



## Research paper

# Post-quantum cryptographic assemblages and the governance of the quantum threat

Kristen Csenkey <sup>1,\*</sup> and Nina Bindel <sup>2,\*</sup><sup>1</sup>Balsillie School of International Affairs, Wilfrid Laurier University, 67 Erb St. W., Waterloo, ON N2L 6C2, Canada and<sup>2</sup>SandboxAQ, 303 S Broadway Suite 105, New York, NY 10591, USA

\*Correspondence author. Kristen Csenkey, Balsillie School of International Affairs, Wilfrid Laurier University, 67 Erb St. W., Waterloo, ON N2L 6C2, Canada.

E-mails: [kcsenkey@balsillieschool.ca](mailto:kcsenkey@balsillieschool.ca), [nina.bindel@sandboxaq.com](mailto:nina.bindel@sandboxaq.com)

Received 31 August 2021; revised 11 March 2022; accepted 10 October 2022

## Abstract

Threats against security in the Internet often have a wide range and can have serious impacts within society. Large quantum computers will be able to break the cryptographic algorithms used to ensure security today, which is known as the *quantum threat*. Quantum threats are multi-faceted and very complex cybersecurity issues. We use assemblage theory to explore the complexities associated with these threats, including how they are understood within policy and strategy. It is in this way that we explore how the governance of the quantum threat is made visible. Generally, the private and academic sectors have been a primary driver in this field, but other actors (especially states) have begun to grapple with the threat and have begun to understand the relation to defence challenges, and pathways to cooperation in order to prepare against the threat. This may pose challenges for traditional avenues of defence cooperation as states attempt to understand and manage the associated technologies and perceived threats. We examine how traditionally cooperating allies attempt to govern the quantum threat by focusing on Australia, Canada, European Union, New Zealand, UK, and USA. We explore the linkages within post-quantum cryptographic assemblages and identify several governmental interventions as attempts to understand and manage the threat and associated technologies. In examining over 40 policy and strategy-related documents between traditionally defence cooperating allies, we identify six main linkages: *Infrastructure*, *Standardization*, *Education*, *Partnerships*, *Economy*, and *Defence*. These linkages highlight the governmental interventions to govern through standardization and regulation as a way to define the contours of the quantum threat.

**Key words:** post-quantum, quantum threat, assemblage, government interventions

## Introduction

Given the importance of cybersecurity ensured by cryptographic algorithms in the Internet, threats against these algorithms pose potentially great risks. For example, if the authenticity of software is compromised, then the software can be changed maliciously. This might lead to installation of spy software, money being transferred to a different account than originally intended, malfunction of brakes in vehicles, or many other scenarios that could potentially lead to serious societal interruptions.

One particularly great risk is posed by quantum computers that are large enough to essentially break all public-key cryptography in use today (1). To prepare for this security threat, cryptographers have been working on alternative algorithms that are not known to be vulnerable to quantum attacks. These alternative algorithms are often called post-quantum or quantum-secure cryptographic algorithms. In addition to academia and early adopters from industry, policy-makers and decision-makers may soon need to confront a landscape where malicious state and non-state actors take advantage

of quantum computing's distinctive characteristics to target critical infrastructure and other potential targets. A critical infrastructure disruption would have a serious impact on the health, safety, and economic well-being of ordinary people. Part of the process of protecting against these threats is governing them and their potential impacts.

This paper aims to explore how governance is made visible through the management of the quantum threat. We use *assemblages* as a tool to collect, understand, and visualize information, as well as to identify and understand the complexities of actors, threats, technologies, practices, strategies, and policies involved in the governance of the threat.

We draw on the use of assemblages to make sense of the various approaches and explore how quantum threats are *made*, who *makes* them, and how the technology is understood. This approach also serves to highlight the interconnectedness, disjointedness, and spaces for cooperation. Our exploration into the *linkages* and the assumptions that bind policies, networks, and actors to the quantum threat is in no way comprehensive. In this context, linkages are the connections between actors, their goals, and contestations within the complex cybersecurity networks. These networks comprise human actors, technologies, and bureaucratic structures, among other things. Our analysis is a singular sliver that focuses on the current perceptions of threats and future visions of addressing said threats.<sup>1</sup> We show how the quantum threat is understood, addressed using post-quantum algorithms instead of current cryptographic algorithms, and regulated as a subject of defence through government interventions. We ask, how is the quantum threat and the preparation against it conceptualized in policies and strategies? Who are the identified actors involved in this process and what roles are they ascribed? We highlight how these framings appear across regional assemblages by focusing on traditional defence cooperation between allies, specifically Australia, Canada, European Union (EU), New Zealand, UK, and USA.

Our paper is structured as follows. First, we explore the uses of assemblages in international relations (IR) theory to understand cybersecurity practices and *realities*. We apply this approach to understanding post-quantum cryptographic assemblages while remaining wary of the recent trend of over-enthusiastically applying *all things quantum* to IR. Following this, we explain the quantum threat from a technical perspective. We visualize parts of the post-quantum cryptographic assemblages in an attempt to highlight the linkages between actors, objectives, and understandings of the technology. We provide an accompanying description of our visualization in an overview of strategies section. This is followed by an exploration into the details of the assemblage, including key links and government intervention practices. We conclude by highlighting possible future areas of cooperation and what this may mean for defence partnerships and allies.

## Introduction to and application of assemblage theory

Assemblages do not privilege any one thing, theory, or actor. Instead, it sees e.g. a technology such as quantum computers, quantum computing, quantum threats, post-quantum cryptography, etc. as materially and immaterially interlinked with (other) technologies, discourses, policies, actors, and networks, among other *things*. The value in assemblages is not in the definition *per se*, but what they do.

In what follows, we explain what assemblages are and how we apply assemblage theory from the literature to the topic of the quantum threat and post-quantum strategies.

### Assemblages in the literature

We rely on Deleuze and Guattari (5) and DeLanda's (6) foundational concepts and follow Collier (7), Stevens (8), Egloff and Cavelti (9), and Liebetrau and Christensen's (10) approaches to cybersecurity assemblages as a conceptual framework to understand the quantum threat and post-quantum strategies. We apply Li (11) and Puar's (12) understanding of assemblages to see how the quantum threat as a concept is understood and specifically how post-quantum algorithms are used to mandate solutions to security problems, and how these solutions are enforced in policy. This provides a *clearer* picture of the multiple and dynamic attempts of various actors involved in the conceptualizations of quantum threats. The explicit focus on preparing for the quantum threat by the post-quantum algorithms/transition as a piece of assemblages is a way to understand the establishment and institutionalization of the strategy into practise to address quantum attackers.

Part of understanding what assemblages do is understanding their multiple and dynamic configurations. Deleuze and Guattari (5) conceptualize assemblages as relations of segments and patterns. It focuses on variations instead of constants and is a conceptual tool to see and understand how things combine, clash, and recombine. DeLanda (6) built off Deleuze and Guattari (5) and systematized the concept of assemblages. For DeLanda (6), assemblages are relations between a mixture of components that are both material and immaterial, territorizing and deterritorializing, and coding and decoding. Assemblages include dynamic networks with multiplicities of actors, ideologies, discourses, objects, etc. These connections and their components change, dissolve, and expand; they are pieces that make up a whole and many wholes. They can recombine, creating new assemblages, and therefore the focus is not on the individual parts, but on the relations between. Focus is placed on the connections and relations within assemblages, the mixing of assemblages, and their transformations, e.g. as applied to cybersecurity assemblages.

### Cybersecurity assemblages and the creation of the quantum threat

The quantum threat is, in part, a number of complex cybersecurity issues. The use of assemblages to understand cybersecurity and cyber-related technologies has received recent interest by the academic community studying cyber. Collier (7) argues for the use of assemblages to understand the configuration of a variety of actors within the cybersecurity environment. Like Abrahamsen and Williams' (13) understanding of global security assemblages, cybersecurity assemblages include public, private, global, and local actors, and their partnerships, agendas, research, strategies, and sites of competition. There are different configurations of cybersecurity assemblages based on actors and the process in which they are involved in cybersecurity challenges. For example, Stevens (8) shows how cybersecurity is *made* through private sector discourses on specific threats, showing how these actors can *make* a threat into a cybersecurity event of global importance. Stevens shows how Symantec's public reporting of malware incidents, such as Struxnet, are important knowledge-making practices, as they make threats visible and important to the public sector. In contrast, the quantum threat needs to be *made* into a threat differently. In particular, it is important to understand the threat now before it becomes apparent through an attack.

<sup>1</sup> We explore other slivers of this topic in previous publications such as refs. (2–4).

The definition of associated challenges within cybersecurity assemblages helps to define how cybersecurity is *made* and understood. For Stevens (8), cybersecurity includes the technologies, processes, practices, and relationships dealing with any aspect of security in cyberspace. It is an ecosystem of these components that is continuously co-produced by various actors, policies, and frameworks. In this case, power is seen through the structures and discourses that work to define actions. Egloff and Cavelty (9) have shown the usefulness of using assemblages to understand the complexities and dynamics of cybersecurity. They focus specifically on knowledge creation assemblages. By focusing on the process of managing cyber incidents and attribution, Egloff and Cavelty show the political linkages, various actors, and processes involved in the knowledge creation process. These assemblages are influenced by and influence knowledge assemblages about threats. This, in turn, shapes the *realities* of cyber conflicts, mainly, the *truths* about cyber conflicts in the world. For them, *truths* are stable, accepted, neutral, and value-free knowledge. They show that truths about cyber conflicts are largely value-laden assumptions made by different actors.

Actors, their responsibilities, and the capabilities of technologies are an important part of cybersecurity assemblages. Actors hold and exercise power as well as enact knowledge practices about specific technologies. In their analysis of the Mirai malware through an assemblage of human and non-human actors, technologies, and relations between, Liebetrau and Christensen (10) show how the intersections between security and politics are dynamically made and unmade over time. For Liebetrau and Christensen, assemblages are intimately tied with politics and involve multiple actors, sites, and interconnected spaces. It is in these multiple sites and spaces that the politics of cybersecurity happens, reflecting the dispersed nature of associated technologies.

Collier (7), Stevens (8), Egloff and Cavelty (9), and Liebetrau and Christensen (10) use assemblages to address the complexities and linkages within the environments, realities, and political contestations of cybersecurity. Our use of assemblages aims to explore the arrangements of technologies, the perceptions, discourses, and actors, including experts and knowledge creators. By using assemblages as a conceptual and analytical tool, we explore how the quantum threat is known, nested, and positioned within institutional and organizational structures, how it creates and is created by scales of realities of the technology and its uses. As shown later in this paper, governmental intervention plays a key role in making and interpreting knowledges about quantum threats, technologies, and capabilities.

### Institutionalized arrangements and anchorings

How quantum threats are understood by various actors, anchored in policy, and shaped by defence logics is a useful way to see the perceived realities and futures of the technology, which can include identifying actors and their relationships. Anchorings are meaning-making methods that ground knowledge, and provide reference points for other linkages within networks. The institutional arrangements (i.e. configurations of powers) of these relationships, logics, perceived threats, and technologies are part of the governance process. Standardization and regulation are a method of governance through shaping perceived pathways of power, problems, and solutions to these problems. As we show later, this is one of the most important tools used in the post-quantum transition as explained later. In this context, problems are the seemingly ungovernable issues, things, and people, among other examples, that are contestable, dynamic, and fluid. For the purposes of this paper, quantum threats are problems. Shaping the production of the problem influences the

delegation and design of power, authority, and legitimizes knowledge (14). Generally, actors within the private sector have been the primary drivers in the cybersecurity field, especially with regards to standardization: for example, the creation of the FIDO2 standard for passwordless authentication and Adobe's PDF. PDF became a *de facto* standard in the marketplace and an international standard (ISO 32000-14) in 2008. Similarly, the FIDO2 protocol became a *de facto* standard as major actors formed the *FIDO Alliance* to agree on the protocol. Generally, states have been relatively slower to identify a response in a similar method.

Assemblages and the elements that make up their composition can be interlinked and interconnected without forming a coherent whole (15). In the context of institutional arrangements of power, this means that various actors, their differing authorities, logics, and objectives can coexist and clash to form a whole, whereby governance can exist without a single centralized power (i.e. the state). Although Collier (7), Stevens (8), Egloff and Cavelty (9), and Liebetrau and Christensen (10) have shown that states and governments have an important role in the management of cybersecurity assemblages, others, like Sassen (16), see a declining role of the state. For Sassen, authority and control to manage certain global problems has transitioned to the private sector as the role of the state has changed. Sassen sees assemblages as tools to understand the complexities of a modern, globalized world and uses them as an analytical category, a tool, an outcome, and a result. Moreover, Sassen places specific focus on territory, authority, and the dynamics of the global to understand specialized assemblages. These specialized assemblages have spatial, temporal, and normative realignments and segmentations. Global in nature, these assemblages shed light on the complexities of the modern world beyond borders and states, and consequently highlight the difficulty of governance. For Sassen, this is a process that starts with the state. Collier (7) builds off this process, and formulates an assemblage framework based on how actors address cybersecurity challenges. Egloff and Cavelty (9) also define a three-phase process whereby private and public actors engage in attribution of attackers. We see the focus on defining processes as a way to use and make sense of assemblages rather restrictive, as it places emphasis on defining what assemblages *are* instead of what they attempt to *do*.

### Connections within assemblages

Drawing on Puar (12), we do not see things within assemblages as discrete, binary, or inherently categorizable. Assemblages can be understood without strict definitions or pronouncing processes to understand connections. It is the focus on the linkages that harkens back to Deleuze and Guattari's (5) original concepts that we draw on. We are interested in the connections between actors, concepts, technologies, and narratives about threats that generate the subject of quantum technology and the normalization of it within defence circles and logics. The aim of normalization is to regulate and define practices, logics, and norms. It makes institutional arrangements apparent. The framings of the quantum threat, within government and related documents, including policy papers, strategies, and bulletins, shed light on how quantum threats are produced, linked to defence frameworks, and institutionalized through cooperation with other actors and other states. We connect the framing of these threats within the discourse to their anchoring within informal and formal defence cooperation.

The anchoring of quantum threats within policy discourses is an attempt to stabilize and institutionalize the relations between and within assemblages. Stabilizing assemblages (i.e. when uncertainties

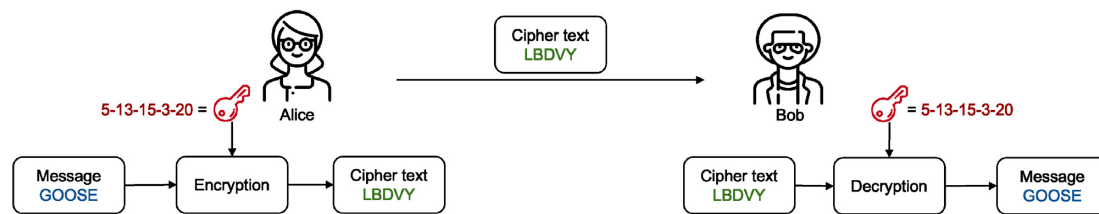


Figure 1: Symmetric encryption.

are given boundaries, made coherent and ascribe meaning) is accomplished through the management of elements of assemblages. Drawing on Li (11), government interventions in the management of assemblages have regional and international linkages. These assemblages include knowledges, objectives, discourses, and actors. Li (11) focuses on how these pieces are brought together through government interventions. This focus also sheds light on the tensions between actors and objectives, and the emergence of new assemblages in the wake of contestations. It also allows a closer examination of the power and relational authority, and the multiple networks of influence that attempt to govern through order-making (17,18). Often, these assemblages emerge or are altered in the space of contestations, disruptions, or problems. In this case, we focus on the quantum threat as a problem or contestation, whereby connections between agents and objectives are brought together by the governments and through their international defence cooperation (i.e. the defence alliance of the *Five Eyes*). This management of assemblages emerges from a space of struggle to understand the technologies and the threats in all its forms. We begin this exploration by understanding the technical details of the quantum threat in the next section. Before that we will separate our approach of *post-quantum assemblages* from *quantizing IR* in the next subsection.

### Quantum and quantizing IR theory

Understanding *all things quantum* has gained popularity in recent discussions about its applicability to IR theory. These understandings have generally manifested in two main ways: quantizing IR and applying quantum ontology to IR theory. Der Derian and Wendt's work on quantum approaches of IR (19) [also see refs. (20–22)] argues for a multiplicity of frameworks. Zanotti (23) calls for a theoretical framework nested in quantum ontologies or quantum conceptions of reality. We find a focus on theorizing quantum or *quantizing* IR theory (whether multiple or singular) valuable, although not holistic enough to understand the quantum threat in all its forms (or lack thereof) in IR theory. We find that perceptions of *all things quantum* are being applied to theory and quantum technologies without fully appreciating the nuances of this approach or the technology itself. This type of theorizing over-emphasizes the importance of applying *quantum* (or perceptions of quantum) to IR theory and misses highlighting the relations and interconnectedness between actors, roles, and technologies. As interesting as it is, we deem this method as not sufficient enough to understand the complexities involved in the use, perceptions, and production of these technologies, theories, actors, and the linkages between them. In an attempt to clarify these complexities, we focus on quantum threats, specifically how they are understood in strategy and policy. We examine the perception of these threats in various state strategies and comment on their linkages using assemblage theory.

### Short introduction to cryptography

In this section, we explain the quantum threat, specifically (1) the types of algorithms large quantum computers are able to break (and which not), (2) how quantum computers are different from classic transistor computers, and (3) how the technology is perceived as a threat by the different actors and the discourse used to frame it. We will start with a short introduction to cryptography and different cryptographic algorithms.

### Symmetric and asymmetric cryptography

For centuries, cryptography has enabled confidential data communication. At first, it was mostly used for defence purposes, but now it is essential for our everyday lives. The most basic principle works as follows. Two parties (in the cryptographic community often called Alice and Bob) share a secret key, known only to the two. Given this key, Alice can encrypt a message, send it to Bob who can then use the same key to decrypt the message. An easy example explains this idea—in an encryption scheme called the (extended) Caesar cipher, every letter in Alice's message will be replaced by a letter some position farther down in the alphabet, e.g. the letter *A* is replaced by the letter *D* (so, three letters down), the letter *B* by *R* (14 letters down), etc. For example, the word *GOOSE* is encrypted to *LBDVY* using the key 5-13-15-3-20, see Fig. 1. Interestingly, if an adversary tries to decrypt the ciphertext *LBDVY* without knowing the key, they will not be able to because the answer could be every five letter bird (strictly speaking it could be any five letter combination). For example, decryption using 4-23-12-7-11 returns *HERON*.

It is important to point out that in the above described algorithm, the secret key needs to be as long as the message to-be-encrypted. In modern algorithms of this kind, called *stream ciphers*, each character of the plain text is combined with a character of a key stream. This key stream is generated from a short key of fixed length (e.g. 128 bit) using a *pseudo-random* generator. Therefore, it is sufficient for the key to be of a fixed length that is usually much shorter than the plain text length. In addition to stream ciphers, there also exist other classes of algorithms such as *block ciphers* that use different construction principles but are also able to take fixed-length keys as input. A prominent example for block ciphers is the widely used *Advanced Encryption Standard* (AES). We omit further details and refer to ref. (24) for more a detailed explanation.

A cryptographic algorithm, where both parties know a single key, is also called symmetric. Other examples for symmetric cryptographic primitive in addition to encryption are message authenticate codes (MAC) or hash functions. The disadvantage of symmetric cryptography is that Alice and Bob need to find a secure way to agree on secret keys of sufficient length to later be able to, e.g. encrypt and decrypt messages. Enter, asymmetric cryptography, such as public-key encryption (PKE).



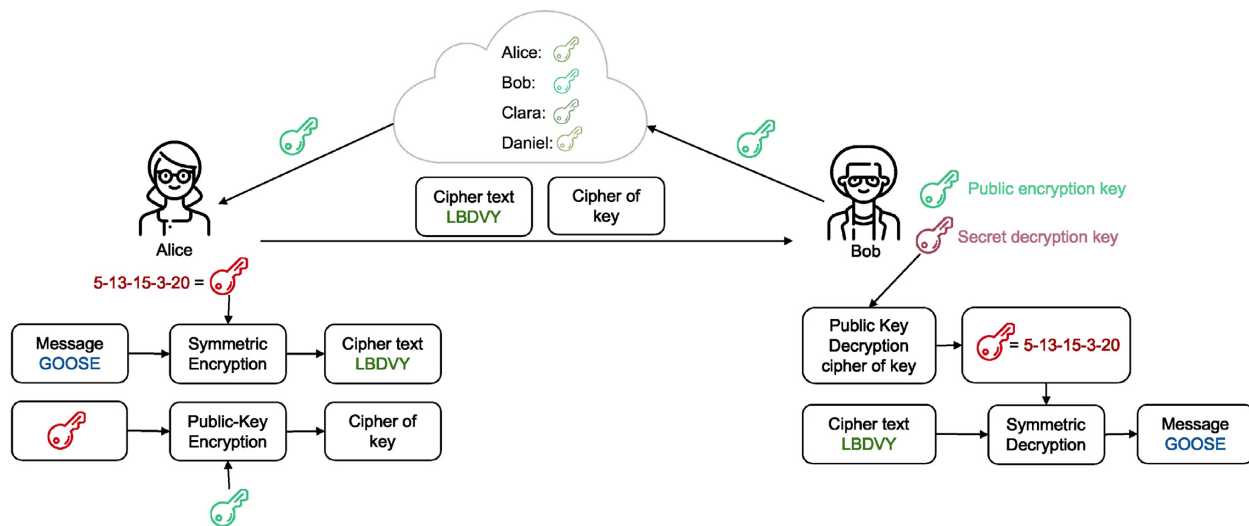


Figure 2: Combination of asymmetric and symmetric encryptions.

To enable PKE, every party needs two keys: an encryption key (which is public) and a decryption key (which will be kept secret and is known to nobody except the owner). Every party generates their own key pairs and uploads the encryption key to a database. If Alice wants to encrypt a message to Bob, she first downloads Bob's encryption key, uses it to decrypt her message, sends the cipher text to Bob, who can then use his decryption key to decrypt the message.

Since asymmetric encryption schemes are rather slow, in practice, asymmetric and symmetric encryptions are usually combined— asymmetric encryption is used to encrypt the short symmetric key (this corresponds to the key agreement), while the actual message is encrypted using faster symmetric encryption (see Fig. 2).

To ensure security of asymmetric encryption, it is of utmost importance that the secret decryption key cannot be computed from the public encryption key. This can be realized based on hard mathematical problems. For example, given two prime numbers, it is easy and very fast to multiply the two integers. It is, however, very difficult to compute the prime factors of a very large integer. This integer prime factorization problem is, in fact, the underlying mathematical problem used in the RSA scheme by Rivest, Shamir, and Adleman. Essentially, the secret key consists of the two prime numbers, and the public key of their product. In addition to PKE, also digital signatures can be constructed from the same underlying mathematical problems. Most of our asymmetric cryptography today is based on the integer prime factorization or the so-called discrete logarithm problem. That means, if an attacker can solve these two mathematical problems, they can essentially break the security of all our currently used public-key cryptographic algorithms.

While no algorithm in the literature solves these mathematical problems in polynomial time (i.e. efficiently) on current transistor (also-called classical) computers, Shor's algorithm solves these problems in polynomial time using a quantum algorithm. Hence, as soon as quantum computers exist that are large enough to implement and run Shor's algorithm for key sizes in-use (e.g. 2048-bit RSA), the current security guarantees do not hold anymore (1).

Interestingly, quantum computers do not have the same devastating impact on symmetric cryptography. Other than increasing the

length of the keys, no changes to the algorithms are required as far as we know.

### Quantum computers

Quantum computers are a new generation of computers that use the principles of quantum physics for computations. Data are saved, processed, and communicated in quantum states, so-called qubits, on such computers.

Small quantum computers already exist and some are even accessible for everyone. The record-holding quantum computer uses 72 qubits (25), meaning that this technology is still in its infancy. To break RSA-2048 in <6 hours, ~20 million qubits are necessary (26). Although this seems to be a long way off, the development of quantum computers has the potential to benefit multiple fields with their diverse uses. This includes accelerating artificial intelligence (AI) and improving simulations, for a variety of purposes, such as weather predictions or pharmaceuticals. Given the potential economic benefits, companies like Google, IBM, Alibaba, and other (27) have invested in quantum computing. This investment is also increasingly integrated within the strategic research plans of universities and governments around the world. This increase in interest of private sector companies, universities, and governments may accelerate the development of large quantum computers. Indeed, in a recent study, quantum computing experts estimate that quantum computers large enough to break RSA-2048 will be built within the next 14 to 30 years (28).

Presumably as a result of the advances in quantum technology, The National Institute for Standards and Technology (NIST) held a workshop to 'engage academic, industry, and government stakeholders [...] to discuss issues related to post-quantum cryptography and its potential future standardization' in 2015 [US.2]. Around the same time, the National Security Agency (NSA) published an updated guidance, which algorithms are to be used and included using post-quantum algorithms [US.3]. These two sources are the first documents mentioning post-quantum algorithms explicitly. Hence, in our analysis, we only analyse policy and strategy documents starting from 2015.

## Perceived threats

While large quantum computers will be able to break the security of most public-key cryptography, the implications of this technology are perceived differently by the various actors involved in the process of understanding and addressing threats. In our analysis of policies, strategies, and other related government documents, we found that the perception of threats varied both in actually understanding the uses of the technology, users, intentions, and the impact of the threat.

Many documents [CA.9, CA.10, EU.1, EU.3, EU.15, US.1, US.4, US.5, US.8, US.7] state the quantum threat plainly as technical as described in the last subsection. Some of them are more specific by stating that quantum computers threaten the integrity and confidentiality of communicated data. For example, [CA.2] states: ‘At that time, quantum computing could put today’s P[ublic]-K[ey]C[ryptography] at risk, and the confidentiality and integrity of encrypted information may no longer be assured’. This might put actors, including governments, at risk. In addition, [EU.5] mentions a legal issue that might arise from the quantum threat: “From business, ethical, and legal perspectives, this [breaking security due to quantum computers] would violate the regulatory requirements for data privacy and security that are in existence today’.

Another, more concrete aspect of the quantum threat mentioned in documents [CA.2, CA.10, CA.12, EU.3, UK.5, US.7] are so-called back-traffic or store-now-decrypt-later attacks, where encrypted communicated data are captured and stored today to be decrypted as soon as the attacker has access to a sufficiently powerful quantum computer. A few documents [AU.3, CA.5, US.7] explicitly mention the threat to national security and defence, such as the US-American Homeland Security, as a consequence.

Moreover, the quantum threat is also perceived as a threat against the supply chain if not all partners participate in the post-quantum transition (29) or against business continuity [EU.3] as businesses must adapt and account for the post-quantum transition. For example, ref. (29) states ‘[businesses] may need to consider shortening the supply chain and creating more products *in-house* for a time if partners do not transition’.

In [EU.1], the European Telecommunications Standards Institute (ETSI) summarizes that post-quantum cryptography and security is essential for (1) protecting government and military communications, (2) securing financial and banking transactions, (3) assuring the confidentiality of medical data and healthcare records, (4) safeguarding the storage of personal data in the cloud, and (5) restricting access to confidential corporate networks.

The documents we analysed do not explicitly give information about the attacker, often called *threat actor*. Indeed, in theory, any actor able to access a full-fledged quantum computer is a threat actor. In practice, however, given the huge cost to build and run state-of-the-art quantum computers, only a few states and corporations could be considered as potential threat actors. For example, IBM or Google who lead the publicly available research, have these abilities.

## Not all is lost

Researchers have been working on post-quantum secure alternatives that are presumably secure against quantum attackers. At the core of these algorithms lie different mathematical problems (i.e. alternatives to the integer prime factorization or the discrete logarithm problem mentioned above) that cannot be solved efficiently by quantum algorithms. By replacing the underlying security assumptions, the design of the entire algorithm changes, and then implementations have to be changed as stand-alone libraries as well as all protocols and applications, such as the Transport Layer Security (TLS) protocol used

to access, e.g. this article online. As stated by NIST in 2017, ‘Historically, it has taken almost two decades to deploy our modern public-key cryptography infrastructure. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing’. Mosca (30) quantified the urgency of starting the transition to post-quantum cryptography using an equation of the following three variables in the equation: The first variable, called  $l$ , gives the life-span of the information that needs to be kept secret (also used in [CA.5]). The second variable, called  $d$ , is how many years it will take to deploy post-quantum algorithms in the used applications. The last and third variable, called  $q$ , is the number of years until quantum computers are powerful enough to break our current algorithms.<sup>2</sup> Now, if

$$l + d > q,$$

this means that quantum computers can break our data protection faster than we can deploy post-quantum algorithms. For example, if quantum computers able to break RSA will exist in  $q = 15$  years, but we need  $d = 12$  years to deploy post-quantum algorithms protecting data that needs to be secret for  $l = 20$  years, it holds that

$$20 + 12 > 15,$$

and hence, the data will not be protected in time. As it is uncertain when quantum computers will be large enough to break our current cryptography, the preparations against the quantum threat need to be taken now. This is also supported in different documents we analysed such as [CA.10]: ‘There is a risk if action is not taken immediately, that a quantum computer will be employed before enough time has passed to render the intelligence value of encrypted information useless to an adversary’.

To keep the security guarantees of our currently used cryptography, and to add security against quantum computers, standardization agencies [EU.13, US.8] recommend utilization of hybrid algorithms. That is, combining classical (i.e. quantum-vulnerable) with post-quantum secure public-key algorithms (31, 32). This is meant as an intermediate phase in the post-quantum transition to ensure trust in the used cryptographic algorithms.

## All things quantum

As there has emerged a certain hype about quantum technology [e.g. ref. (33)], we would like to carefully distinguish between different terms.

The first is *quantum computing* (related to quantum computers, quantum technology, quantum devices). This means a device that is able to run operations using superposition quantum states, be it a full-fledged universal computer capable of many different operations, or a smaller device able to run some computations making use of quantum states to solve a very focused problem.

Another notion that is often mentioned in this context is quantum cryptography, quantum key exchange, or quantum key distribution (QKD). This technology uses principles of quantum physics as well, but in a different way than quantum computers do. It sends and receives quantum states but it does not manipulate (i.e. it does not compute on) them. QKD is a way of agreeing on a key instead of, e.g. using PKE as in Fig. 2. In a nutshell, the advantage of this technology is that we know it is secure if our understanding of quantum

2 In [EU.3], another variable is added, namely the number of years  $t$  it takes to ensure trust in a cryptographic algorithm, with  $d$  strongly depending on  $t$ .

physics is correct (enough). The disadvantage is that it needs a completely new cryptographic infrastructure than our current public-key infrastructure. Implementing a full QKD-based system and comparing the (dis-)advantages with other quantum-safe cryptography (such as post-quantum cryptography) depends very much on the use-case. Therefore, we omit a more detailed comparison.

The arguably most important advantage of post-quantum cryptography is that it preserves the current infrastructure. That means the cryptographic solutions are designed to be used by our current transistor-based (and non-quantum) computers and our current infrastructure but are secure against classical *and* quantum attackers. Hence, current (quantum-vulnerable) cryptographic algorithms have to be replaced but essentially no physical changes to the infrastructure have to be made. That being said, due to different run times and sizes (e.g. key sizes or signature or cipher text size), components within the existing infrastructure have to be changed, such as allowing for larger signature sizes in software libraries.

In what follows, we focus primarily on post-quantum algorithms and not on quantum cryptography, QKD, quantum computers, or quantum technology in general, although at times the distinction between these *all things quantum* in the documents was difficult to decipher. For example, *quantum* is often used generally to refer broadly to quantum computers, quantum technology, quantum cryptography, etc. as well as quantum threats. We attempt to distinguish the intended meaning, where applicable, based on the context of the document, publisher, and related references therein. We explore the linkages between objectives, actors, and technology regarding preparation against the quantum threat by transitioning to the post-quantum algorithms.

## Main strategies to prepare against the quantum threat

To discuss the different strategies for preparing for the quantum threat by preparing the post-quantum transition, we analysed policy and strategies-related documents associated with different government departments and agencies from Australia, Canada, the EU, New Zealand, the UK, and the USA. While others [see CIFAR 2021 (34)] have focused on national quantum strategies specifically with a focus on Research and Development (R&D), we examine national strategies in addition to other documents, such as bulletins, policy frameworks, calls for proposals, and published statements, in order to gain a more holistic understandings of the linkages that comprise the assemblages. It is important to emphasize that we do not include investments to quantum computing or QKD. While, in particular, QKD can be viewed as a way to prepare for the quantum threat, this is out of scope of this article as mentioned earlier.

The detailed list of our analysed documents can be found below as our list of primary resources. We use assemblages to understand the linkages between quantum threats, relationships between actors, and objectives within the select documents. We indicate the country code to each document to give a better understanding of partnerships and linkages. It is important to note that we do not distinguish different agencies of the same state, e.g. NSA and NIST or the European Union Agency for Cybersecurity (ENISA) and ETISI.

In our analysis, we identified six different primary purposes in the analysed documents, namely *Economy*, *Education*, *Defence*, *Infrastructure*, *Partnerships*, and *Standardization*, that are visualized in Fig. 3. In this figure, we (sub-)visualized the strategies that were mentioned or were identified in the policy and strategy documents. As can be seen in the figure, some categories appear more than once.

For example, while *Standardization* is a primary purpose, it is also a category of government-to-government partnerships.

We only list strategies that are identified in the policy- and strategy-related documents and organized different strategies to identify different actors and linkages. For example, in the primary purpose *Education*, we make a distinction in different actors such as the private sector as these separations were made in the documents. As a further distinction between private sector companies handling government data and others, we only list supporting documents in these two subcategories but do not cite them as resources for the private sector in general. The same also holds when analysing the purpose of *Infrastructure*, and more concretely critical infrastructure, where documents where *Protecting government data* have been mentioned (i.e. [AU.1,US.1,US.4]) are not listed together with the documents where *Critical Infrastructure* in general has been mentioned (i.e. [EU.15, US.8]). Moreover, the same document might appear in several subcategories. For example, [US.8] described migration strategies (as a primary purpose of *Standardization*) for different actors, hence, it appears in all subcategories.

It is important to note that we do not place emphasis or importance on any single document or resource. For example, while NIST's post-quantum standardization [US.4] is arguably one of the most important documents and projects, we do not attribute more importance to it in our visualization. Instead, it acts as a temporal starting point to situate the analysis of governmental interventions.

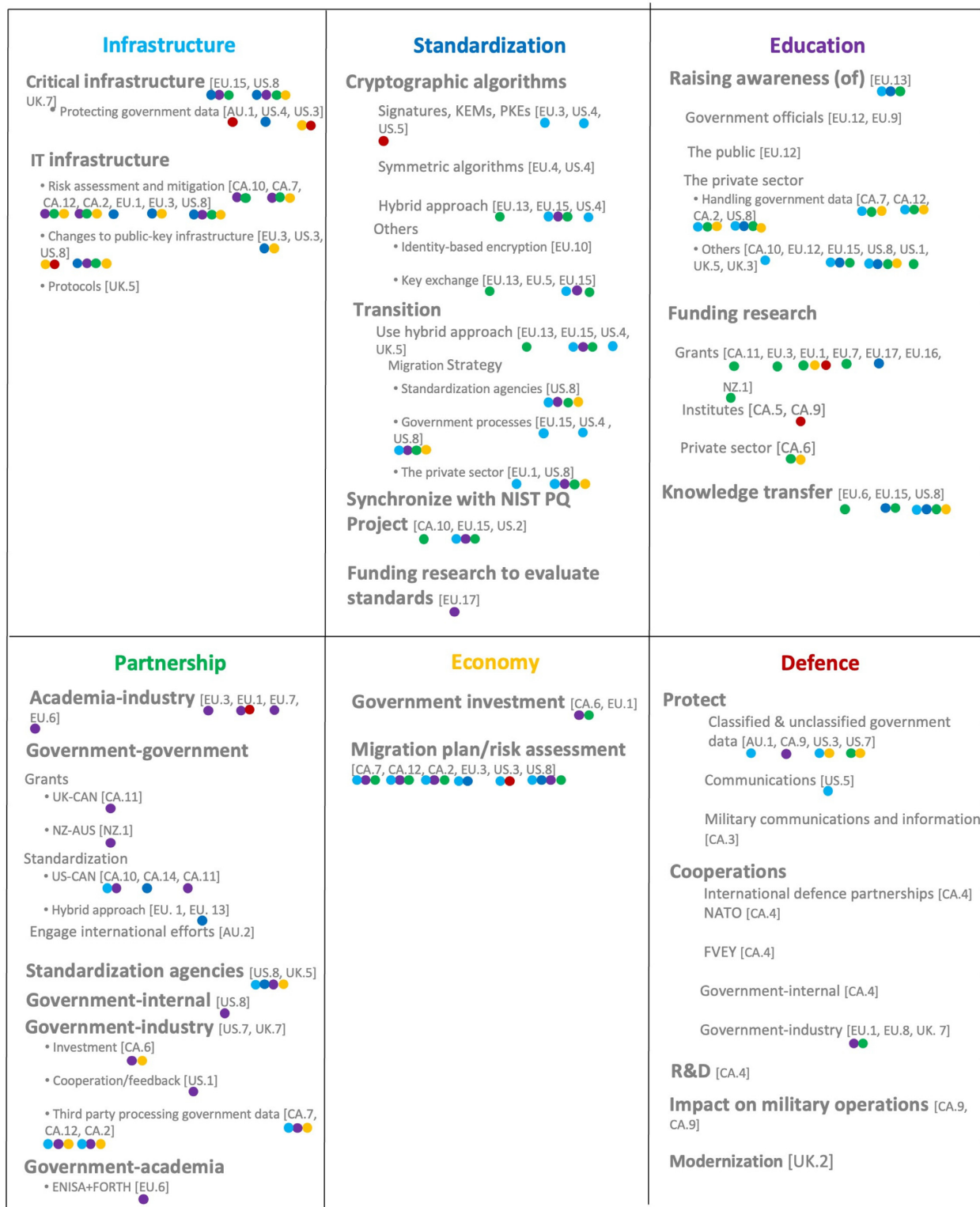
In addition to the categories of strategies and the supporting documents, we also visualize the linkages using dots of the respective colours in Fig. 3. For this, each primary purpose is written in a different text colour, namely *Economy* (yellow), *Education* (purple), *Defence* (red), *Infrastructure* (light blue), *Partnerships* (green), and *Standardization* (dark blue).

More concretely, we show links between the purposes when more than one purpose can be found in a document. For example, [US.8] mentions five of the six main purposes: *Economy*, *Education*, *Infrastructure*, *Partnerships*, and *Standardization*. Therefore, when listed in *Infrastructure*, four coloured dots are below the reference. There are, however, of course also documents listed in one column, without any links to other purposes, such as [US.7]. Our visualizations uses colours to allow for easier identification of strong linkages. For example, *Partnership* and *Education* seem to be very much intertwined, and *Standardization* seems to rely heavily on *Partnership*. We discuss the different linkages further in the next section.

## Post-quantum cryptographic assemblages

Our visualization in Fig. 3 attempts to highlight the pieces of different post-quantum cryptographic assemblages among traditional defence allies in an effort to identify the institutional anchoring, linkages, and interconnections between actors, objectives, and technology. This serves to shed light on attempts at governing the quantum threat by preparing for the post-quantum transition. Government interventions may attempt to forge connections and form a coherent whole and this coherent whole may seem easier to govern and manage. Yet, we identify several contestations, competing priorities, and assumptions within these interventions.

Thus far, the private sector has led interventions in this field, but government interventions are becoming increasingly important as states grapple with the governance of the technology and the management of the associated and perceived threats. These government interventions have similar contours, regardless of the assemblage. Li (11) identifies six general practices of assemblages: (1) forging alignments,



**Figure 3:** Visualization of strategies and primary purposes; linkages are visualized using dots in the colour of the respective primary purpose.

(2) rendering technical, (3) authorizing knowledge, (4) managing failures and contradictions, (5) anti-politics, and (6) reassembling. *Forging alignments* focuses on the act of linking objectives between actors within an assemblage. *Rendering technical* is making a problem intervenable with an associated process for a manageable end result.

*Authorizing knowledge* entails specifying a body of knowledge that confirms assumptions and contains critiques. *Managing failure and contradictions* is handling the perception of failure as a fixable outcome. *Anti-politics* is when *the political* is re-positioned as a matter of technique. As such, reference to expertise re-positions the prob-



**Table 1:** Identified general practices in the observed main strategies.

	Forging alignments	Rendering technical	Authorizing knowledge	Managing failure	Anti-politics	Reassembling
Infrastructure	×					
Standardization	×	×	×	×		×
Education	×		×			
Partnership	×					
Economy						
Defence			×			

FA = forging alignments, RT = rendering technical, AK = authorizing knowledge, MFC = managing failures and contradictions, AP = anti-politics, R = reassembling.

lem, while limiting engagement about the governance process itself. Lastly, *reassembling* is reworking, combining, and grafting new elements with old ones.

By using Li's (11) method of examining how assemblages are actually assembled, we find that post-quantum cryptographic assemblages have emerged in the struggle to understand the technology itself, specifically within the defence context and the linking intersection points.

For Li (11), the six practices are found in all assemblages, yet, we see an emphasis on forging alignments, authorizing knowledge, and reassembling as the main practices of post-quantum cryptographic assemblages. The six primary purposes we identified within the policy and strategy documents relating to quantum threats and depicted in Fig. 3 allow us to see how these assemblages are created and the contexts of government interventions to govern quantum threats. We summarize the identified practices in the six main strategies in Table 1.

### Partnerships

The most prominent practice of assemblages in partnerships is the first practice-forging alignments. The observed diversity of *Partnerships*, including government–government, internal-government, government–industry, and academia–industry, as well as through standardization projects, seem to indicate a forging of alignments with not only communities of experts, but with current and future actors. Although other partnership combinations are observed, the *triple helix* of university–industry–government (35) is not prominently seen in these linkages, except in [US.7], [US.8], and [UK.5].<sup>3</sup> Generally, the UK-related documents show that the state seems to place an emerging importance on the triple helix in addressing the quantum threat. Forging alignments within existing defence cooperation, is identified as an option. This is apparent in the mention of government–industry cooperation.

### Infrastructure

The multiple linkages within *Infrastructure*, especially through risk assessment and migration plans, also seem to provide a path to forge alignments (general practice 1) between multiple actors beyond states. This may function as a way to open up new pathways. The specific focus on critical and IT infrastructure may also shed light on navigating public–private cooperation on infrastructure protection.

Risk assessments and mitigation plans also seem to be important from an economic perspective, as the many links (indicated

by the yellow dots) show. In particular [US.8] indicates that partnerships with other states, as well as internal governmental departments and agencies, is part of infrastructure protection as well as anticipating threats. In this document, we see linkages carved out for specific actors and their expertise. These linkages may indicate a convergence of paths for cooperation—but also of exclusion. For example, participants in some partnerships or certain projects include only government–government, internal-government, government–industry, and academia–industry, or all three in combination.

### Education

Authorizing knowledge (general practice 3) is best encapsulated within the purpose of *Education*. On the one hand, expertise is established by funding research through grants, on the other hand, the gathered knowledge is transferred to, e.g. decision-makers through workshops and similar. We identify this as a primary way to control the uncertainty associated with the uses of quantum technologies, especially malicious users. By seeking to both understand the threat as well as provide information about it, state actors seek to broaden linkages in their favour, while defining the parameters of future co-operation.

Another identified practice is forging alignments (general practice 1) as the linkages between *Education*, *Economy*, *Standardization*, *Infrastructure*, and *Partnerships* are prominent with multiple actors identified within raising awareness projects. Raising awareness could be seen as a way to identify other actors to include within future expert communities. This may also serve to specify, prioritize a specific area of expertise, and therefore *make* a certain body of expertise.

### Defence

*Defence* remains siloed in attempts to engage in interventions to authorize knowledge (general practice 5). The nature of defence and trust between actors may play a role in limiting the possible diversity of associated actors as well as sharing knowledge they produce through communities of experts. The apparent lack of linkages with other purpose areas and the focus on protecting government data and communications may indicate a contestation point in strategies to address post-quantum threats. It could also be due to the sensitive nature of this topic and the lack of unclassified information available on this topic.

### Standardization

The reassembling of assemblages (general practice 6) involves the re-positioning and transposing of objectives and meanings onto ex-

3 In addition, [CA.13] mentions that some organizations, such as *quantum-safe.ca*, aim to establish industry–government cooperation through such forums as the Canadian Forum for Digital Infrastructure Resilience (CFDIR).

isting assemblages. *Standardization* of cryptographic algorithms and the post-quantum transition using hybrid algorithms configure controllable and knowable solutions to the quantum threat. In this case, reassembling projects are not a practise of downsizing or decentralizing, as Li (11) argues is associated with a neoliberalist focus on promoting market efficiency. Instead, although the intersections between *Economy*, *Partnerships*, *Education*, and *Infrastructure* have market alignments, the reassembling piece seems to focus more on changing old meanings and *ways of doing* in cryptographic algorithms and preserving the existing public-key infrastructure.

NIST's PQ project in particular functions as a reassembling piece, whereby governmental interventions forges new connections from a variety of technical and non-technical elements, all based in a strategy to prepare for the quantum threat. This intervention can be seen as an institutional anchoring whereby standardization is an act of governance. By defining the contours of the threat and the solution, standardization shapes both the productions of the threat and the solution, including who is able to participate in the process. By crafting standardization as a linking practice, it renders the uncertainties about the threat as controllable, regulated, and therefore more governable. In addition, it also authorizes knowledge (general practice 3).

NIST's PQ standardization of digital signature schemes, PKEs and KEMs can be seen as being at the centre of the post-quantum transition of the partners we analysed. While the document itself [US.4] focuses on the primary purpose of *Standardization* and does only link with *Infrastructures*, implicitly it is at the core of many other strategies and impacts the decisions and action of many players other than NIST, as summarized for the most important documents that explicitly mention to *Synchronize With the NIST PQ Project* such as [CA.10, EU.15, US.8]. Further, the academic research community is strongly involved in the project as can also be seen in explicit *Funding research to evaluate standards* [EU.17]. In addition, the submitters of algorithms to the NIST PQ standardization are affiliated very diversely; with universities, research institutes, and corporations. Furthermore, in practice, NIST seems to monitor closely the discussions in the post-quantum research community, and stimulates and participates in it actively using open discussion forums, white papers, workshops, and participation of their employees at academic conferences. It appears that NIST plans to mirror this interactive process regarding deciding on future transition strategies, as they (in partnership with NCCoE and Dakota Consulting) published a white paper [US.8] based on the NIST PQ project and discussing comprehensively the challenges of the post-quantum transition and asking for comments from the post-quantum community. Observing the cooperation of NIST with the academic community but also within the academic community (submitters come from a larger range of different affiliations both in academia and industry), forging alignments (general practice 1) plays an important role in this strategy.

In addition, the strategy to *Use hybrid approach* as a transition strategy can be identified with two different general practices of assemblages. As a reminder, hybrid approach means to combine a classical (quantum-vulnerable) algorithm that has been used for decades with a post-quantum algorithm of the same kind (e.g. combining two different signature schemes). The advantage is that our nowadays established security guarantees are still given, while security against quantum attackers is added. This way the uncertainty of whether the newer post-quantum algorithms are secure is overcome since these hybrid schemes are at least as secure as currently used algorithms. In this sense, to *Use hybrid approach* can be categorized as the practice of rendering technical (general practice 2) as the process of first

switching to hybrid approaches seems to be a more manageable result. Interestingly, using a hybrid approach can also be seen as a practice to manage failures and contradiction (general practice 4), the contradiction here being the urgency to transition on the one hand and the uncertainty about the security of new algorithms on the other. Using hybrid approaches, the risk of failing (i.e. that security of a system is broken because the post-quantum alternatives turn out not to be secure) is decreased.

## Economy

The lack of explicitly economic-focused and related strategies to address the quantum threat (leading to no identified general practices) may indicate the already integrated nature of economic objectives within government interventions. It also makes it more difficult to definitively identify a practise of assemblages. This is because government interventions are nested within a neoliberalist framework, whereby market optimization and market rationality are applied to all aspects of life, including within policies, strategies, and schemes. It stands in contrast to the large economic investment for quantum technology or quantum cryptography such as QKD that we identified in the documents (but these are out of the scope of this article). We see investment in an emerging technology without equal investment in protecting against the threats of this technology critical.

## Discussion

In our assessment of the relations between the multiple wholes of post-quantum cryptographic assemblages, we identify major trends among the six primary purposes, mainly that partnerships through formal and informal channels and through largely preexisting cooperation are a way that states attempt to configure, territorialize, and reassemble the quantum space. Standardization projects, especially the NIST PQ project, are also a way for states to reassemble post-quantum cryptographic assemblages to make it easier to govern and account for future threats. This type of government intervention also has governance implications as it places emphasis on multi-stakeholder interactions, and regulation, and ascribes legitimacy to certain actors, while reassembling expertise within an assemblage.

In our analysis, we have not identified or discussed the political and anti-political linkages within assemblages. However, we have shown how the management of the perceived quantum threat has taken shape in policy and strategy documents from traditional defence allies.

It is worth drawing attention to the observation that there were few notable strategies for addressing the quantum threat from Australia and New Zealand. This may be due to the sensitive and secretive nature of this topic and may not necessarily reflect the actual government interventions. In this paper, we only analyse publicly available information and assume that the *full picture* may lie within classified documentation and therefore is beyond the scope of this paper.

## Conclusion

The linkages within post-quantum cryptographic assemblages provide spaces to look for cooperation between a variety of actors and objectives. Overall, our analysis indicates that a number of practises of assemblages are being used to make linkages between knowledge and actors and their objectives, namely governmental interventions, specifically forging alignments, authorizing knowledge, and reassembling. These are made visible through creating new partnerships, un-

derstanding the quantum threat through education, and regulating it through standardization. These are governance strategies that may have implications for cooperation between actors involved in creating and navigating these post-quantum cryptographic assemblages. Without overemphasizing or privileging a state-focused perspective on addressing the quantum threat, it is clear that there are differences between actors and their approaches. A focus on *Education* through research funding, *Standardization*, *Infrastructure*, and *Partnerships* stands out through the linkages within the assemblage. The lack of *Defence* focus and a clearly articulated focus on *Economy* may indicate a point of contestation or specific contextual understanding of the threat. A deeper exploration into the reasons for this lack of foci may provide an interesting area for future research. It may be worthwhile to extend this study to then also include QKD and quantum cryptography.

As states begin to understand the contours of the post-quantum threat, the opportunities for cooperation take shape through a variety of preexisting, informal and formal channels, mainly through standardization. As traditionally cooperating allies, especially on defence issues, Australia, Canada, EU, New Zealand, UK, and USA will need to find linking wholes among the post-quantum cryptographic assemblages.

Future research on this topic might include expanding a study to include other traditionally cooperating states and novel public-private partnerships. There are also future research opportunities to expand on the political and anti-political linkages within assemblages, or explore why they were not inherently visible in our study. Additionally, future studies could place more focus on identifying the practises of how the quantum threat is rendered technical. This could be examined through other documents, aside from policies and strategies, with a focus on exploring the narratives and discourses, and even visual representations that frame threats. Managing the failures, specifically the failure to create governable linkages or to address the quantum threat, is also an interesting opportunity for future scholarship endeavours.

There are several pathways to follow in order to address the quantum threat. Cooperation between multiple actors is an important part of this project. For industry, academia, governments, and other actors, this may involve continuing to understand the technology and the associated threats. Leveraging existing pathways and expertise, and building trusted new ones will continue to require collaboration between actors. Leveraging expertise in the private sector and academia may prove to be a government intervention for defence cooperating states beyond raising awareness about threats.

## List of abbreviations

ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
IR	International relations
IT	Information technology
KEM	Key encapsulation mechanism
NATO	North Atlantic Treaty Organization
NCCoE	National Cybersecurity Center of Excellence
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PDF	Portable document format
PKE	Public-key encryption
PQ	Post-quantum
QKD	Quantum key distribution

R&D	Research and development
RSA	Rivest–Shamir–Adleman
TLS	Transport layer security

## List of primary sources

- [AU.1] ACSC, 2019, [https://www.cyber.gov.au/sites/default/files/2019-03/ISM\\_22\\_Guidelines\\_for\\_Using\\_Cryptography.pdf](https://www.cyber.gov.au/sites/default/files/2019-03/ISM_22_Guidelines_for_Using_Cryptography.pdf), accessed on 2021-07-07.
- [AU.2] CSIRO, 2020, <https://www.csiro.au/en/work-with-us/services/consultancy-strategic-advice-services/csiro-futures/futures-reports/quantum>, accessed on 2021-07-07.
- [AU.3] CSIRO, 2020, <https://www.csiro.au/en/news/News-releases/2020/Researchers-develop-worlds-most-efficient-quantum-safe-and-privacy-preserving-blockchain-protocol>, accessed on 2021-07-09.
- [AU.4] DoD, 2020, <https://www1.defence.gov.au/strategy-policy/strategic-update-2020>, accessed on 2021-07-08.
- [AU.5] Department of Home Affairs, 2020, <https://www1.defence.gov.au/strategy-policy/strategic-update-2020>, accessed on 2021-07-10.
- [CA.1] DND, 2017, <https://www.canada.ca/content/dam/dnd-mdn/documents/reports/2018/strong-secure-engaged/canada-defence-policy-report.pdf>, accessed on 2021-07-07.
- [CA.2] CSE, 2017, <https://cyber.gc.ca/sites/default/files/publications/itsb-00-017-eng.pdf>, accessed on 2021-07-07.
- [CA.3] CFC, 2018, <https://www.cfc.forces.gc.ca/259/290/308/192/begin.pdf>, accessed 2021-07-09.
- [CA.4] DND/CAF, 2018, [https://www.canada.ca/content/dam/dnd-mdn/documents/reports/DGM-61120-DD8\\_DNDCAF\\_QuantumSTStrategy\\_EN\\_v3.pdf](https://www.canada.ca/content/dam/dnd-mdn/documents/reports/DGM-61120-DD8_DNDCAF_QuantumSTStrategy_EN_v3.pdf), accessed on 2021-07-10.
- [CA.5] PSC, 2018, <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scrtrg/ntnl-cbr-scrtrg-en.pdf>, accessed on 2021-07-09.
- [CA.6] GoC, 2019, <https://www.canada.ca/en/innovation-science-economic-development/news/2019/04/government-of-canada-partners-with-digital-industries-to-invest-in-ground-breaking-technology-and-businesses.html>, accessed on 2021-07-08.
- [CA.7] CSE, 2019, <https://www.cyber.gc.ca/sites/default/files/publications/itsb-127-en.pdf>, accessed on 2021-07-07.
- [CA.8] FedDev Ontario, 2019, <https://www.feddevontario.gc.ca/eic/site/723.nsf/eng/02511.html?OpenDocument>, accessed on 2021-07-10.
- [CA.9] PSC, 2019, <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scrtrg-2019/ntnl-cbr-scrtrg-2019-en.pdf>, accessed on 2021-07-07.
- [CA.10] CSE, 2020, <https://www.cyber.gc.ca/sites/default/files/publications/ITSE.00.017.pdf>, accessed on 2021-07-07.
- [CA.11] NSERC, 2020, [https://www.nserc-crsng.gc.ca/Professors-Professeurs/RPP-PP/Canada-UK\\_eng.asp](https://www.nserc-crsng.gc.ca/Professors-Professeurs/RPP-PP/Canada-UK_eng.asp), accessed on 2021-07-09.
- [CA.12] CCCS, 2020, [https://www.uoguelph.ca/ccs/system/files/CCS\\_USING%20ENCRYPTION%20TO%20KEEP%20YOUR%20SENSITIVE%20DATA%20SECURE.pdf](https://www.uoguelph.ca/ccs/system/files/CCS_USING%20ENCRYPTION%20TO%20KEEP%20YOUR%20SENSITIVE%20DATA%20SECURE.pdf), accessed on 2021-07-07.

- [CA.13] CFDIR, 2020, <https://www.ic.gc.ca/eic/site/smt-gst.nsf/en/sf11618.html>, accessed 2021-07-10.
- [CA.14] CCCS, 2021, <https://cyber.gc.ca/en/cyber-centres-summary-review-final-candidates-nist-post-quantum-cryptography-standards>, accessed on 2021-07-08.
- [CA.15] CSE, 2021, <https://cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-annual-report-2020-2021>, accessed on 2021-07-10.
- [EU.1] ETSI, <https://www.etsi.org/technologies/quantum-safe-cryptography>, accessed on 2021-07-07.
- [EU.2] European Commission, 2016, [https://qt.eu/app/uploads/2018/04/93056\\_Quantum-Manifesto\\_WEB.pdf](https://qt.eu/app/uploads/2018/04/93056_Quantum-Manifesto_WEB.pdf), accessed on 2021-07-07.
- [EU.3] ETSI, 2016, [https://www.etsi.org/deliver/etsi\\_eg/203300\\_203399/203310/01.01.01\\_60/eg\\_203310v010101p.pdf](https://www.etsi.org/deliver/etsi_eg/203300_203399/203310/01.01.01_60/eg_203310v010101p.pdf), accessed on 2021-07-08.
- [EU.4] ETSI, 2017, [https://www.etsi.org/deliver/etsi\\_gr/QSC/001\\_099/006/01.01.01\\_60/gr\\_QSC006v010101p.pdf](https://www.etsi.org/deliver/etsi_gr/QSC/001_099/006/01.01.01_60/gr_QSC006v010101p.pdf), accessed on 2021-07-09.
- [EU.5] ETSI, 2017, [https://www.etsi.org/deliver/etsi\\_tr/103500\\_103599/103570/01.01.01\\_60/tr\\_103570v010101p.pdf](https://www.etsi.org/deliver/etsi_tr/103500_103599/103570/01.01.01_60/tr_103570v010101p.pdf), accessed on 2021-07-07.
- [EU.6] ENISA, 2018, <https://www.enisa.europa.eu/news/enisa-news/getting-ready-for-the-fifth-enisa-forth-nis-summer-school>, accessed on 2021-07-10.
- [EU.7] European Commission, 2018, <https://digital-strategy.ec.europa.eu/en/news/pqcrypto-eu-funded-project-success-story>, accessed on 2021-07-08.
- [EU.8] European Commission, 2018, [https://publications.jrc.ec.europa.eu/repository/bitstream/JRC107386/jrc\\_report\\_quantumcommunications.pdf](https://publications.jrc.ec.europa.eu/repository/bitstream/JRC107386/jrc_report_quantumcommunications.pdf), accessed on 2021-07-10.
- [EU.9] ENISA, 2019, <https://www.enisa.europa.eu/news/enisa-news/knowledge-building-on-cryptography-for-eidas-supervisory-bodies>, accessed on 2021-07-07.
- [EU.10] ETSI, 2019, [https://www.etsi.org/deliver/etsi\\_tr/103600\\_103699/103618/01.01.01\\_60/tr\\_103618v010101p.pdf](https://www.etsi.org/deliver/etsi_tr/103600_103699/103618/01.01.01_60/tr_103618v010101p.pdf), accessed on 2021-07-08.
- [EU.11] European Commission, 2020, <https://ec.europa.eu/programmes/horizon2020/en/h2020-section/future-and-emerging-technologies>, accessed on 2021-07-09.
- [EU.12] ENSIA, 2020, <https://www.enisa.europa.eu/news/enisa-news/telecom-security-authorities-meeting-in-brussels>, accessed on 2021-07-09.
- [EU.13] ETSI, 2020, [https://www.etsi.org/deliver/etsi\\_ts/103700\\_103799/103744/01.01.01\\_60/ts\\_103744v010101p.pdf](https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.01.01_60/ts_103744v010101p.pdf), accessed on 2021-07-07.
- [EU.14] European Commission, 2020, <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade>, accessed on 2021-07-09.
- [EU.15] ENISA, 2021, <https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation>, accessed on 2021-07-08.
- [EU.16] ERC, 2021, <https://cordis.europa.eu/project/id/644729>, accessed on 2021-07-08.
- [EU.17] ERC, 2021, <https://cordis.europa.eu/project/id/805031>, accessed on 2021-07-07.
- [NZ.1] MBIE, <https://www.mbie.govt.nz/science-and-technology/science-and-innovation/funding-information-and-opportunities/investment-funds/catalyst-fund/catalyst-strategic-the-cyber-security-research-programme/>, accessed on 2021-07-08.
- [NZ.2] Minister of Defence, 2018, <https://www.defence.govt.nz/assets/Uploads/8958486b29/Strategic-Defence-Policy-Statement-2018.pdf>, accessed on 2021-07-08.
- [NZ.3] Department of the Prime Minister and Cabinet, 2019, <https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf>, accessed on 2021-07-09.
- [UK.1] UKNQTP, 2015, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/414788/Strategy\\_QuantumTechnology\\_T15-080\\_final.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/414788/Strategy_QuantumTechnology_T15-080_final.pdf), accessed on 2021-07-07.
- [UK.2] MOD, 2019, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/830139/20190829-DTF\\_FINAL.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/830139/20190829-DTF_FINAL.pdf), accessed on 2021-07-08.
- [UK.3] NCSC, 2020, <https://www.ncsc.gov.uk/pdfs/whitepaper/quantum-security-technologies.pdf>, accessed on 2021-07-09.
- [UK.4] MOD, 2020, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/927708/20201019-MOD\\_ST\\_Strategy\\_2020\\_v1-23.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/927708/20201019-MOD_ST_Strategy_2020_v1-23.pdf)
- [UK.5] NCSC, 2020, <https://www.ncsc.gov.uk/pdfs/whitepaper/preparing-for-quantum-safe-cryptography.pdf>, accessed on 2021-07-09.
- [UK.6] Department for Digital, Culture, Media and Sport, 2020, <https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy>, accessed on 2021-07-08.
- [UK.7] HGM, 2021, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/971983/Defence\\_and\\_Security\\_Industrial\\_Strategy\\_-\\_FINAL.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971983/Defence_and_Security_Industrial_Strategy_-_FINAL.pdf), accessed on 2021-07-09.
- [UK.8] HMG, 2021, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/975077/Global\\_Britain\\_in\\_a\\_Competitive\\_Age\\_the\\_Integrated\\_Review\\_of\\_Security\\_Defence\\_Development\\_and\\_Foreign\\_Policy.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age_the_Integrated_Review_of_Security_Defence_Development_and_Foreign_Policy.pdf), accessed on 2021-07-10.
- [UK.9] MOD, 2021, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/974661/CP411\\_-Defence\\_Command\\_Plan.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/974661/CP411_-Defence_Command_Plan.pdf), accessed 2021-07-08.
- [UK.10] GDS, 2021, <https://gds.blog.gov.uk/2021/05/20/government-digital-service-our-strategy-for-2021-2024/>, accessed on 2021-07-09.
- [US.1] NCCoE NIST, <https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography>, accessed on 2021-07-08.
- [US.2] CRSC NIST, 2015, <https://csrc.nist.gov/events/2015/workshop-on-cybersecurity-in-a-post-quantum-world>, accessed on 2021-07-06.
- [US.3] NSA, 2015, [https://www.nsa.gov/ia/programs/suiteb\\_cryptography/index.shtml](https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml), accessed on 2021-07-08.
- [US.4] CSRC NIST, 2017, <https://csrc.nist.gov/projects/post-quantum-cryptography>, accessed on 2021-07-08.
- [US.5] The White House, 2018, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>, accessed on 2021-07-08.



- [US.6] DoD, 2018, <https://dod.defense.gov/Portals/1/Document%20Publications/2018-National-Defense-Strategy-Summary.pdf>, accessed on 2021-07-09.
- [US.7] DHS, 2020, [https://www.dhs.gov/sites/default/files/publications/final\\_emerging\\_technologies\\_quantum\\_report\\_1.pdf](https://www.dhs.gov/sites/default/files/publications/final_emerging_technologies_quantum_report_1.pdf), accessed on 2021-07-08.
- [US.8] CSRC NIST, 2021, <https://csrc.nist.gov/publications/detail/white-paper/2021/04/28/getting-ready-for-post-quantum-cryptography/final>, accessed on 2021-07-09.

## Acknowledgements

The authors would like to thank Aniska Graver and Kaitlyn Csenkey for diligent research assistance and editing provided during the course of this project, respectfully. The authors would also like to thank Dr. Michele Mosca who provided valuable insights and feedback on earlier versions of this paper. In addition, we thank the anonymous reviewers for their constrictive feedback on earlier versions of this paper.

## Author contributions

Kristen Csenkey (Conceptualization, Data curation, Formal analysis, Funding acquisition, Methodology, Project administration, Supervision, Visualization, Writing – original draft, Writing – review & editing), Nina Bindel (Conceptualization, Data curation, Formal analysis, Project administration, Supervision, Visualization, Writing – original draft, Writing – review & editing).

## Conflict of interest statement

None declared.

## Funding

This work has been supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery grant [RGPIN-2016-05146] to N.B.; NSERC Discovery Accelerator Supplement grant [RGPIN-2016-05146] to N.B.; National Research Council of Canada (NRC) [program 927517] to N.B.; Public Works and Government Services Canada [and Contract 2L 165-180499/001/sv, 'PQC Analysis'] to N.B.; and the Canadian Department of National Defence (DND) through a Mobilizing Insights in Defence and Security (MINDS) Targeted Engagement Grant (TEG) awarded in 2020 to K.C.

Moreover, this work has been supported by the University of Waterloo Institute for Quantum Computing (IQC); IQC is supported in part by the Government of Canada and the Province of Ontario.

## References

- Bernstein DJ, Buchmann J, Dahmen E. *Post-Quantum Cryptography*. Berlin: Springer, 2009.
- Bindel N, Csenkey K. How Canada can prepare for the quantum threat. *CGAI Policy Perspective*. Ottawa: Canadian Global Affairs Institute, 2021.
- Csenkey K, Bindel N, Gold J., et al. *Simplifying Emerging Technologies – Risks and How to Mitigate Them*. Waterloo: Balsillie School of International Affairs, 2020.
- Bindel N, Csenkey K. *Governing the future(s) of emerging technologies*. NAADSN Quick Impact Reports. North American and Arctic Defence and Security Network (NAADSN), 2021
- Deleuze G, Guattari F. *A Thousand Plateaus*. Minneapolis, MN: University of Minnesota Press, 1987.
- DeLanda M. *A New Philosophy of Society: Assemblage Theory and Social Complexity*. London: Bloomsbury Publishing, 2006.
- Collier J. Cyber security assemblages: a framework for understanding the dynamic and contested nature of security provision. *Politics Gov* 2018;6:13–21.
- Stevens C. Assembling cybersecurity: the politics and materiality of technical malware reports and the case of Stuxnet. *Contemp Secur Policy* 2020;41:129–52.
- Egloff FJ, Cavelti MD. Attribution and knowledge creation assemblages in cybersecurity politics. *J Cybersecur* 2021;7:114–20.
- Liebetrau T, Christensen KK. The ontological politics of cyber security: emerging agencies, actors, sites, and spaces. *Eur J Int Secur* 2021;6:25–43.
- Murray Li T. Practices of assemblage and community forest management. *Econ Soc* 2007;36:263–93.
- Puar JK. *Terrorist Assemblages: Homonationalism in Queer Times*. Durham, NC: Duke University Press, 2007.
- Abrahamsen R, Williams MC. Security beyond the state: global security assemblages in international politics. *Int Political Sociol* 2009; 1:1–17.
- Hauffer V. Producing global governance in the global factory: markets, politics, and regulation. *Glob Policy* 2018;9:114–20.
- Allen J. Powerful assemblages? *Area* 2011;43(2):154–7.
- Sassen S. *Territory, Authority, Rights: From Medieval to Global Assemblages*. Princeton, NJ: Princeton University Press, 2008.
- Lake DA. Rightful rules: authority, order, and the foundations of global governance. *Int Stud Q* 2010;54:587–613.
- Koppell JG. *World Rule: Accountability, Legitimacy, and the Design of Global Governance*. Chicago, IL: University of Chicago Press, 2010.
- Der Derian J, Wendt A. “Quantizing international relations”: the case for quantum approaches to international theory and security practice. *Secur Dialogue* 2020;51:399–413.
- Der Derian J. *Virtuous War: Mapping the Military-Industrial-Media-Entertainment-Network*. London: Routledge, 2009.
- Der Derian J. Quantum diplomacy, German–US relations and the psycho-geography of Berlin. *Hague J Dipl* 2011;6:373–92.
- Der Derian J. A quantum of insecurity. *New Perspect* 2019;27:13–27.
- Zanotti L. *Ontological Entanglements, Agency and Ethics in International Relations: Exploring the Crossroads*. London: Routledge, 2018.
- Katz J, Lindell Y. *Introduction to Modern Cryptography*, 2nd edn. Boca Raton, FL: CRC Press, 2014.
- Kelly J. A preview of bristlecone, Google’s new quantum processor. <https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html>. (23 July 2018, date last accessed).
- Gidney C, Ekerå M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum* 2021;5:433.
- Gibney E. Quantum gold rush: the private funding pouring into quantum start-ups. <https://www.nature.com/articles/d41586-019-02935-4>. (7 July 2021, date last accessed).
- Mosca M, Piani M. Quantum Threat Timeline Report. *Global Risk Institute in Financial Services(GRI)*, 2021. <https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/>. (17 August 2022, date last accessed).
- Vermeer MJD, Peet ED. *Securing Communications in the Quantum Computing Age*. RAND Corporation. [https://www.rand.org/pubs/research\\_reports/RR3102.html](https://www.rand.org/pubs/research_reports/RR3102.html). (8 July 2021, date last accessed).
- Mosca M. Cybersecurity in an era with quantum computers: will we be ready? *IEEE Secur Priv* 2018;16:38–41.
- Bindel N, Brendel J, Fischlin M., et al. Hybrid key encapsulation mechanisms and authenticated key exchange. In: Ding J, Steinwandt R (eds.), *Post-Quantum Cryptography – 10th International Conference, PQCrypto 2019. Lecture Notes in Computer Science*. Cham: Springer, 2019, 206–26.
- Bindel N, Herath U, McKague M., et al. Transitioning to a quantum-resistant public key infrastructure. In: Lange T, Takagi T (eds.), *Post-Quantum Cryptography – 8th International Workshop, PQCrypto 2017. Lecture Notes in Computer Science*. Cham: Springer, 2017, 384–405.

33. Smith III FL. Quantum technology hype and national security. *Secur Dialogue* 2020;51:499–516.
34. Kung J, Fancy M. A quantum revolution: report on global policies for quantum technology. 2021. <https://cifar.ca/wp-content/uploads/2021/04/quantum-report-EN-10-accessible.pdf>. (11 March 2022, date last accessed).
35. Leydesdorff L, Etzkowitz H. The triple helix as a model for innovation studies. *Sci Public Policy* 1998;25:195–203.