balances of power. Other informational impacts, such as decryption of a State's critical communications infrastructure during peacetime (or conflict) could similarly meet such thresholds (Scenario 1). In the case of Scenario 2, interference with entangled quantum resources may be immediate, direct and potentially invasive and severe depending on how reliant the target State may be upon such resources into the future.

D. Use of QIT during conflict

Once the use of force by way of a cyber operation constitutes an armed attack, two States can said to be in a conflict scenario. In this case, the classification of a cyber operation as an armed attack then triggers the availability of rights of self-defence against an armed attack under both Article 51 of the UN Charter and international customary law. Scenarios 1 and 2 above both envisage the use of QIT where conflict has arisen.

1. Self defence

Rule 71 (*Self-defence against armed attack*) both Article 51 and customary international law recognise the inherent right of individual and collective self-defence. Armed attacks must have trans-border characteristics (affecting the territorial or extra-territorial interests of a State). As noted in the *Manual*, the medium of attack is immaterial to whether the operation constitutes an armed attack [5], thus in principle causal use of QIT can constitute an armed attack under this rule. The exact threshold at which cyber operation would

constitute an armed attack is acknowledged as uncertain. An example discussed both in the literature and the *Manual* is the 2010 Stuxnet cyber operation [58] that caused damage to Iranian nuclear infrastructure (centrifuges). The Stuxnet attack was considered to constitute a use of force but views diverge on whether it satisfied an armed attack.

Moreover, there are also questions about whether a sequential and/or cumulative series of cyber operations may in aggregate constitute an armed attack, and whether less than physical damage may still notwithstanding constitute an armed attack for the purposes of international doctrine. Similar doctrines regarding reasonable foreseeability (and the recklessness or intentionality) of impacts also are considered in the *Manual* to be effects taken into account when assessing a cyber operation's classification as an armed attack or not (noting that intention is considered to not matter per se). Thus in Scenario 1, it may be plausible that the conflict use-case of QIT for decryption of strategic military information to afford a military advantage could be justified as a use of force in self-defence for example. In Scenario 2, the disruption of critical communications infrastructure in response to an imminent attack (see below) may also constitute lawful use of force by way of a quantum cyber operation.

2. Necessity and proportionality

The use of force as a means of self-defence must accord with criteria of necessity and proportionality (Rule 72), twin principles that have long been recognised [3, 5, 6]. *Necessity* requires that non-forceful responses be insufficient to respond to the armed attack, not that there be no other option, albeit the existence of alternatives (e.g. firewalls or reasonably implementable countermeasures) would be factors in considering the legitimacy of the use of force in self-defence. *Proportionality* concerns the degree of necessary force, acting as a limit upon the extent and severity of a State's response (but noting that it is not a requirement to respond in kind). It is unclear about the extent to which, for example, decryption en masse of an adversary State's communications by way of QIT use may be disproportionate, but in principle the extent and severity of the consequences of such widespread decryption could factor into the analysis as to the proportionality of QIT use.

3. Imminence, immediacy and anticipatory self-defence

Rule 73 (*Imminence and immediacy*) sets out that the right to use force in self-defence against a cyber armed attack arises if the attack is imminent and immediate. States need not wait idly by for attacks to eventuate before responding under the doctrine. Anticipatory self-defence is thus limited to cases where the attack is imminent. The concept of anticipatory self-defence refers to the use of force by a state to defend itself against an imminent armed attack that has not yet occurred but is about to happen. This concept is rooted in customary international law and is often associated with the *Caroline Case (1837)*,

which established criteria for lawful self-defense in situations where the necessity is instant, overwhelming, and leaving no choice of means, and no moment for deliberation [7]. The principle is sometimes expressed as the 'last feasible window of opportunity' meaning the last opportunity for a State to effectively defend itself, albeit distinctions between preparatory stages lacking the quality of imminence and the stage at which an adversary can be said to be capable of such an attack are germane to this issue. Moreover, strategic considerations, such as the need to act in an anticipatory fashion without signalling to an adversary about that action. The signalling of intention and taking of preparatory actions by an adversary is generally considered a necessary (but not sufficient) condition for anticipatory preventative strikes against an adversary State, the standard being something like whether the potential target State can reasonably conclude that the adversary has formed the intention and has the capability to so attack. Being unable to form this conclusion limits the target State to responses that do not include the use of force. The *Manual* also provides discussion for when collective self-defence is valid under international law. This would be particularly relevant in any case of quantum networks where one or more allied States seek to use the network against an adversary. This poses further interesting strategic and legal questions but we do not address this scenario directly here. One interesting question is the extent to which State B may have rights to anticipatory self-defence if it anticipates an imminent use of QIT that would have severe or catastrophic decryption effects. The extreme example of this is touched upon above where, for example, a State regards decryption that undermined its nuclear second-strike capabilities as severe enough to warrant the use of its own nuclear arsenal or other significant response.

E. QIT and Cyber Armed Conflict

Part IV (*The law of cyber armed conflict*) of the *Manual* sets out a detailed exposition of the application of the laws of armed conflict to cyber operations. Rule 80 notes that cyber operations fall within the subject matter of the law of armed conflict. The term "armed conflict" derives formally from the 1949 Geneva Conventions I-IV (Article 2) [8, 9, 10, 11] and is considered jurisprudentially synonymous with "war". The *Manual* defines armed conflict to refer to a situation of hostilities (in our case, among States) including those using cyber means, with different threshold criteria in the case of international (Rule 82) and non-international (Rule 83) conflict. Cyber operations can become governed by the law of armed conflict even if they do not in themselves constitute an armed attack. The extent of the nexus is contextual, but relates in general to cyber operations in furtherance of hostilities.

1. Geographical factors

As noted in the *Manual* (Rule 81), geographic considerations are relevant to characterisation of the lawfulness of cyber operations. Cyber operations during conflict may be conducted in and upon the territory of State belligerents (with distinctions between international and non-international conflicts). Rule 82 sets out that an *international* armed conflict exists whenever there exist hostilities among multiple States (which may include cyber operations) (Article 2 of the 1949 Geneva Conventions) with contingencies for when States act by proxies or non-State actors. We focus only on such conflicts (not non-international) for our purposes. As with other principles governing adversarial behaviour of States, there is debate about the threshold that must be met for an act by a State to constitute an international armed conflict, with some views that any armed conflict suffices, in contrast to other views that assert some greater de minimus level of conflict (such as with respect to intermittent border disputes, for example). This is particularly relevant to cyber operations which are often gradated in scope and where cyber espionage plays an important preparatory and gradated role towards any hostilities that do emerge. In both Scenario 1 and Scenario 2, in principle once hostilities have commenced then the types of actions envisaged for State A ought to meet geographic criteria.

2. Cyber attacks

Rule 92 sets out the definition of "cyber attack", being as noted above a cyber operation (offensive or defensive) that is reasonably expected to cause injury or death to persons or damage or destruction to objects. "Attack" is a jurisprudential term of art from which consequences flow such as regarding targeting (targeting civilians and civilian infrastructure is proscribed). The term connotes meanings of offensive or defensive violence against an adversary [12]. As noted in the *Manual*, acts of violence are not restricted to kinetic or vernacular definitions. Rather, the connotation is one of causality, hence the consequences caused by an action, such as a cyber operation, are the basis for classifying it as a cyber attack. In this regard, violence refers to the consequences of an action, not necessarily the action itself. The idea of consequential harm is manifest in concepts of loss, danger, injury and other terms in various international law sources. The concept of *causality* encompasses reasonably foreseeable consequences including damage, destruction, injury or death. Thus using cyber operations to effect massive destruction or harm in some way would likely qualify that use as a cyber attack.

From a computational perspective, cyber operations against data and other 'non-physical entities' or entities that are more abstractly defined can be subject to an attack. So too may cyber operation-based interference with the functionality of an object, being equated to damage to the functionality of an object. This may include corruption of software control systems in ways that occasion harm. Other views hold that simply the interference with

cyber infrastructure could constitute an attack rather than requiring further consequential harm. An important point of discussion in the *Manual* are cumulative effects on for example social functionality (such as mass email disruption), however this is viewed by some literature as too remote from the law of armed conflict itself. So too do cyber operations that are mere inconveniences, or even espionage, fail to meet the threshold of a cyber attack. Moreover, the consequentialist approach to classification of attacks also encompasses attempted, but unsuccessful, attacks or those cyber operations whose intent is to cause harm but which may not have been executed, such as the backdooring of malware or viruses. A similar analysis in the QIT case would apply as in the classical case in this respect. Whether, for example, interference with shared entangled resources in Scenario 2 was sufficient to constitute an attack would, as with the classical case, be a question of context.

3. Other armed conflict principles

Other armed conflict principles of relevance to considerations of QIT use include the two cardinal principles of customary international law of armed conflict recognised by the ICJ [5]. These are the principle of *distinction* (Rule 93), that the only legitimate object is the military forces of the enemy, and the *prohibition of unnecessary suffering* (Rule 104). These two rules essentially focus on minimising targeting of non-combatants (civilians etc) and seek to impose precautionary obligations on States to avoid their harm. These concepts are manifest in the distinction between civilian objects and military objectives. A military objective (as a jurisprudential term of art) is defined in Rule 100 to include those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage. While the question of whether data as a category constitutes a military objective *per se* is debated, given the centrality of data to modern State security and armed conflict operations, it is reasonable to assume that data can be a military objective (witness the importance of intelligence data throughout history) and one which would be the target of QIT-based uses of force as set out in Scenario 1 and Scenario 2.

The use of civilian objects for military purposes can render it a military objective. To this end, of particular interest to information technologies are *dual use* protocols discussed above. Rule 101 provides that cyber infrastructure used for dual civilian and military purposes is considered to be a military objective provided that its destruction offers military advantage. This draws upon the distinction (Rule 100) between civilian objects and military objects, drawing upon Article 52(1) of the Additional Protocol I [12]. Military objectives are thus those which make an effective contribution to military action such that attacking or harming them will provid a military advantage for the aggressor. This advantage must be definite [13]. Dual use considerations can give rise to precautionary

obligations upon States to ensure that (consistent with the principles of distinction and prohibition of unnecessary suffering) civilian harm or harm to civilian infrastructure is mitigated. As noted in the *Manual*, cyber activities present difficulties due to their dual use being often geographically or infrastructurally indistinguishable, such as in the case of networks used for dual civilian and military purposes. The extent to which attacks can be localised against distributed targets, such as internets, is thus important and is also relevant to considerations around proportional response. Rule 102 inheres a precautionary principle for careful deliberation before such dual use infrastructure is targeted. These considerations of dual use are important as QIT, along with other computational technologies, is likely to have a considerable dual use functionality. This is in part due to the considerable infrastructure required to support QIT: quantum computers are not envisaged as being as mobile as classical computational devices. They are in effect immobile in the main and would likely be utilised for a combination of State and civilian purposes given how challenging they are to construct.

4. Methods of warfare

The *Manual* sets out consideration of the means and methods of cyber warfare, noting the general laws regarding legality of weapons and methods will also apply in the cyber case. Rule 103 defines *means of cyber warfare* in terms of cyber weapons and their associated cyber systems. *Methods of warfare* is defined to include cyber tactics, techniques and procedures by which hostilities are conducted. Both are terms of art within international jurisprudence. The *Manual* defines cyber weapons in terms of cyber means that are used, designed or intended to cause damage or destruction, essentially the same criteria for rendering cyber operations a cyber attack (under Rule 92 - see above). The term includes both cyber weapons and weapon systems, the former being an aspect of a system used to cause damage, destruction or injury. Cyber means is broadly considered to include devices, materiel, instruments, mechanism or software for cyber attacks. The *Manual* distinguishes between computational systems which may be means of warfare, as distinct from cyber infrastructure (e.g. the internet) that is not considered to be a means of warfare, albeit due to a purported lack of control. In the case of a quantum internet, this may be different in that the internet in that case is limited and influenced by a limited number of States. Methods of warfare concerns strategies used, e.g. denial of service strategies rather than the instruments. Clearly the use of QIT would fall within these conceptual categories with similar rules applying. Thus in Scenario 2, State A ought to consider the effect of interfering with State B's quantum resources or quantum internet even if it only does so by interaction with its own entangled qubits.

The *Manual* also examines a range of applicable principles such as prohibitions on cyber warfare means or methods. These include: methods and means that cause superfluous injury or unnecessary suffering (Rule 104); prohibitions on indiscriminate use (Rule

105) including snowballing or viral-style effects that propagate and cyber booby traps, those cyber devices who may operate unexpectedly (and so be indiscriminate) (Rule 106). Rule 110 sets out consequential principles that mandate States using cyber means of warfare ensure they do so within the rules of law of armed conflict and that, additionally, where they are parties to Additional Protocol I, they undertake sufficient precautionary due diligence regarding the development, acquisition or adoption of new means to ensure compliance with said international obligations. In the case of QIT, this arguably would involve something along the lines of considering how the application of QIT in various contexts has differential impacts by comparison with classical information technologies. This in turn relates to concepts flagged earlier on in our discussion about the imperative for detailed technological governance architecture for emerging QIT systems. These types of due diligence-style obligations on States provide motivation for how and why technology-specific governance instruments are justified, even possibly required, from an international law perspective.

5. Conduct of cyber attacks

A number of rules in the *Manual* cover the actual execution and conduct of cyber attacks. Rule 111 reiterates that the conduct of attacks which is indiscriminate (e.g. striking targets that are not lawful targets, or fail to distinguish between civilian and non-civilian objects) are prohibited. This is drawn from Article 51(4)(a) to (c) of the Additional Protocol I and forms part of customary international law. The rule is distinguished from Rule 105 above in that it concerns cases where a system that may have the capacity for discriminate targeting in particular cases fails to meet such discriminatory criteria i.e. a discriminate means employed indiscriminately. Discriminability is thus considered a central tenet of the conduct of cyber warfare operations and in turn connects with obligations upon States to undertake reasonable precautionary analysis of the effects of their offensive cyber activities. Rule 112 covers the case where a cyber attack targeting cyber military objectives may in effect cause unlawful disproportionate impacts on protected classes of object (e.g. civilians or infrastructure). Thus even where a cyber attack itself on a dual use system may be proportionate it may fall foul of this requirement, though whether it does is clearly contextual depending on facts at the time.

Proportionality considerations relating to cyber attacks are considered in Rule 113, where a cyber attack is considered not meeting standards of proportionality (based upon the Additional Protocol I) in cases where damage to civilians, civilian objects or other protected classes is excessive in relation to the concrete and direct military advantage that may be afforded by doing so. The rule is a customary one of the international law of armed conflict. Its focus is on incidental harm and collateral damage which do not render a cyber attack unlawful per se, but does require a calculus between collateral harm and military advantage to be undertaken or demonstrated by an aggressor State. Similar

concepts as discussed above in terms of thresholds of cyber activities constituting armed attacks apply when determining whether a cyber operation may give rise to collateral harm sufficient to meet the proscription. Collateral harm is sometimes parsed into (i) immediate first-order effects and (ii) those which are delayed or intermediated by other events of actions. The *Manual* notes difficulties in assessing what constitutes excessive and what constitutes a sufficient military advantage, though notes a number of sources that discuss a preference for quantifiably concrete and direct impact in assessing military advantage. The principle inheres a precautionary element obliging States to act reasonably in conducting preliminary assessments of such trade-offs, as is required for conventional attacks (being an objective reasonableness test [14]).

However, certainty of outcome is not itself required especially given the difficulty of estimating collateral harm in advance. This touches to some degree on the inherent uncertainty of QIT use. Such precautionary principles are consistent with other principles espoused by the *Manual* of international law of conflict, such as the duty of State belligerents to take constant care during hostilities to avoid harming protected classes of object (Rule 114), requirements to verify targets as much as feasible to avoid harming protected classes of object (Rule 115) along with further rules obliging selection of means and methods of cyber attacks that respect similar principles and proportionality (Rule 117). Rule 118 sets out a rule where, in the event there exists an equivalence class of cyber attacks to obtain similar military advantage, States ought to select the cause of action (cyber attack) which minimises harm and danger to protected classes of objects. Rule 121 further reiterates such precautionary principles, requiring States to take necessary protective precautions to avoid harm or danger to protected classes from cyber attacks (drawing upon Article 58(c) of the Additional Protocol I and protection against the dangers of military operations). The advanced capabilities of QIT do not create exceptions to this rule. Belligerents, such as State A in our Scenarios above, must still conduct a proportionality assessment to determine whether the collateral damage is justifiable. The speed, stealth, or complexity of QIT-enhanced attacks do not exempt States from this balancing test.

6. Perfidy and deception

A number of rules deal with proscriptions against perfidy, where it is prohibited to kill or injure an adversary by resort to perfidy (Rule 122) e.g. harming surrendered or surrendering combatants after accepting their surrender. The underlying concept draws upon the notion of *treachery* set out in Article 37(1) of the Additional Protocol I. The rule of perfidy has four elements (i) inviting the confidence of an adversary, (ii) an intent to betray that confidence, (iii) a specific protection provided for in international law and (iv) death or injury of the adversary. The *Manual* considers different view as to whether the Rule may encompass cyber systems, such as where States agree to a computational monitoring system and one State defects, or deceptive authentication mechanisms are used by one

State. Perfidy is distinguished from cyber ruses, which are lawful and it does not apply to destruction of property. But it does relate (Rule 124) to the improper use of enemy indicators. While we do not focus on it in this paper, there are interesting game-theoretic considerations here that arise with respect to our Scenario 2 where States share entangled resources and can signal their decision to commit to certain strategies.

F. Comparison with Telecommunication Law

1. International Telecommunications Union

One final area of interest from the *Manual* we mention is that between quantum communication and international telecommunications law. Most States are party to international law instruments governing the regulation of international telecommunications, the primary example of which is the treaty regime set out in the International Telecommunications Union (a UN agency that regulates international telecommunication). As a subdivision of international law, international telecommunication law covers both the provision of telecommunication services and infrastructure and so plays a central role in classically facilitating cyber operations by States globally. The regime is relevant both as a point of comparison with quantum communication and quantum internet proposals and as a model for how, in the event a quantum internet or similar is established among States, such quantum network infrastructure may be regulated. It is also instructive to analyse the extent to which the ITU regime may already encompass QIT systems. The ITU has already commenced a series of standards' development initiatives relating to QKD protocols [15], covering functional requirements [16], functional architecture [17], key management [18] and control [19], with additional research in the post-quantum cryptography domain also canvassed [132].

2. Sources of law and obligations of States

The primary sources of jurisprudential principle are set out in the ITU Constitution [20] and a series of International Telecommunication Regulations [21, 22]. *Telecommunication* is defined as any transmission, emission or reception of signs, signals, writing, images, and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems. The definition is regarded as technology neutral, thus can reasonably be considered to encompass quantum communication and non-classical methods of communicating within its scope. *International communications* as per the *Manual* concerns the transmission of data across State borders and through extra-territorial regions while an *international telecommunication service* is the provision of telecommunication capability among States. The ITU Constitution sets out a number of principles, including the presumption as to the secrecy of communication of international correspondence (Article 37(1)). Rule 61 of the *Manual*, based on Article 38 of the ITU Constitution, sets out the principle that

States must take measures to safeguard the establishment of international telecommunication infrastructure required for rapid and uninterrupted telecommunications. This includes maintaining any cyber infrastructure of a State established for this purpose. States are considered under an obligation of conduct equivalent to a 'best efforts' obligation, thus subject to reasonableness and feasibility. This includes a duty to maintain operational safeguards and ensure data can be reliably and efficiently transmitted.

3. Sovereignty and telecommunication

The paramount nature of State sovereignty is recognised in the ITU constitution (Articles 35 and 34(2)). States retain a sovereign prerogative to suspend international cyber communication within their territory (and must give notice to other States of this) and may also stop transmission of private cyber communications contrary to municipal law (Rule 2). The ITU Constitution and Rule 63 set out principles whereby States ought not interfere with protected electromagnetic (radio) frequencies. State obligations are modified during armed conflict (a form of *lex specialis*) where for example jamming or other interference may be considered lawful in certain circumstances. Under Rule 64, States retain complete freedom regarding their military radio installations. While specific to the electromagnetic spectrum, the rules provide a basis for the development of jurisprudence for quantum communications.

VIII. Conclusion

Quantum information technology is continuing to emerge as both a strategic asset for States and a technology that raises its own governance questions. The unique affordances of QIT, from entanglement - based communication channels to quantum-enhanced cryptanalysis — both sit within existing legal frameworks for the governance of classical information systems, but also give rise to potentially distinct jurisprudential questions regarding jurisdiction, sovereignty and the application of force in certain strategic contexts owing to the role of superposition and entanglement. As we have noted throughout, the promise of QIT, if realised, presents States with compelling opportunities for advantage in peacetime and conflict scenarios. The ability to potentially decrypt classically encrypted sensitive information, together with other opportunities arising from quantum sensing and quantum communication, demonstrates how States may in principle leverage QIT for economic gain, strategic advantage, or enhanced security.

QIT remains at the developmental and experimental stage across most of its sectors, with extensive challenges to overcome primarily related to fault-tolerant scaling of the technology. Thus there is little motivation to seek to implement any new or adapted international legal instruments regarding international QIT governance per se. However, QIT

is already subject to a raft of dual-use laws across States globally which already are having an impact on how the technology is developed and distributed. This speaks to both the strategic importance of QIT, but also one way in which international law instruments could be relevant at this early stage to the development of QIT. Further research may consider how such instruments may be used to deal with dilemmas that dual use controls place upon QIT development, including considering options for multilateral treaties that set forth common standards for QIT export controls, prohibit certain quantum-enhanced offensive cyber operations, or mandate transparency in quantum sensing capabilities. Regional or global regulatory bodies might supervise the deployment of entangled quantum networks akin to how international telecommunications networks have been deployed. These instruments could incorporate verification regimes tailored to the special characteristics of QIT, such as standard protocols for monitoring quantum key distribution networks or auditing quantum computation facilities.

Such instruments could contribute to the development of existing international cyber law, bridging the gap between traditional principles and the novel capabilities that QIT presents. In principle, over time a *lex specialis* for QIT could emerge, integrated with broader arms control, non-proliferation, and technology governance efforts. By proactively forging these instruments and institutions, States may be able to address strategic issues that enable the development of QIT technology and its potential gains, while mitigating its potential as a source of destabilisation and conflict.

REFERENCES

[1] *Corfu Channel Case (United Kingdom v. Albania)*, (1949) ICJ Rep 244.

[2] *International Law Commission, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with Commentaries*, Report to the General Assembly, 53 UN GAOR Supp. (No. 10), at 370–436, UN Doc. A/56/10 (2001).

[3] *Military and Paramilitary Activities in and against Nicaragua (Nicar. v. US)*, 1986 ICJ 14 (27 June).

[4] *Charter of the United Nations*, (23 May 1969, 1155 UNTS 331).

[5] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996 ICJ 226 (8 July).

[6] *Oil Platforms (Iran v. US)*, 2003 ICJ 161 (6 November).

[7] *Judgment of the International Military Tribunal Sitting at Nuremberg, Germany*, (30 September 1946), in 22 The Trial of German Major War Criminals: Proceedings of the International Military Tribunal Sitting at Nuremberg, Germany (1950).

[8] *Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, (12 August 1949, 75 UNTS 31).

[9] *Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea*, (12 August 1949, 75 UNTS 85).

[10] *Convention (III) Relative to the Treatment of Prisoners of War*, (12 August 1949, 75 UNTS 135).

[11] *Convention (IV) Relative to the Protection of Civilian Persons in Time of War*, (12 August 1949, 75 UNTS 287).

[12] *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts*, (8 June 1977, 1125 UNTS 3).

[13] volume (Yves Sandoz *et al.* eds., 1987).

[14] *Prosecutor v. Stanislav Galić*, Case No. IT-98-29-T, Trial Chamber judgment (Int'l Crim. Trib. for the Former Yugoslavia 5 December 2003).

[15] *Recommendation ITU-T Y.3800*, (2019)/Cor.1 (2020), Overview on networks supporting quantum key distribution.

[16] *Recommendation ITU-T Y.3801*, (2020), Functional requirements for quantum key distribution networks.

[17] *Recommendation ITU-T Y.3802*, (2020), Quantum key distribution networks - Functional architecture.

[18] *Recommendation ITU-T Y.3803*, (2020), Quantum key distribution networks – Key management.

[19] *Recommendation ITU-T Y.3804*, (2020), Quantum Key Distribution Networks - Control and Management.

[20] *Constitution of the International Telecommunication Union*, (22 December 1992, 1825 UNTS 331).

[21] *International Telecommunication Regulations*, (WATTC-88, Melbourne, 9 December 1988).

[22] *International Telecommunication Regulations*, (WCIT-2012, Dubai, 14 December 2012).

[23] S. Aaronson. *Quantum Computing Since Democritus*. Quantum Computing Since Democritus. Cambridge University Press, 2013.

[24] Gorjan Alagic, Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, et al. Status report on the third round of the nist post-quantum cryptography standardization process. 2022.

[25] Gorjan Alagic, Maxime Bros, Pierre Ciadoux, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, et al. Status report on the first round of the additional digital signature schemes for the nist post-quantum cryptography standardization process. 2024.

[26] R. Allenby. *Governance and Technology Systems: The Challenge of Emerging Technologies*. Springer Netherlands, 2011.

[27] Vincent P Bantz. International legal status of condominia, the. *Fla. J. Int'l L.*, 12:77, 1998.

[28] Stephen D. Bartlett, Terry Rudolph, and Robert W. Spekkens. Reference frames, superselection rules, and quantum information. *Reviews of Modern Physics*, 79(2):555–609, April 2007.

[29] Riccardo Bassoli, Holger Boche, Christian Deppe, Roberto Ferrara, Frank HP Fitzek, Gisbert Janssen, and Sajad Saeedinaeeni. *Quantum communication networks*, volume 23. Springer, 2021.

[30] Craig Bauer. *Secret history: The story of cryptology*. Chapman and Hall/CRC, 2021.

[31] Fathalla Belal, Mokhtar Mabrouk, Sherin Hammad, Hytham Ahmed, and Aya Barseem. Recent applications of quantum dots in pharmaceutical analysis. *Journal of Fluorescence*, 34(1):119–138, 2024.

[32] J.S. Bell. *Speakable and Unspeakable in Quantum Mechanics*. Cambridge University Press, Cambridge, 2nd edition, 2004.

[33] Yohsua Bengio, Daniel Privitera, Tamay Besiroglu, Rishi Bommasani, Stephen Casper, Yejin Choi, Danielle Goldfarb, Hoda Heidari, Leila Khalatbari, Shayne Longpre, Vasilios Mavroudis, Mantas Mazeika, Kwan Yee Ng, Chinasa T. Okolo, Deborah Raji, Theodora Skeadas, Florian Tramèr, and Soren Mindermann. *International scientific report on the safety of advanced AI*. May 2024.

[34] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[35] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical Review Letters*, 70(13):1895–1899, 1993.

[36] Daniel J Bernstein and Tanja Lange. Post-quantum cryptography. *Nature*, 549(7671):188–194, 2017.

[37] Jonathan L Black-Branch and Dieter Fleck. *Nuclear Non-Proliferation in International Law: Volume II-Verification and Compliance*, volume 2. Springer, 2015.

[38] Hans Blix. Verification of nuclear nonproliferation: The lesson of iraq. *Washington Quarterly*, 15(4):57–65, 1992.

[39] Joppe W Bos, Craig Costello, Michael Naehrig, and Douglas Stebila. Post-quantum key exchange for the tls protocol from the ring learning with errors problem. In *2015 IEEE symposium on security and privacy*, pages 553–570. IEEE, 2015.

[40] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu. Experimental realization of teleporting an unknown pure quantum state via dual classical and einstein-podolsky-rosen channels. *Physical Review Letters*, 80(6):1121–1125, 1998.

[41] John Bostanci and John Watrous. Quantum game theory and the complexity of approximating quantum nash equilibria. *Quantum*, 6:882, 2022.

[42] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger. Experimental quantum teleportation. *Nature*, 390:575–579, 1997.

[43] Anthony J. Brady, Christina Gao, Roni Harnik, Zhen Liu, Zheshen Zhang, and Quntao Zhuang. Entangled sensor-networks for dark-matter searches. *PRX Quantum*, 3(3):030333, September 2022.

[44] Časlav Brukner. Quantum causality. *Nature Physics*, 10(4):259–263, 2014.

[45] Tracie J Bukowski and Joseph H Simmons. Quantum dot research: current state and future prospects. *Critical Reviews in Solid State and Material Sciences*, 27(3-4):119–142, 2002.

[46] Angela Sara Cacciapuoti, Marcello Caleffi, and Giuseppe Bianchi. When entanglement meets classical communications: Quantum teleportation for the quantum internet. *IEEE Transactions on Communications*, 67(5):3426–3439, 2019.

[47] Marcello Caleffi, Angela Sara Cacciapuoti, and Giuseppe Bianchi. Quantum switch for the quantum internet: Noiseless network switching. *IEEE Journal on Selected Areas in Communications*, 36(3):292–303, 2018.

[48] Gianfranco Cariolaro. *Quantum communications*, volume 2. Springer, 2015.

[49] Jeffrey S Caso. The rules of engagement for cyber-warfare and the tallinn manual: A case study. In *The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent*, pages 252–257. IEEE, 2014.

[50] Lily Chen, Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray A Perlner, and Daniel Smith-Tone. *Report on post-quantum cryptography*, volume 12. US Department of Commerce, National Institute of Standards and Technology . . . , 2016.

[51] Giulio Chiribella, G Mauro D'Ariano, and Paolo Perinotti. Quantum circuit architecture. *Physical review letters*, 101(6):060401, 2008.

[52] C.L. Degen, F. Reinhard, and P. Cappellaro. Quantum sensing. *Reviews of Modern Physics*, 89(3):035002, July 2017.

[53] John F Donoghue and Gabriel Menezes. Quantum causality and the arrows of time and thermodynamics. *Progress in Particle and Nuclear Physics*, 115:103812, 2020.

[54] D. D'Alessandro. *Introduction to Quantum Control and Dynamics*. Chapman Hall/CRC Applied Mathematics Nonlinear Science. Taylor Francis, 2007.

[55] Dan Efrony and Yuval Shany. A rule book on the shelf? tallinn manual 2.0 on cyberoperations and subsequent state practice. *American Journal of International Law*, 112(4):583–657, 2018.

[56] Jens Eisert, Martin Wilkens, and Maciej Lewenstein. Quantum games and quantum strategies. *Physical Review Letters*, 83(15):3077, 1999.

[57] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[58] James P Farwell and Rafal Rohozinski. Stuxnet and the future of cyber war. *Survival*, 53(1):23–40, 2011.

[59] Dieter Fleck. Searching for international rules applicable to cyber warfare—a critical first assessment of the new tallinn manual. *Journal of Conflict and Security Law*, 18(2):331–351, 2013.

[60] Marchant G, W. Wallach, Kenneth W.Abbott Marchant, and Braden Allenby. *Governing the Governance of Emerging Technologies*. Edward Elgar Publishing, 2013.

[61] Yan Ge, Wu Wenjie, Chen Yuheng, Pan Kaisen, Lu Xudong, Zhou Zixiang, Wang Yuhan, Wang Ruocheng, and Yan Junchi. Quantum circuit synthesis and compilation optimization: Overview and prospects. *arXiv preprint arXiv:2407.00736*, 2024.

[62] I. M. Georgescu, S. Ashhab, and Franco Nori. Quantum simulation. *Reviews of Modern Physics*, 86:153–185, 2014.

[63] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Advances in quantum metrology. *Nature Photonics*, 5(4):222–229, April 2011.

[64] Nicolas Gisin and Rob Thew. Quantum communication. *Nature photonics*, 1(3):165–171, 2007.

[65] Daniel Gottesman. Theory of fault-tolerant quantum computation. *Physical Review A*, 57(1):127–137, January 1998.

[66] Daniel Gottesman. An introduction to quantum error correction and fault-tolerant quantum computation. In *Quantum information science and its contributions to mathematics, Proceedings of Symposia in Applied Mathematics*, volume 68, page 13–58, 2010.

[67] Daniel Greenbaum. Introduction to quantum gate set tomography. *https://arxiv.org/abs/1509.02921v1*, September 2015.

[68] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing*, STOC '96, page 212–219, New York, NY, USA, July 1996. Association for Computing Machinery.

[69] Hong Guo, Juheng Zhang, and Gary J Koehler. A survey of quantum games. *Decision Support Systems*, 46(1):318–332, 2008.

[70] Yukai Guo and Xing Gao. Quantum simulation of open quantum dynamics via non-markovian quantum state diffusion. *arXiv preprint arXiv:2404.10655*, 2024.

[71] Gus Gutoski and John Watrous. Toward a general theory of quantum games. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 565–574, 2007.

[72] Nicholas Harrigan and Robert W. Spekkens. Einstein, incompleteness, and the epistemic view of quantum states. *Foundations of Physics*, 40(2):125–157, February 2010.

[73] Elisa D Harris, Robert Rosner, James M Acton, and Herbert Lin. Governance of dual-use technologies: Theory and practice. American Academy of Arts and Sciences, 2016.

[74] Chris Jay Hoofnagle and Simson L Garfinkel. *Law and policy for the quantum age*. Cambridge University Press, 2022.

[75] Kazuki Ikeda. Quantum contracts between schrödinger and a cat. *Quantum Information Processing*, 20(9):313, September 2021.

[76] Kazuki Ikeda. Quantum extensive-form games. *Quantum Information Processing*, 22(1):66, January 2023.

[77] Kazuki Ikeda and Shoto Aoki. Theory of quantum games and quantum economic behavior. *Quantum Information Processing*, 21(1):27, December 2021.

[78] Jessica Illiano, Marcello Caleffi, Antonio Manzalini, and Angela Sara Cacciapuoti. Quantum internet protocol stack: A comprehensive survey. *Computer Networks*, 213:109092, August 2022.

[79] Lucjan Jacak, Pawel Hawrylak, and Arkadiusz Wojs. *Quantum dots*. Springer Science & Business Media, 2013.

[80] Walter G Johnson. Governance tools for the second quantum revolution. *Jurimetrics*, 59:487, 2018.

[81] Erik W Johnston. *Governance in the Information Era*. Taylor Francis, 2015.

[82] David Joseph, Rafael Misoczki, Marc Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Olivier Lacombe, Stefan Leichenauer, Jack Hidary, Phil Venables, and Royal Hansen. Transitioning organizations to post-quantum cryptography. *Nature*, 605(7909):237–243, 2022.

[83] Oliver Kessler and Wouter Werner. Expertise, uncertainty, and international law: a study of the tallinn manual on cyberwarfare. *Leiden Journal of International Law*, 26(4):793–810, 2013.

[84] Sumeet Khatri, Ryan LaRose, Alexander Poremba, Lukasz Cincio, Andrew T Sornborger, and Patrick J Coles. Quantum-assisted quantum compiling. *Quantum*, 3:140, 2019.

[85] H. Jeff Kimble. The quantum internet. *Nature*, 453:1023–1030, 2008.

[86] Mauritz Kop. Establishing a legal-ethical framework for quantum technology. *Yale Law School, Yale Journal of Law Technology (YJoLT), The Record*, 2021.

[87] Mauritz Kop. Ethics in the quantum age. *Physics World*, 34(12):31, 2021.

[88] Mauritz Kop. Quantum computing and intellectual property law. *Berkeley Technology Law Journal*, 35(3), 2021.

[89] Mauritz Kop. Quantum computing and intellectual property law. *Berkeley Technology Law Journal*, 35(3), 2021.

[90] Mauritz Kop, Mateo Aboy, Eline De Jong, Urs Gasser, Timo Minssen, I Glenn Cohen, Mark Brongersma, Teresa Quintel, Luciano Floridi, and Ray Laflamme. Towards responsible quantum technology. *Harvard Berkman Klein Center for Internet & Society Research Publication Series*, 1, 2023.

[91] Mauritz Kop, Mateo Aboy, Eline De Jong, Urs Gasser, Timo Minssen, I. Glenn Cohen, Mark Brongersma, Teresa Quintel, Luciano Floridi, and Raymond Laflamme. Ten principles for responsible quantum innovation. *Quantum Science and Technology*, 9(3):035013, April 2024.

[92] Brian Koziel, Reza Azarderakhsh, Mehran Mozaffari Kermani, and David Jao. Post-quantum cryptography on fpga based on isogenies on elliptic curves. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 64(1):86–99, 2016.

[93] Michal Krelina. Quantum technology for military applications. *EPJ Quantum Technology*, 8(24), 2021.

[94] Ilan Kremer. *Quantum communication*. Citeseer, 1995.

[95] Manoj Kumar and Pratap Pattnaik. Post quantum cryptography (pqc)-an overview. In *2020 IEEE High Performance Extreme Computing Conference (HPEC)*, pages 1–9. IEEE, 2020.

[96] Xiang Li, Su-Xiang Lyu, Yao Wang, Rui-Xue Xu, Xiao Zheng, and YiJing Yan. Towards quantum simulation of non-markovian open quantum dynamics: A universal and compact theory. *arXiv preprint arXiv:2401.17255*, 2024.

[97] Sheng-Kai Liao, Wen-Qi Cai, Johannes Handsteiner, Bo Liu, Juan Yin, Liang Zhang, Dominik Rauch, Matthias Fink, Ji-Gang Ren, Wei-Yue Liu, Yang Li, Qi Shen, Yuan Cao, Feng-Zhi Li, Jian-Feng Wang, Yong-Mei Huang, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Li Li, Nai-Le Liu, Franz Koidl, Peiyuan Wang, Yu-Ao Chen, Xiang-Bin Wang, Michael Steindorfer, Georg Kirchner, Chao-Yang Lu, Rong Shu, Rupert Ursin, Thomas Scheidl, Cheng-Zhi Peng, Jian-Yu Wang, Anton Zeilinger, and Jian-Wei Pan. Satellite-relayed intercontinental quantum network. *Physical Review Letters*, 120(3):030501, January 2018.

[98] Yu-Chen Liu, Yuan-Bin Cheng, Xing-Bo Pan, Ze-Zhou Sun, Dong Pan, and Gui-Lu Long. Quantum integrated sensing and communication via entanglement. *Physical Review Applied*, 22(3):034051, September 2024.

[99] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94(23):230504, 2005.

[100] Chao-Yang Lu, Yuan Cao, Cheng-Zhi Peng, and Jian-Wei Pan. Micius quantum experiments in space. *Reviews of Modern Physics*, 94(3):035001, July 2022.

[101] Benjamin K. Malia, Yunfan Wu, Julián Martínez-Rincón, and Mark A. Kasevich. Distributed quantum sensing with a mode-entangled network of spin-squeezed atomic states. (arXiv:2205.06382), May 2022. arXiv:2205.06382.

[102] Rodney Van Meter. *Quantum Networking*. Wiley-IEEE Press, 2013.

[103] David A Meyer. Quantum strategies. *Physical Review Letters*, 82(5):1052, 1999.

[104] M. Mohseni, A. T. Rezakhani, and D. A. Lidar. Quantum-process tomography: Resource analysis of different strategies. *Phys. Rev. A*, 77(3):032322, March 2008.

[105] Fred L Morrison. Condominium and coimperium. In *Max Planck Encyclopedia of Public International Law*, page 598. Oxford University Press, 2012.

[106] Lyria Bennett Moses. *Regulating in the face of sociotechnical change*. 2017.

[107] Hamid Nejatollahi, Nikil Dutt, Sandip Ray, Francesco Regazzoni, Indranil Banerjee, and Rosario Cammarota. Post-quantum lattice-based cryptography implementations: A survey. *ACM Computing Surveys (CSUR)*, 51(6):1–41, 2019.

[108] Niels M. P. Neumann, Maran P. P. van Heesch, and Patrick de Graaf. Quantum communication for military applications. *arXiv preprint arXiv:2011.04989*, 2020.

[109] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[110] Irmgard Niemeyer, Mona Dreicer, and Gotthard Stein. *Nuclear Non-proliferation and Arms Control Verification: Innovative Systems Concepts*. Springer, 2020.

[111] Elija Perrier. Ethical quantum computing: A roadmap. (arXiv:2102.00759), April 2022. number: arXiv:2102.00759 arXiv:2102.00759 [quant-ph].

[112] Elija Perrier. The quantum governance stack: Models of governance for quantum information technologies. *Digital Society*, 1(3):22, October 2022.

[113] Elija Perrier, Akram Youssry, and Chris Ferrie. Qdataset, quantum datasets for machine learning. *Scientific Data*, 9(1):1–22, 2022.

[114] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8(1):15043, April 2017.

[115] John Preskill. Fault-tolerant quantum computation. *arXiv:quant-ph/9712048*, December 1997. arXiv: quant-ph/9712048.

[116] John Preskill. Quantum computing 40 years later. *arXiv preprint arXiv:2106.10522*, 2021.

[117] Lindsay Elizabeth Rand. *Schrodinger's Technology Is Here and Not: A Socio-Technical Evaluation of Quantum Sensing Implications for Nuclear Deterrence*. Ph.d., University of Maryland, College Park, United States – Maryland, 2023.

[118] M. Riebe, H. Häffner, C. F. Roos, W. Hänsel, J. Benhelm, G. P. T. Lancaster, T. W. Körber, C. Becher, F. Schmidt-Kaler, D. F. V. James, and R. Blatt. Deterministic quantum teleportation with atoms. *Nature*, 429:734–737, 2004.

[119] Laurent Sanchez-Palencia. Quantum simulation: From basic principles to applications. *Comptes Rendus Physique*, 20:1–2, 2019.

[120] Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin. Security of quantum key distribution with imperfect devices. *Physical Review Letters*, 92(5):057901, 2004.

[121] Michael N Schmitt. *Tallinn manual 2.0 on the International Law applicable to Cyber Operations*. Cambridge University Press, 2017.

[122] Peter Schneider. Condominium. In *Encyclopedia of Disputes Installment 10*, pages 58–60. Elsevier, 1987.

[123] Maria Schuld and Francesco Petruccione. *Introduction*, page 1–19. Quantum Science and Technology. Springer International Publishing, 2018.

[124] Maria Schuld and Francesco Petruccione. *Machine Learning with Quantum Computers*. Springer, 2021.

[125] C. Shannon. A mathematical theory of communication. *Bell Syst. Tech. J.*, 27:379–423, 1948.

[126] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, page 124–134. Ieee, 1994.

[127] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[128] Christoph Simon. Towards a global quantum network. *Nature Photonics*, 11:678–680, 2017.

[129] John S Townsend. *A modern approach to quantum mechanics*. University Science Books, 2000.

[130] Alan M Turing. Turing's treatise on enigma. *Unpublished Manuscript*, 1939.

[131] Géza Tóth and Iagoba Apellaniz. Quantum metrology from a quantum information science perspective. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424006, October 2014.

[132] Christine Vanoli. Quantum: No longer 20 years away? *ITU*, November 2024.

[133] Wolff Heintschel von Heinegg. The tallinn manual and international cyber security law. *Yearbook of international humanitarian law*, 15:3–18, 2012.

[134] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

[135] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412):eaam9288, 2018.

[136] Shi-Hai Wei, Bo Jing, Xue-Ying Zhang, Jin-Yu Liao, Chen-Zhi Yuan, Bo-Yu Fan, Chen Lyu, Dian-Li Zhou, You Wang, Guang-Wei Deng, et al. Towards real-world quantum networks: a review. *Laser & Photonics Reviews*, 16(3):2100219, 2022.

[137] Scott Wesley. Linguaquanta: Towards a quantum transpiler between openqasm and quipper. In *International Conference on Reversible Computation*, pages 142–160. Springer, 2024.

[138] H. M. Wiseman and G. J. Milburn. *Quantum Measurement and Control*. Cambridge University Press, URL, 2010.

[139] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, October 1982.

[140] William K Wootters. Quantum entanglement as a quantifiable resource. *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 356(1743):1717–1731, 1998.

APPENDIX

A. JURISPRUDENTIAL CATEGORIES

A. Tallinn Manual definitions

Definition	Classical	Quantum
Cyber infrastructure	Includes classical hardware such as servers, storage devices, and communication networks.	Encompasses quantum-specific hardware like quantum processors, quantum communication devices, and the classical infrastructure supporting them.
Cyberspace	The environment formed by physical and non-physical components enabling data storage, modification, and exchange using classical computer networks.	Extends to include quantum networks and environments enabling entanglement-based communication and quantum data processing.
Cyber activity	Any activity using classical infrastructure or means to affect its operation, such as hacking or data breaches.	Activities involving the use of quantum systems, such as quantum-enhanced encryption or quantum-based attacks on classical systems.
Cyber operations	Employment of classical cyber capabilities to achieve objectives in or through cyberspace, often involving offensive or defensive operations.	Utilises quantum capabilities for objectives like secure quantum communication or quantum algorithm-based attacks on classical encryption.
Cyber reconnaissance	Use of classical tools to gather information about systems, networks, or capabilities, such as scanning or data mining.	Employs quantum techniques, like quantum-enhanced sensing, to detect adversaries or analyse systems with greater precision.
Computer system	Interconnected classical devices, including general-purpose and specialised systems, connected via classical networks.	Includes quantum computers, quantum sensing systems, and nodes of quantum networks integrated with classical systems.
Computer network	Infrastructure of interconnected classical devices enabling data exchange over wired or wireless media.	Extends to quantum communication networks, leveraging entanglement and quantum teleportation for secure data exchange.
Internet	A global system of interconnected classical networks using standardised protocols for communication and routing.	Incorporates quantum internet concepts, enabling secure communication using quantum protocols alongside classical routing systems.
Data	Basic digital elements processed or produced by classical computers, typically represented in bytes.	Quantum data represented by qubits, stored in superposition or entangled states, requiring repeated measurements for extraction.
Data center	Physical facilities housing classical infrastructure for data storage and processing, including cloud services.	Includes quantum data centers for storing and processing quantum information alongside classical data infrastructure.
Electronic warfare	Use of electromagnetic energy to exploit or disrupt classical communication and sensing systems.	Could involve quantum sensing to detect electromagnetic emissions or quantum attacks targeting classical systems.
Cyber attack	Offensive or defensive operations causing injury, destruction, or damage using classical cyber means.	Quantum-based disruptions targeting classical or quantum systems, such as decoherence induction or interception of quantum communication.
Cyber espionage	Classical methods of covertly obtaining information, such as hacking or intercepting communications.	Quantum-enhanced espionage using quantum sensing or exploiting weaknesses in quantum communication protocols.

Table 9: Comparison of Definitions from the Tallinn Manual Glossary in Classical and Quantum Contexts. This table highlights differences and parallels between classical and