UNIVERSITY OF SOUTHAMPTON

Faculty of Engineering and Physical Sciences

School of Electronics and Computer Science

Shaping the Quantum Internet

Evidence of US–Chinese strategic competition over quantum technologies from interviews and patent data ERGMs

by Juljan Krause

March 2023

ORCID ID: 0000-0002-1956-6720

Thesis for the Degree of Doctor of Philosophy in Web Science:

Computer Science and International Relations

Abstract

This thesis is the first study to investigate how the strategic competition over innovative technologies between the United States and China shapes the emergence of the quantum internet. A quantum internet will connect first-generation quantum computers over secure quantum channels to provide and distribute at scale a new type of compute resource that promises a significant speedup of compute power and better security. The US and China consider emerging technologies in general, and quantum internet technologies in particular, of utmost importance in their efforts to contain their strategic rival. This thesis investigates how the quantum internet is being framed in security terms in this aggravating rivalry, and what this means for the future of the internet. As warnings of the dangers of a fragmented internet increase, the thesis maps out the significant obstacles on the way to maintaining interoperability.

In an original contribution to research methods, this thesis is the first application of ERGMs to the analysis of patent data and their citation trees in the domain of quantum internet technologies. It conducts a statistical analysis of 4,200 patent family records and the 10,000+ patents they cite. Following a mixed-method approach, this thesis also evaluates a corpus of interviews with GCHQ, the British government and several internet governance and China experts.

It finds robust evidence for two separate and siloed quantum research programmes in the US and China. These programmes are further characterised internally by significant homophily and the preferential treatment of domestic industries. Findings further suggest a tentative edge for China in the domain of quantum communication, an important technology for realising the quantum internet. China's significant progress in developing components for a quantum internet is found to have great potential to give its increasingly assertive stance on internet governance additional momentum.

The thesis argues that China should be expected to try and offer what may be called ‘quantum patronage’: a complete package of quantum technology stacks and appropriate standards in line with its recent ‘China Standards 2035’ plan. Quantum patronage may offer hitherto non-aligned countries critical technologies to secure their communication and build up quantum compute resources in exchange for a commitment to allegiance and strategic alignment.

The empirical findings of this thesis inform the building blocks of a coalitional game theory model of standards-finding for the quantum internet. It recommends the US make side payments to China as compensation for easing its strategic ambitions, in particular around its ‘New IP’ many-nets proposal. The model is a first step towards designing a mechanism for finding a global standard for the future quantum internet. If the fragmentation of the quantum internet is to be avoided, the US and its allies should be prepared to incur new and unexpected political and financial costs to ensure long-term interoperability. Given the empirical evidence that this thesis presents, which points towards fragmentation, this could be a price worth paying for an open quantum internet.

Declaration of Authorship

Print name: Juljan Krause

Title of thesis: Shaping the Quantum Internet: evidence of US–Chinese strategic competition over quantum technologies from interviews and patent data ERGMs

I declare that this thesis and the work presented in it are my own and has been generated by me as the result of my own original research.

I confirm that:

1. This work was done wholly while in candidature for a research degree at this University;

2. Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated [not applicable];

3. Where I have consulted the published work of others, this is always clearly attributed;

4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;

5. I have acknowledged all main sources of help;

6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself [not applicable];

7. None of this work has been published before submission.

Acknowledgements

I would like to acknowledge both the Engineering and Physical Sciences Research Council's Centre for Doctoral Training in Web Science Innovation and the Heinrich Boell Foundation in Berlin for their financial support. I am indebted to both in making this PhD possible.

I would like to thank my supervisors, Profs Mark Weal and Christian Enemark at the University of Southampton for their excellent steer, oversight and continuous, thoughtful guidance to this thesis. And, above all, for their inexhaustible patience: a fair number of deadlines for draft chapters were missed during my time with the Web Science CDT. I must also thank Alison Tebbutt and the ECS programme team for all their administrative support throughout. I want to extend my thanks to Prof Susan Halford at the University of Bristol for earlier sociological reflections on the intersections of power and technology. While they have not found their way into the final version of the thesis, they were paramount for guiding my thinking about the forces that are shaping the quantum internet. And any acknowledgements would be incomplete without saying thank you to Prof Dame Wendy Hall for several inspiring discussions about the future of the Web on trips to China and Singapore.

At the Heinrich Boell Foundation in Berlin I must thank Dr Sevilay Karaduman and her team for their continuous support, and the Head of the Foreign and Security Policy Division, Giorgio Franceschini, for excellent discussions of the security implications of emerging technologies. The Boell Foundation's learning and development opportunities have been of great support.

I am grateful to my good friend, study buddy and Web Science veteran Dr Ashton Kingdon for invaluable advice and support from day one of our journey together towards our PhDs. Needless to say, she got there first. Massive thanks to my parents Annette Hartmann and Lutz Kaiser for their support. Finally, and most importantly, I am immensely grateful to my partner Murat Adash, for encouraging me to go back to university after many years 'in the wild', and for keeping me sane (I hope) throughout this entire time.

Contents

List of Figures

List of Tables

List of Abbreviations

AFRINIC	Internet Numbers Registry for Africa
AfTLD	African Top Level Domain Association
AI	Artificial Intelligence
ALAC	At-Large Advisory Committee
APNIC	Asia Pacific Internet Address Registry
APTLD	Asia Pacific Top Level Domain Name Association
ARIN	American Registry for Internet Numbers
ARPANET	Advanced Research Projects Agency Network
ASO	Address Supporting Organization
AUKUS	‘Australia, United Kingdom, United States’ alliance
BoE	Bank of England
ccNSO	Country Code Names Supporting Organization
ccTLD	country code top-level domain
CENTR	Association of European ccTLD Registries
CEO	Chief Executive Officer
CSIS	Center for Strategic and International Studies
CPC	Cooperative Patent Classification
DoD	US Department of Defense
EPO	European Patent Office
EPSRC	Engineering and Physical Sciences Research Council

ERGM	Exponential Random Graph Model
EU	European Union
EuroDIG	European Dialogue on Internet Governance
EuroQCI	European Quantum Communication Infrastructure
FCC	US Federal Communications Commission
FDI	Foreign Direct Investment
FEPS	Faculty of Engineering and Physical Sciences
GAC	Governmental Advisory Committee
GCHQ	Government Communications Headquarters
GNSO	Generic Names Supporting Organization
GPI	Global Patent Index
gTLD	generic top-level domain
HDMI	High Definition Multimedia Interface
HMRC	HM Revenue & Customs
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum

IoT	Internet-of-Things
IP	Internet Protocol
IPC	International Patent Classification
IPO	Initial Public Offering
IPR	Intellectual Property Rights
IR	International Relations
IRTF	Internet Research Task Force
ISO	International Organization for Standardization
ISOC	Internet Society
ITU	International Telecommunication Union
LACNIC	Latin American and Caribbean Internet Addresses Registry
LACTLD	Latin American and Caribbean Association of ccTLDs
MFA	Multi-Factor-Authentication
MIDI	Musical Instrument Digital Interface
ML	Machine Learning
MMR	Mixed-Method Research
MoD	UK Ministry of Defence
MS	Microsoft
NASA	National Aeronautics and Space Administration
NFC	Near-Field Communication
NHS	National Health Service

NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTC	US National Science and Technology Council
PAN	Personal Area Network
PC	Personal Computer
PDF	Portable Document Format
PTI	Public Technical Identifiers
QCaaS	Quantum Computing as a Service
QISG	Quantum internet security governance
QKD	Quantum Key Distribution
QUESS	Quantum Experiments at Space Scale
RCA	Radio Corporation of America
RIPE	Réseaux IP Européens
RIRs	Regional Internet Registries
RSA	Rivest–Shamir–Adleman
RSSAC	Root Server System Advisory Committee
RUSI	Royal United Services Institute
SACs	Systems with Autonomous Capabilities
SEPs	Standard Essential Patents
SIPO	China's State Intellectual Property Office
SMEs	Small and Medium-Sized Enterprises

SSAC	Security and Stability Advisory Committee
TCP/IP	Transmission Control Protocol/Internet Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network
WIPO	World Intellectual Property Organization
WSN	Wireless Sensor Network
W3C	World Wide Web Consortium
XLR	External Line Return

‘Quantum computing is interesting, but it requires a real quantum internet.’

Respondent A, Singapore.

Chapter 1

Introduction

This thesis is the first study to investigate how the strategic competition over innovative technologies between the United States and China shapes the emergence of the quantum internet. A quantum internet will connect first-generation quantum computers that have only limited capabilities over secure quantum channels to provide and distribute at scale a new type of compute resource that promises a significant speedup of compute power and better security. The US and China consider emerging technologies in general, and quantum internet technologies in particular, of utmost importance in their efforts to contain their strategic rival.

The two powers are increasingly competing over internet infrastructure and technologies, which reflects in standards and governance competition over internet architecture and protocols. The ways in which the quantum internet is going to shape up, both in terms of its technological affordances and the standards that govern it, are likely to have significant repercussions for the rapidly evolving international security landscape.

This thesis has its disciplinary home in Web Science. Web Science is the study of the World Wide Web as a complex sociotechnical system (Berners-Lee et al. 2006, Hendler & Hall 2016, O'Hara & Hall 2014) that is shaped by intersecting technological, social and political forces. The same is true for the World Wide Web's enabling infrastructure: the internet.[1] The internet, the 'network of networks', has now arrived at a critical juncture. Tasked to accommodate waves of innovation in Internet of Things (IoT), Artificial Intelligence (AI) and autonomous systems technologies, calls for an upgrade to the internet's infrastructure as well as the standards that govern it have grown. As a discipline, Web Science must investigate how the internet is going to change–the Web being the most important application layer that sits 'on top' of it. Changes to internet architecture and protocols will affect the Web to no small degree.

In light of the darkening outlook for international security at present, this thesis enquires into possible quantum internet futures. How is the emergence of the quantum internet being shaped by the strategic competition between the US and China? As further developed below, the term 'shaping' is to capture efforts to determine technical specifications as well as standards and governance models. This introductory chapter is organised as follows. Section 1.1 provides some background to the internet and Chinese ambition to help frame the research questions. Section 1.2 builds up the set of research questions that this thesis seeks to answer. Section 1.3 provides a summary overview of the thesis as whole in outlines of the chapters that follow.

[1] The internet is a global network that connects a vast collection of subnetworks which communicate over the TCP/IP protocol suite. For a history of its evolution from the ARPANET see (Abbate 2000).

1.1 Backdrop: internet struggles

The internet has transformed considerably over the past fifteen years, and it has done so in ways that defied prediction. Conceived primarily as a communication system, it has gradually evolved toward an advanced command-and-control network that manages many affordances of daily life well beyond the smart phone. Today, it is indispensable to modern manufacturing systems and the allocation of public resources. It also manages critical national infrastructure, such as power grids and traffic networks (Krause 2021*a*).

On its path of expansion, the number of interconnected devices has skyrocketed. While the original ARPANET protocol had limited the number of possible nodes to around 1,000, the internet would experience its first boom period in the mid-1980s when the adoption of the TCP/IP protocol suite enabled nearly 30,000 hosts to connect (Craig 2022). By 2030, up to 30 billion devices can be expected to link over the internet (Statista 2022*a*), which presents new challenges to the very ways in which activity on the IoT can be measured and analysed (Siow et al. 2019). Today, the internet is indeed in 'everything' and has become the backbone of an interconnected 'world with no off-switch' (DeNardis 2020).

In a world where loss of connectivity is simply no longer an option, the infrastructure and protocols that constitute the internet have become critical concerns for national governments. The larger the number of interconnected devices, and the more important they are in keeping things running as they should, the bigger the exposure to external threats that adversaries may pose. Yet managing external cybersecurity threats is only one dimension of a whole range of challenges that the internet presents today. The rise of 'big tech' companies, hungry for customer data, has generated serious questions about good regulation, democratic oversight and the design of institutions that can implement internet governance models that are fit for purpose. Increasingly visible fault lines in global cooperation only amplify the issue.

There are few, if any, technologies in history other than the internet and the Web that have been shaped to such extent by their intrinsic technological potential as well as 'by political, ideological, social, and economic factors' (Naughton 2016). What the internet should become has always been as much a question of technological affordances as one about socioeconomic realities and political will. The internet was not built to connect autonomous vehicles, or, in the era of deteriorating international relations, operate weapons systems with autonomous capabilities. To get the internet ready for the next wave of emerging technologies that demand connectivity at all times, at large scale and at high speed, the internet requires an update to its physical infrastructure, its protocols and standards, as its basic infrastructure is creaking and its potential for further growth exhausted–at least according to those who have vested political and economic interests to fundamentally reshape the internet of the future.

For nodes and devices to interconnect over the internet, they need to meet certain specifications that ensure their interoperability. Internet standards bodies, also known as internet standardisation bodies, issue detailed technical specifications to this end. These standards and protocols determine which hardware and software can operate on the internet. There are several international bodies that engage in various aspects of this work. The Internet Engineering Task Force (IETF)[2] considers itself the 'premiere standards development organization for the Internet'. It aims 'to make the Internet work better'; its mission is 'to produce high quality,

[2] https://www.ietf.org/about/introduction/

relevant technical and engineering documents that influence the way people design, use, and manage the Internet'.[3]

The Internet Society (ISOC)[4] 'supports and promotes the development of the Internet as a global technical infrastructure, a resource to enrich people's lives, and a force for good in society'; it claims to do so by facilitating the 'open development of standards, protocols, administration, and the technical infrastructure of the Internet' while providing 'reliable information about the Internet' itself.

The Internet Architecture Board (IAB)[5], an advisory body of ISOC, 'provides long-range technical direction for Internet development, ensuring the Internet continues to grow and evolve as a platform for global communication and innovation'; it enjoys 'architectural oversight of IETF activities'. The International Telecommunication Union-Telecommunication Standardization Sector (ITU-T)[6], a body of the United Nations, defines 'elements in the global infrastructure of information and communication technologies'. Its purpose is to find specifications for network technologies in 'a contribution-led, consensus-based approach to standards development'. Not tasked to find internet standards specifically, the ITU can nevertheless exert considerable influence on internet governance as its 'recommendations' for telecommunications standards are routinely picked up by governments and turned into national law, which can have sizeable bearings on internet governance overall.

Traditionally dominated by Western interests, as evidenced throughout this thesis, China has grown more assertive in its aim to shape the internet of the future

[3] The quotations in this paragraph are lifted from the 'About Us' sections of the websites of these organisations. There are several more important bodies. The W3C is omitted as its mission is to develop Web standards. In practice however, concerns overlap.

[4] https://www.internetsociety.org/mission/

[5] https://www.iab.org/about/

[6] https://www.itu.int/en/ITU-T/about/Pages/default.aspx

through influencing some of these bodies. China has done so successfully at the ITU for instance, as the following chapter discusses. Ordinarily not hotbeds of open struggles that would have considerable global repercussions, internet governance fora have witnessed more engagement from China since the beginning of this decade. Addressing internet governance issues, President Xi Jinping declared that the 'game of great powers is not only a game of technology but also a game of ideas and discourse power' (quoted in (Shivakumar 2022)), which exemplifies an important point that Web Science has been making over the years: questions over the diffusion of technology are inseparable from issues of power and the capability of influential actors to shape how technologies are being employed.

In July 2022, China announced its new 'China Standards 2035' strategy that follows its 'Made in China 2025' plan to build all critical technologies at home rather than source them abroad. The new standards masterplan recognises the fact that shaping standards, in particular future internet standards, promises vast economic as well as political returns. China seems determined to shape international standards to a much larger degree than it used to, and advocate for governance regimes alongside them. 'In this way, China hopes to boost domestic economic growth and project geopolitical influence' (Gargeyas 2021). The US has responded with its own strategy, or elements thereof, that seeks to contain Chinese ambition. At present, US–Chinese competition over emerging technologies and standards to govern them is in full swing.

This race for leadership in technology, which will shape future economic as well as military successes, is coupled with a 'turn to infrastructure' (Musiani et al. 2015) in internet governance that has witnessed state actors develop a keen interest in controlling internet architecture and protocols, besides many countries' already sophisticated control apparatuses that manage what people can and cannot do on the Web. Control over the very technologies that are going to make up the hardware backend of the internet of tomorrow promises significant strategic advantage and political gain.

In an increasingly multipolar world marked by hostility between the leading powers, state actors have re-established themselves as agents of change in internet governance–narratives of 'multi-stakeholder' involvement or industry-led initiatives have, at times, glossed over the fact that ultimately, state actors have the power to 'pull the plug': Russia, China and Iran are examples of countries where governments do retain an internet off-switch to stifle protest and dissent (Claessen 2020, Burgess 2022). However, regarding the internet of the future, the relationship between public and private sector interests is certainly a complex and entangled one. While private companies have always been involved in military procurement, R&D in dual purpose emerging technologies has shifted in that much of the cutting-edge technology today is developed in the private sector in the first instance, which then spills over into public domains or the military (Howell et al. 2021). This finds reflection in patenting activity, one of the sources of data of this thesis.

Quantum technologies in particular are of considerable interest to the Chinese leadership. Chapter 4 characterises them in detail. President Xi Jinping seems especially invested in them, as he proclaimed himself in his speech on the occasion of the hundredth's anniversary of the Communist Party in the summer of 2021 (Xi 2021). As will be discussed in later chapters, China scrambles to build quantum technologies, in particular quantum computing and quantum communication systems, for the purpose of presenting to the world the first genuinely

Chinese computing technology. Such a milestone would not just offer President Xi considerable reputational gains but provide the Chinese leadership at home with a general purpose technology they can trust–trust, or lack thereof, being one of the key reasons why China wants to decouple from Western high technologies. A Chinese quantum internet would be trusted by the Chinese leadership to shield its economy and society from foreign influence.

Since 2020, literature has begun to emerge that discusses quantum technologies in relation to national security and military planning (Lele 2021, Lindsay 2020). These works provide welcome overviews of wider, general implications of quantum technologies, including sensing and metrology.[7] While this thesis aims to contribute to a nascent, interdisciplinary body of work in the quantum domain, it also seeks to make for a more targeted contribution regarding the strategic implications of either US or Chinese advantage in building the quantum internet.

This thesis is motivated to a large degree by a desire to add to a nuanced debate; to provide grounds for being optimistic about the potential of a quantum internet whilst being mindful and honest about obstacles, challenges and outright problematic efforts of state actors to integrate quantum internet technologies with existing surveillance and control regimes. In the academic literature the quantum internet has not yet been discussed with a view to the intensifying competition between the US and China. This thesis is the first study of the quantum internet with a focus on US–Chinese rivalry over emerging technologies.

[7] Quantum sensing is an emerging field that aims to build devices that detect motion by exploiting quantum phenomena to register changes in electric and magnetic fields. Metrology is the general study of scientific measurement.

1.2 Research questions

This thesis seeks to investigate how the development of a quantum internet is influenced by, or subject to, the strategic competition between the US and China. Put differently, the big overarching question this project pursues is

> **R.1** How is the quantum internet being shaped by US–Chinese competition?

‘Competition’ in this context means ‘strategic competition’. Following the RAND Corporation, the term can be defined as ‘a long game between those with a vested interest in preserving the international order of rules and norms dating back to the post–World War II era’, i.e. the United States, ‘and revisionist powers seeking to disrupt or reshape this order’–in the context of this thesis, China (Paul et al. 2022). **R.1** is exploratory in character as opposed to seeking exact verification or confirmation, and as such invites the study of ‘descriptive facts’ as well as ‘structural arrangements’ and ‘beliefs and belief systems’ (Stebbins 2008). Exploration involves being mindful that technologies have the persistent habit of turning out very differently from what their inventors intended for them. The World Wide Web is certainly a good example of this phenomenon (Berners-Lee 2019, Bridge 2018, Solon 2017).

In pursuing **R.1**, this thesis does not make definite claims as to what exactly the quantum internet is going to be. Rather, it is curious about present-day forces that try to shape it and attempt to place it on a certain trajectory. While the thesis avoids making assumptions about the exact reality of a future quantum internet, it does assume that *some* quantum technology futures are more probable than others. It is the point of this thesis to identify and establish the important drivers that make for this probability. To investigate the ways in which the US and China hope to bend the quantum internet to their political preferences is one way to do this, but it is certainly not the only plausible perspective.

The quantum internet is unlikely to be built by governments directly, at least not all of it. Private companies, in particular spin-outs and startups, big tech corporations, universities, and the military are all involved in building the quantum internet. Governments differ in their power to influence this wide range of actors. However this thesis assumes that governments hold at least *some* sway over the degrees of freedom these stakeholders have in building a new internet architecture. As discussed in the following chapter, such influence may manifest in various ways, from funding decisions to key appointments or otherwise preferential treatment.

Discussing engineering advances in the quantum domain, an article in *Nature*, playing on the fundamental principle in quantum physics that quantum objects can be in more than one place at a time (see Chapter 4), is appropriately titled 'The quantum internet has arrived (and it hasn't)' (Castelvecchi 2018). The quantum internet has not yet been fully developed. Much can be said about present efforts to build it and the power games around it, however. To a large degree such an inquiry is speculative. In parts very tangible, in other parts still more proof of concept than reality, the quantum internet is a difficult research object to study empirically.

Two statements can be made at this point, which will be supported further in the following chapter: i) future internet technologies, including quantum, will be shaped by US–Chinese competition in governance and standards-finding; and ii) ownership of and leverage over internet technologies provide antagonistic state actors with bargaining power to push for their envisioned standards, which adds to their influence and, ultimately, political power. Therefore, in order to get to the overarching research question above in a meaningful and empirically informed way, **R.1** is broken down into two subquestions:

> **R.1.1** What do domain experts observe regarding US–Chinese competition in internet governance?,

and

> **R.1.2** What do patent data suggest about US and Chinese activity in building the quantum internet?

There is no readily available dataset that could help answer the central research question **R.1**. Rather, the evidence base must be assembled. **R.1.1** and **R.1.2** achieve this by pairing intelligence gathered in interviews with signals from patenting activity (a full justification for this approach can be found in Chapter 3). Breaking down **R.1** in this fashion is motivated by China's policy position that seeks to maximise patenting activity for quantum internet technologies while simultaneously pushing for a reform of internet standards and governance regimes, as the following literature review chapter demonstrates.

Coupled in this way, **R.1.1** and **R.1.2** effectively call for a mixed-method approach that integrates the qualitative analysis of interview data with the quantitative study of patent data in the domain of quantum internet technologies. The key assumption, motivated by a review of the literature and official policy positions, is that technological progress in building component parts for the quantum internet add to US and Chinese bargaining power in the internet standards and governance domain. This raises the question, how can such technological progress be observed?

In response, this thesis argues that there are two principal ways to do this: first, speaking to experts, who have privileged access to sources and knowledge, is a means to extract rich qualitative data. And second, quantum technology patent data contain important signals about the scale and the pace of US and Chinese efforts to establish a dominant position in quantum internet technologies. The flow chart below is a simplified visualisation of the larger framing against which the research questions are developed.

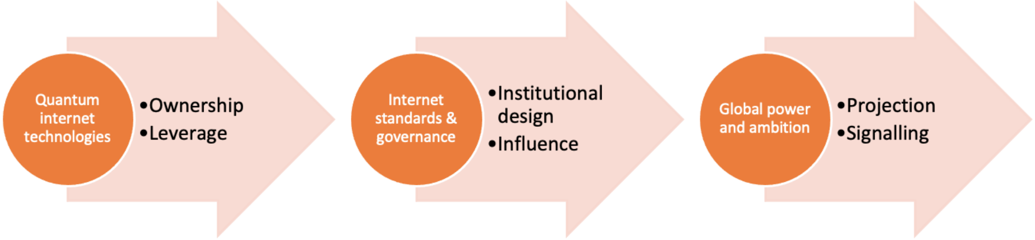

Quantum internet technologies
•Ownership
•Leverage
Internet standards & governance
•Institutional design
•Influence
Global power and ambition
•Projection
•Signalling

Figure 1.1: The relationship between quantum technologies and global influence.

The above chain of impact is confirmed in various publications and official policy statements, and is justified in full in the literature review chapter. While this thesis does not suggest strict causality, it assumes a relationship between ownership of, and leverage over, quantum internet technologies and the projection of power. If there was no such relationship there would be no emerging technology race between the US and China. Ownership of important quantum internet technologies translates into bargaining power to set standards and governance principles at international institutions, which, in turn, supports power politics and influencing on a global scale. Traditionally this has been a picture painted by US dominance. At present, it is increasingly being recoloured by Chinese ascent.

1.3 Thesis structure and chapter summaries

This thesis has a total of eight chapters. Chapter 2 discusses relevant literature, and Chapter 3 develops a methodology for researching the quantum internet. Chapter 4 provides a high-level introduction to quantum computing and quantum communication to prepare the reader for the two empirical chapters that follow: Chapter 5 explores interview data while Chapter 6 analyses a dataset of 4,200 patent families and their 10,000+ citation trees. Chapter 7 discusses the empirical findings of this thesis. Chapter 8 concludes.

Each chapter ends with a summary and a collection of the major takeaways in bullet points. They serve as a quick overview and a point of reference for each chapter.

The Appendix collects details of the R and Matlab code that was used for analysis. It provides a link to the University of Southampton's data repository system 'Pure' where a .zip folder of the code files is available for download. The raw data however cannot be made publicly available as they were retrieved from proprietary data services provided by the European Patent Office. Chapter 3 includes a detailed discussion of how data were retrieved for easy replication of the research process, including data files.

Chapter 2: Literature review

This chapter situates the empirical analysis of US and Chinese efforts to build the quantum internet in a broader discussion of the political factors that shape the strategic competition over emerging technologies. It argues that China is pursuing a dual strategy aimed at patenting innovation in quantum internet technologies while simultaneously extending its sphere of influence over organisations and institutions that shape norms and set standards for the internet.

Quantum technologies are found to be embedded in a larger emerging technology and security arms race between the US and China. Quantum internet technologies may present quantum-enabled state actors with new capabilities to offer non-aligned states what the thesis calls 'quantum patronage' in return for a commitment to strategic alignment and alliance-building. For China, quantum technologies are an opportunity to present to the world a genuinely Chinese technology that does not imitate or duplicate Western inventions. For the Chinese government, actual engineering and technology leadership in the quantum domain and influencing standardisation and governance bodies are not two separate issues but bundled in a comprehensive quantum strategy.

The chapter develops the concept of QISG, quantum internet security governance. QISG is about mapping processes of multi-actor involvement in the emergence and control of security and governance practices in quantum networks. QISG studies the quantum internet along three axes: i) it being an object of security concern to state actors, ii) as requiring an internet policy response in the governance domain and iii) a network that involves actors outside government, such as international standardisation bodies, industries, universities and the military.

Chapter 3: Methodology

This chapter explains the choice of methods of this thesis with a view to the qualitative and quantitative character of the two subquestions it pursues. It develops a justification for a mixed-method approach to studying issues of power and governance surrounding the emergence of the quantum internet. The proposed mixed-method framing brings together semi-structured interviews and patent network analysis for pursuing the overarching question, how the strategic competition between the US and China is shaping the quantum internet.

A mixed-method approach is argued to bring together complementary approaches to the study of the inevitably fuzzy variables that will shape the quantum internet. The approach reaches beyond methodological siloes and appeals to a larger body of readers than any strictly separated method alone. Interviews in empirical international relations research are found to support the identification of larger intersecting themes and tropes that escape a purely quantitative approach or are difficult to evidence by statistical means alone.

Patent analysis, on the other hand, is an established research field that investigates the diffusion of knowledge as well as the scale and the pace at which innovation translates into novel products and processes. Patent citation networks in particular can provide valuable insights into the dynamics by which innovation diffuses in national research programmes.

The analysis of patent citation networks requires a dedicated class of statistical models due to the interdependence of network events. The chapter argues that Exponential Random Graph Models (ERGMs) are a sophisticated class of models that estimate the entire network in one step, thus avoiding untestable assumptions not backed by further evidence or theory. The chapter also discusses the data collection and preparation strategies that have been pursued.

Chapter 4: the quantum internet

A network that connects at least some quantum computers (nodes) with either 'classical' computers or other quantum machines over a secure quantum communication channel is called a quantum internet. This chapter provides a high-level introduction to quantum computing and quantum communication, the two technologies that will constitute the quantum internet. It argues that computationally expensive programs in AI and ML will soon run into hardware problems. This is because digital (or 'classical') computing built on micro-transistors placed on silicon chips has reached a natural limit to its growth.

In addition to a massive increase in compute resources, quantum computers are hoped to run certain classes of algorithms that are intractable even for the best digital supercomputer. The most prominent example is 'Shor's Algorithm' for factoring large integers, which poses a considerable threat to RSA encryption models. However, the single biggest obstacle to realising even a modest quantum computer is error correction. Quantum communication, on the other hand, is the application of the quantum phenomena of superposition and entanglement for the purpose of encrypting messages over significant distances. Essentially a distributed system, the quantum internet will provide entanglement at scale.

There are several important applications and use cases for a quantum internet, the most important ones being information security, the provision of compute resources over a quantum-secured network, cyber defence and attack, the modelling of complex systems and the provision of secure cloud services. A quantum internet is hoped to protect critical national infrastructure against highly sophisticated state-sponsored cyberattacks.

Chapter 5: Internet governance in the 2020s

In conversations with domain experts, this chapter discusses how China has grown considerably more assertive, and now seeks to dominate important standardisation bodies. China's strategic outlook has changed under President Xi. Informants suggest that China has come to consider the US its chief strategic rival while blocks such as the European Union matter only little in China's strategy portfolio. Participants argue that China is concerned about the extent to which US big tech corporations shape US policy positions. Too much private sector involvement in the US makes it difficult for China to identify who the actual powerful actors are in the emerging technology race with the US.

Quantum communication is likely going to be the key technology for China to compete over and push globally for Chinese internet and communications standards. Informants at GCHQ and the British Government consider the direct security implications of Chinese Quantum Key Distribution (QKD), and a Chinese quantum internet, manageable. Researchers in countries at the periphery of Chinese influence, such as Singapore, seem less relaxed: the quality of intelligence signals will drop when China moves to communicate internally over quantum channels.

Interviews further suggest that the US and its allies struggle to formulate a response when China offers solutions to actual technology gaps and problems in internet governance, yet the West believes it can only reject them. Non-aligned countries will expect better than defaulting to knee-jerk rejections of Chinese proposals, even if Chinese ambition is not universally appreciated. 'New IP' is a prime example of Chinese ambition in this context. A signal of intent rather than a workable proposal, respondents fear its implementation would mean the end to the open internet.

Chapter 6: Quantum patent data–descriptive statistics and ERGMs

The chapter analyses 4,200 patent family records in the domain of quantum internet technologies (and the 10,000+ other patents they cite as 'prior art'). The analysis reveals a strong preferential treatment of domestic technologies in both the US and Chinese citation networks. New patents registered by entities headquartered in China between January 2015 and December 2021, if relevant to building the quantum internet, overwhelmingly cite patents that were registered at a Chinese patent office. New patents registered by entities headquartered in the US during the same period, if relevant to building the quantum internet, overwhelmingly cite patents that were registered at a US patent office.

The Chinese network contains two large components (complete subgraphs) of around 2,000 nodes each; the remaining 338 components are of size 2 to 20. This is evidence for two separately evolving research programmes in China. If this is due to strategic separation or accidental because of a lack of steer and oversight is not in the data. The US network, on the other hand, contains a single-biggest component of 1,589 nodes followed by a dozen or so smaller subgraphs that range between 10 and 38 vertices, and a vast trail of dyads. This suggests a more unified approach in that the US quantum research programme seems to be one big project that draws on the same sources of prior research.

Building and testing six separate ERMGs, the chapter finds robust statistical evidence for preferential treatment in both the US and China regarding the countries of filing (China, Germany, Spain, the UK, Japan, South Korea, the US and 'World'), the type of organisation that registers patents (industry, private individual, university or research institute, military, other) and the number of IPC codes that were given. These variables are strong predictors of US and Chinese quantum patenting activity.

Chapter 7: Discussion The purpose of this chapter is to discuss the findings of Chapters 4, 5 and 6 in response to the research questions developed in Chapter 1 and the literature discussed in Chapter 2.

It first discusses Chinese ambition. 'New IP' must be considered a precursor to the ways in which China envisions the implementation of the quantum internet. Quantum capabilities could be made available to selected subnetworks only, effectively splitting the internet into a classical network and a quantum-powered one. A *'New IP' quantum internet* would connect to the rest of the network via strongly policed access points. It must be assumed that the Chinese leadership does not expect the rest of the world to embrace 'New IP' and rebuild the internet accordingly. What 'New IP' has already achieved, however, is to signal to the West that China is a serious contender for dominance.

With a view to the UK, the quantum internet is likely to create new dependency risks for Britain as it potentially exacerbates the problem of increased market concentration among cloud service providers, a critical market presently dominated by US companies. The same companies that dominate the UK cloud services market are investing heavily in building up quantum capabilities.

The empirical analysis of six ERGMs finds that each side is 'doing its own thing'. Within each sub-cluster of the already siloed Chinese and US quantum internet research programmes, the preferential treatment stretches even further, which suggests that 'doing one's own thing' and group think are the ultimate drivers of patenting activity in the quantum domain. University researchers prefer citing other university researchers, while military research rather cites other military research and so forth.

The final section of the chapter develops the building blocks of a coalitional game theory model in which utility is transferable. It suggests that the quantum internet will not be interoperable but fragmented unless the US makes the conscious decision to offer China payment to shelve its ‘New IP’ many-nets approach. The model suggests an allocation rule that specifies how much compensation China can reasonably demand. The important insight of the model, which is an initial attempt at formalising the problem and should be developed further in future research, is that it will be strictly beneficial for the US and its allies to make financial sacrifices to obtain a global standard for an open quantum internet, even if this requires a change of perspective: the West is no longer able to implement internet standards at will.

Chapter 8: Conclusion The concluding chapter first revisits the research process and the research questions. It then proceeds to discussing further the main findings of the thesis under the following ten headings:

1. Chinese ambition

2. Chinese big tech and quantum small tech

3. ‘New IP’ and good old surveillance

4. The UK’s response

5. The quantum internet will create new dependency risks for the UK

6. China dominates the quantum patenting landscape

7. Strong evidence for significant preferential treatment in China and the US

8. US quantum internet patenting activity seems more coordinated

9. Countries of publication, the type of registering organisation and IPC codes drive patenting activity

10. Good quantum internet standards should be procured, not hoped for

The final section of the Conclusion takes stock and reflects on the future of Web Science as a discipline. For Web Science as the interdisciplinary study of the Web, the question of how the internet, its chief enabling technology, will evolve over the coming years, is of paramount concern. The thesis finds that the quantum internet of the future will be shaped to extraordinary degree by US–Chinese strategic competition. If Web Science is the study of the Web as a complex sociotechnical system and as a discipline questions the narrative that complex problems could be solved by technical solutions alone, it is difficult to imagine a better object to study than the quantum internet.

Chapter 2

Literature Review

This chapter aims to situate the empirical analysis of US and Chinese efforts to build the quantum internet in a broader discussion of the political factors that shape their strategic competition over emerging technologies. It argues that China pursues a dual strategy aimed at patenting innovation in quantum internet technologies while simultaneously extending its sphere of influence over organisations and institutions that shape norms and set standards for the internet. The United States and its allies seem surprised at the level of China's determination to not just offer novel quantum technologies but also technical specifications and standards that give China and its (few) allies a competitive edge, which would translate into considerably more bargaining power in international diplomacy.

China's concerted efforts pose a new, and serious, challenge to Western technological leadership that reaches far beyond past Chinese policy of merely building cheaper, and thus more competitive, versions of existing Western technology stacks. China is aiming high and seeks to offer not just novel internet technologies but standardisation and governance packages alongside them that help lock in participating actors and thus erode US dominance. While the history of the internet up to this point has been very much an American story, its future could indeed be largely Chinese.

To develop these points, the chapter is organised as follows. Section 2.1 discusses what internet governance involves, and considers conflicts in this domain against the backdrop of an increasingly assertive China in international relations. Section 2.2 considers how emerging technologies are related to international security and great-power rivalry. It reviews official US and Chinese policy positions to make the point that the US now considers China a strategic rival in the domain of emerging technologies, and openly calls for containment. This is a departure from previous positions and is likely to mean that multi-stakeholder standard-finding for the quantum internet is a thing of the past.

Both the US and China have issued strategy papers that signal a strong commitment to shaping the internet of the future. 'China Standards 2035' is a 15-year plan to forge international standards to Chinese specification well beyond internet technologies (Gargeyas 2021, Mbeba 2021, Wu 2022). It complements China's policy to place senior officials in international organisations. Section 2.2 goes on to make the point that patenting activity, standardisation and governance-finding for the internet should be considered in tandem–the Chinese leadership is pursuing these issues in parallel, which establishes a firm link between 'discursive power' and patenting activity. For the Chinese government, patenting new quantum technologies is paramount for securing property rights, which, in turn, yields bargaining power in international standard-setting games.

Section 2.3 discusses the political economy of networks and standards to argue that Chinese ambition is not out of the ordinary–US technology and internet standards have shaped the history of the internet to a large degree and it should come as no surprise that a newly emerging superpower should want to challenge US dominance. This is an important point to make so that critical reflection on Chinese activity does not descend into ‘China bashing’. While internet standards have always been contested, the section argues that the turn to infrastructure in internet governance is a fairly recent, and very serious, challenge to a free and open internet: authoritarian regimes are increasingly concerned with controlling network infrastructure. Quantum internet technologies will provide them with new opportunities to increase their grip over the network of networks.

With regard to the overall conceptual framing of this thesis, section 2.4 deploys the concept of ‘security governance’. It outlines QISG, or quantum internet security governance, as a lens for studying quantum internet governance. This conceptual perspective pays particular attention to the coproduction of norms and standards but argues that at a time of intensifying great-power rivalry in an increasingly multi-polar world, state actors are, more than ever, the ultimate agents of change. While state actors aggregate and integrate preferences from a wide range of corporate and civil society stakeholders it would be short-sighted to ignore the re-emergence of the state as the principal actor. Section 2.5 concludes and provides headline summaries of the major takeaways of this chapter.

2.1 Internet governance in US–Chinese competition

The internet has always been an object of power play. As such, it has always enjoyed a special status in interstate competition. The past decade has witnessed an intensification of conflicts over the internet, and an increase in focus on the infrastructure of the network of networks: the physical systems and platform architecture of the internet itself, rather than the application spaces they afford, such as the Web, have moved centre-stage in national security policy and strategy-making. The optimistic public discourse of a borderless world thanks to borderless communication and the utopia of a free and unregulated cyberspace, most prominent in the 1990s and early 2000s when the Web entered the mainstream, could never truly mask territorial power dynamics and hard-fought battles over internet governance (Castells 2002, DeNardis 2014*b*).

Even at the peak of globalisation in the late 2000s, which saw the considerable enlargement of the European Union and, to great fanfare, the ratification of new trade agreements across the world, critical warnings against ignoring the decisive weight of nation states in shaping the future of the internet were plentiful. Commentators would point out that the internet will always reflect 'the interests of powerful nations and the conflicts within and between them' (Goldsmith & Wu 2008). This remains true today. If anything, state wrangling over internet infrastructure has only intensified. At present, with the emergence of new quantum internet technologies, efforts among state actors, notably the US and China, to shape the internet of the future to their political preferences have surged.

This comes at a time when interstate competition is already accelerating. The global resurgence of nationalism and the return to protectionism over the past decade have fuelled new agendas of state control and influence that have shaped a great many political agendas. Discourses on internet governance are no exception. The shift among policymakers and officials to view communication networks primarily through the lens of security and risk seems a particularly powerful narrative at present. Accounts of the national security risks of global communication networks have reframed the internet in security terms.

The literature describes the processes by which an object becomes a concern for national security as ‘securitisation’. The concept of securitisation can be broadly defined as ‘a process in which an actor declares a particular issue, dynamic or actor to be an ‘existential threat’ to a particular referent object’ (Williams (2013, p. 72), cf. Wæver (1995)). For instance, the internet may become a threat to the state due to an adversary’s internet-based disinformation campaign that challenges the integrity of domestic elections. Over time, an insufficiently leveraged internet at the infrastructural level has emerged as a considerable risk to national security–in the eyes of many policymakers, at least.

While state actors in the 1990s and 2000s were primarily concerned with controlling who is doing what on the internet, since then the attention has broadened towards the physical makeup of the internet as such–the hardware and mechanisms that constitute the backbone of the network. This ‘turn to infrastructure’ reflects states’ recognition that ‘points of infrastructural control can serve as proxies to regain (or gain) control or manipulate the flow of money, information, and the marketplace of ideas in the digital sphere’ (Musiani et al. 2015, p. 4). This is not to suggest that today intelligence services are less nervous about what people do on the Web than they used to be. Rather, national security agendas have deepened to include a considerable infrastructural component.

This newly found concern with network architecture comes at a time of increasing tension between China and the West. In June 2020, the UK government’s decision to ban the Chinese telecommunications giant Huawei from building Britain’s 5G network highlighted the now ubiquitous role of communication networks, provided by the private sector, in national security narratives: following a review from the cybersecurity arm of its communications intelligence service GCHQ, and bowing to pressure from the US, the UK government ordered a 'total ban' on purchasing new Huawei equipment from 2021. Huawei 'will be completely removed from the UK's 5G networks by the end of 2027' (DCMS 2020). In October 2022, for some parts of Huawei equipment, the deadline was pushed back by a couple of months (News 2022*a*). In November 2022, the US announced a blanket ban of future sales of Huawei and ZTE equipment. In the words of the US Federal Communications Commission, this is to protect 'our national security by ensuring that untrustworthy communications equipment is not authorised for use within our borders', a spokesperson said (News 2022*b*).

While China's combative government broadsheet *Global Times* called for 'public and painful' retaliation in response to the UK ban (Times 2020), the then-US government applauded Britain for joining 'a growing list of countries from around the world that are standing up for their national security' (US Department of State 2020). To China, however, the move appeared to be less about mitigating security risks and more about inflicting economic damage on its global telecommunications figurehead. It vowed to 'take measures to safeguard' the 'legitimate interests' (News 2020) of Chinese corporations abroad. China's robust response reflects the new status of exercising control over global communication hardware for the projection of power. The UK's position also demonstrates the degree to which national security now has network security at its flipside, and how much internet technology has become sensitive to alliance-building in a shifting international security landscape.

Parallel to this infrastructural turn, efforts to influence international standardisation bodies that implement internet governance frameworks have also intensified. The internet is a vast collection of subnetworks. To ensure interconnectivity between these subsystems, a large set of protocols, rules, policies, and mechanisms for managing the internet needs to be maintained. There is no central management function in place to achieve this. ‘Internet governance’ involves many actors; it is very much an umbrella term that captures the policies, practices, standards, and technical specifications that ensure that the internet works across jurisdictions.

Official documentation and policy announcements usually emphasise that internet governance is a group effort. To this effect, ‘governance’ seeks to convey a ‘polycentric, less hierarchical order’ (Mueller 2022) grounded on cooperation and collaboration, at least in principle. The closest to an official definition of internet governance was developed in 2005 by the UN Working Group on Internet Governance, which settled on the following phrase:

> ‘Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet’ (WGIG 2005, p. 4, no. 10).

Processes of ‘shaping’ are central to this definition; the term has informed the title of this thesis. The definition highlights that internet governance involves a diverse group of actors with a range of different perspectives and potentially conflicting objectives. ‘Internet governance’ involves standardisation bodies such as ICANN, the Internet Corporation for Assigned Names and Numbers and IETF, the Internet Engineering Task Force, which looks after technical specifications, just as much as human rights groups and civil society advocates that are concerned about data privacy or AI-enabled decision-making, for instance.

This potpourri of interests and expertise is commonly referred to as the 'multi-stakeholder model' (Bygrave & Bing 2009, DeNardis et al. 2020, Radu et al. 2014), which seeks to demonstrate that there is not a single mighty supranational body at the heart of the internet but that governance is a multiplex crossover of institutions that are all engaged in shaping the network, each from a unique perspective. CENTR, the Council of European National Top-Level Domain Registries, offers informative infographics that provide an overview of the actors involved in internet governance, one of which is reproduced below.

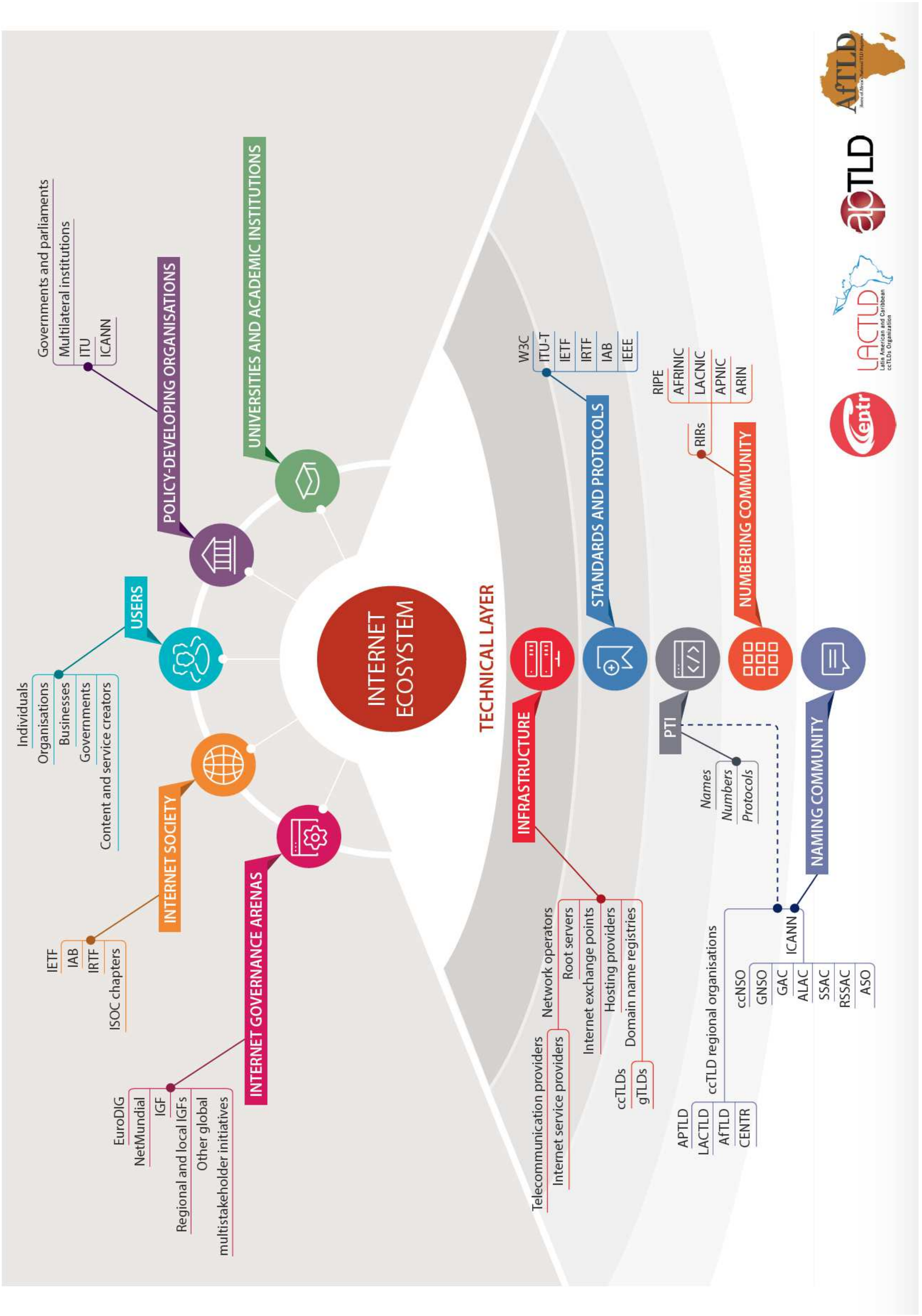
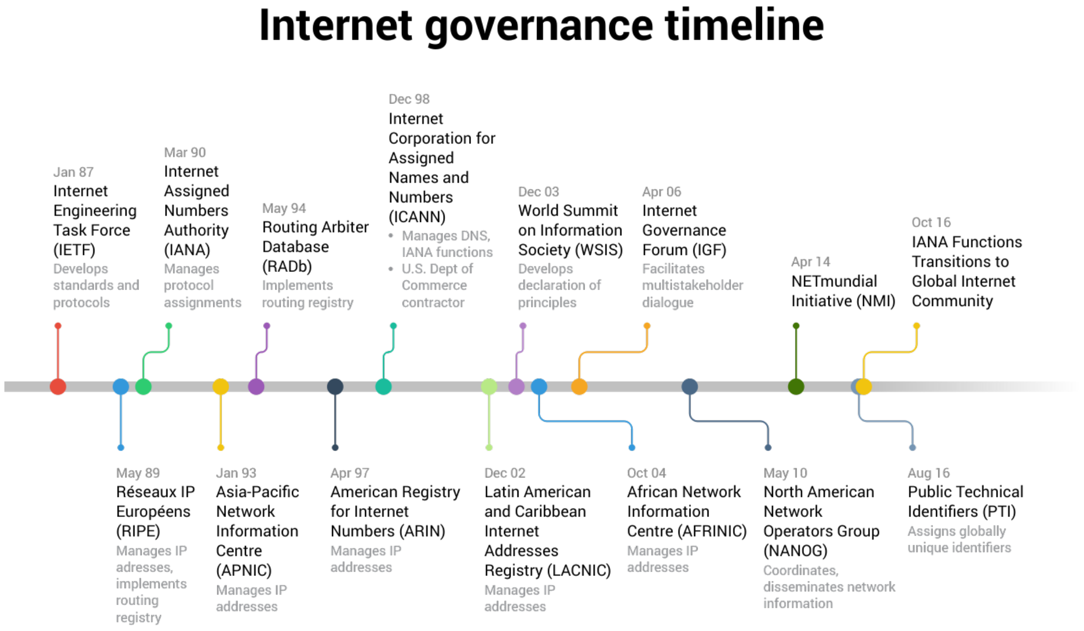


Figure 2.1: Key actors and institutions in internet governance. Source: (Winkler 2022).

The internet governance ecosystem did not develop overnight. Since the 1990s, there has been a steady increase in the number of bodies that speak to the issue. Some have, or used to have, political affiliations. A prominent example is ICANN, which was officially contracted to manage internet address namespacing by the US Department of Commerce until October 2016. This relationship has caused some Chinese officials to view ICANN primarily as a vehicle to advance US interests while US and European officials habitually pointed out the body's independence. Disagreements about ICANN's legitimacy stretch back at least twenty years (?). The timeline below provides and illustration of the emergence of some of the most important institutions and fora that are involved in internet governance making.



Internet governance timeline
Jan 87
Internet Engineering Task Force (IETF)
Develops standards and protocols
Mar 90
Internet Assigned Numbers Authority (IANA)
Manages protocol assignments
May 94
Routing Arbiter Database (RADb)
Implements routing registry
Dec 98
Internet Corporation for Assigned Names and Numbers (ICANN)
• Manages DNS, IANA functions
• U.S. Dept of Commerce contractor
Dec 03
World Summit on Information Society (WSIS)
Develops declaration of principles
Apr 06
Internet Governance Forum (IGF)
Facilitates multistakeholder dialogue
Apr 14
NETmundial Initiative (NMI)
Oct 16
IANA Functions Transitions to Global Internet Community
May 89
Réseaux IP Européens (RIPE)
Manages IP adresses, implements routing registry
Jan 93
Asia-Pacific Network Information Centre (APNIC)
Manages IP addresses
Apr 97
American Registry for Internet Numbers (ARIN)
Manages IP addresses
Dec 02
Latin American and Caribbean Internet Addresses Registry (LACNIC)
Manages IP addresses
Oct 04
African Network Information Centre (AFRINIC)
Manages IP addresses
May 10
North American Network Operators Group (NANOG)
Coordinates, disseminates network information
Aug 16
Public Technical Identifiers (PTI)
Assigns globally unique identifiers

Figure 2.2: Milestones in internet governance: timeline of key initiatives. Source: (Mueller 2022).

The appointment of Houlin Zhao as Secretary General of the ITU on 1 January 2015 was a major success for China in its endeavour to place top officials at international organisations. Institutions such as the ITU are going to have significant implications for shaping how the quantum internet of the future will be governed. While not able to impose rules that are legally binding with immediate effect, the ITU has considerable power to establish voluntarily adopted, early protocols that can rapidly become de facto standards across the world.

The successful placement of senior officials allows China to exercise downward pressure on working groups by 'subsidizing the participation of its companies in study groups, advisory groups, conferences, and meetings that negotiate technical standards and guidelines' (Schaefer & Pletka 2022, p. 2). China seems to be pursuing a well-rounded strategy of placing actors at key vantage points where they can be expected to judge favourably on standards proposed by domestic industries. The country 'has adopted a state-directed strategy to influence international standards-setting, and use them as a foreign policy tool to enhance its global standing', an Indian newspaper, worried about increasing Chinese meddling in India's regional affairs, reports (ANI 2022). It has taken Western alliances five years to wake up to China's considerable efforts in this area.

China's global standard-setting ambitions are matched by a tighter internet governance regime at home. Since President Xi Jinping took office the country has witnessed a significant extension of its operations to restrict the scope for online dissent, such as a clampdown on the use of private VPN use (Ensafi et al. 2015).[1] However, the Chinese leadership seems mindful that too many restrictions on the flow of information can disrupt innovation, university research and business development. The challenge for China, it seems, is to advance commerce and research

[1] VPNs, or Virtual Private Networks, establish a private connection between a computer and the internet. These VPNs are deployed to mask network data that can help locate and identify individuals, such as their IP address. While VPNs cannot make internet activity completely anonymous, they establish an encrypted point-to-point connection that increases privacy and security.

collaboration (which thrives online) while at the same time stifling online dissent (Normile 2017, Economy 2018).

One way for China to achieve this, it seems, is to foster a new sense of national pride, one that accepts strict authoritarian principles. It is no surprise that commentators find a strong positive correlation between China's increasingly restrictive internet policy model and a surge of nationalist attitudes and support for authoritarianism among young people (Wang 2020). A new, and genuinely Chinese quantum internet technology, proudly developed and built at home, would certainly feed the narrative of Chinese exceptionalism. The potential success of a Chinese internet technology that exploits quantum phenomena, one which may diffuse internationally thanks to China-friendly standards passed by international institutions, would provide the Chinese leadership with significant reputational assets both at home and abroad.

While this thesis focuses on US-Chinese rivalry, it would be unfair to single out China as the only actor that would challenge the idea of a free and open internet. Russia, too, seems to have been following a path of restrictive measures since long before the invasion of Ukraine in February 2022. In December 2019, the Russian government announced it had successfully tested an 'unplugged' alternative to the internet, a domestic network that has access points to the internet but can be physically separated from it. This prompted some leading computer scientists to warn against 'an increasing breaking-up of the internet' (Wakefield 2019). Parallel to these tests, the Russian State Duma passed legislation that enables an 'autonomous Russian internet' not only to block users in Russia from accessing undesirable sources but also to prevent the physical transmission of any unwanted incoming traffic in the first place (Claessen 2020). Border control, not borderless communication, seems to be the ultimate goal of Russian internet policy.

Appeals to nationalist, or regional, sentiment are now seen in Europe too where the European Commission has called repeatedly for ‘technological sovereignty’ in high-stakes domains such as AI and quantum communication. Galileo, Europe’s own navigation satellite, is an early example of Europe’s efforts to become infrastructurally independent from the US and China (EGSA 2011). For the Commission, technological sovereignty ought to be ‘institutionalised’ in cross-European technology programmes that align with ‘European values’ (Bauer & Erixon 2020, Scott 2019), even if it is not necessarily clear what these are. Some commentators argue that, ‘given the absence of a leading AI industry and a coherent defence strategy’, the Commission may be overestimating its reach in some key network technology domains (Calderaro & Blumfelde 2022).

There is no lack of ambition, however. In June 2022, the European Commission launched the aforementioned European Quantum Communication Infrastructure (EuroQCI) Initiative, an ambitious programme to develop a rudimentary yet ‘fully operational’ quantum internet by 2027 (Commission 2022).

Against this backdrop of protectionism, nationalism and international competition, some analysts have expressed concern about a fragmentation of the internet and point to the ‘fragility’ and ‘contingency’ of its governance regime, and caution against a split into several parallel ‘authoritarian’ and ‘commercial’ internets (O’Hara & Hall 2018). It is possible to imagine an internet of the future that is multi-layered and held together by different infrastructures that connect via multiple access points, much like fast lanes and flyovers on a motorway where tolls are due and/or special permission is required to access the fast lane, paralleled by free-to-use slow lanes for the majority of retail users.

When it comes to designing the policy principles for the internet of tomorrow, state actors certainly recognise that internet governance has become a key domain of security policy. Presently, conflicts in internet governance 'are the new spaces where political and economic power is unfolding in the twenty-first century' (DeNardis 2014*b*, p. 1). This thesis focuses on one hugely important area within these dynamics, that of quantum technologies and internet standardisation in light of strategic rivalry. How will quantum technologies shape the internet of the future now that the internet has indeed become a foreign policy tool, is exposed to unprecedented efforts of state control, and is at the risk of breaking up? A response to this question requires an engagement with the accelerating competition over emerging technologies more generally that characterises US-Chinese relations at present.

2.2 US–Chinese competition over emerging technologies

The global security implications of emerging technologies are widely discussed in the security studies literature. In particular high-performance computing is recognised for its import in realising strategic ambitions in international relations such as the competition between strategic rivals for global dominance, and how they influence other state actors in the pursuit of their agendas (Castree et al. 2013). Emerging technologies, on the other hand, may be characterised by a set of factors such as their '(i) radical novelty, (ii) relatively fast growth, (iii) coherence, (iv) prominent impact, and (v) uncertainty and ambiguity' (Rotolo et al. 2015). In practice, not all five factors will be equally important at all times. Taxonomies of this sort help limit the scope of potentially significant inventions: not every piece of innovation is in and for itself an emerging technology. Questions regarding the securitisation of emerging technologies, then, mean inquiring into the implications of innovation and novelty for strategy-making and the projection of power.

With regard to international security, emerging technologies 'have potentially transformative implications for the international balance of power, alliances and security organizations, how governments control information, how international actors compete militarily and economically, and how they wage war', the editors of a recent anthology in this domain argue (Steff et al. 2021, p. 1). While this is a very broad list indeed, technology should not be misconstrued as the only driver of change. From a Web Science perspective, of course, no technology should be considered in isolation and independent but embedded in larger social and political structures. As for quantum internet technologies, it seems more appropriate to speak of a *coproduction* of the quantum internet, its governance regime and the transformative effects that the editors above identify.

To say that the quantum internet will be 'coproduced' is to suggest it will be shaped by various factors; international relations, domestic policy concerns, market forces, research ecosystems and technological affordances all intersect. 'The term *co-production* reflects this self-conscious desire to avoid both social and technoscientific determinism' (Jasanoff 2004, p. 20, emphasis in original). Hence the 'transformative implications' of quantum technologies should be read as interwoven with larger political, economic and ideological tropes. In this sense, this thesis does not seek to endorse 'technological determinism', the ontological view that technology alone is the ultimate driver of novelty (Dafoe 2015, MacKenzie & Wajcman 1999). The transformative implications of emerging technologies must be realised against competing forces within existing power structures, as well as the ebbs and flows of ideas about what is good and bad. As such, ‘concern about new technologies is warranted, but determinism is not’ (Talmadge 2019, p. 865).

With this positioning in mind, within the webs that ideologies, technologies, power, economic, and political structures span, technological innovation may still enjoy a privileged status. Radical novelty may upset the status quo. At many points in history, then-newly emerging technologies had the potential to change the balance of power and tip it toward actors who were quick enough to establish technology leadership, from the ‘crossbow to H bomb’ (Brodie & Brodie 1973). Minuscule change can have significant long-term repercussions. ‘In the eighteenth century, for example’, Eliot A. Cohen argues, ‘minor improvements in the design and manufacture of gun barrels and carriages, coupled with the standardization of cannon calibers, laid the groundwork for the vastly improved cannonades of the armies of the French Revolution and Empire’ (Cohen 1996, p. 38). Minor amendments to the design of gun barrels were enough to give these armies a military edge. If the ‘right’ kind of technology is coupled with the ‘right’ group of determined decision-makers, power structures may shift quite significantly and suddenly. As such, the quantum of novelty may go a long way.

At present, commentators in the US military establishment consider the golden days of American technology leadership under threat, a darkening strategic outlook amplified by the ostensive ferocity, grit and determination of the new Eastern enemy. ‘We are playing a losing game’, the former Staff Director for the US Senate Armed Services Committee writes. ‘[N]ow we face highly capable and motivated competitors that are using advanced technologies to erode our military edge, and with it, our ability to prevent war, deter aggression, and maintain peace’ (Brose

2020). For William Carter, Deputy Director of the Center for Strategic and International Studies (CSIS), the US has entered ‘a new era of strategic competition with China, one defined by our competing progress in advanced technologies’ (Carter 2018, p. 2). Many scholars converge on the view that the ‘underlying driver’ of US-Chinese competition ‘is a race for global technological dominance’ (Schneider-Petsinger et al. 2019, p. 2).

The current US government certainly confirms this view in its public-facing communication. In his first address to a joint session of the US Congress in April 2021, President Biden proclaimed that America ‘is in competition with China and other countries to win the 21st Century’ (House 2021). As ‘China and other countries are closing in fast’, he continued, ‘[w]e have to develop and dominate the products and technologies of the future: advanced batteries, biotechnology, computer chips, clean energy’ (ibid.). A future quantum internet is part and parcel of this accelerating security arms race.

Yet it is important to note that US–Chinese rivalry is very much unlike the Cold War with the Soviet Union in that the USSR never posed a threat in terms of technological prowess, innovation, and economic capability. Competition with China is very different. Some commentators suggest that ‘the playing field does not favor the U.S. as the core underpinning element is its main weakness: efficiency’ (Kuo 2022). This is because ‘the support base is faltering, as its credibility among its allies has reached a historical low’ (ibid.). In this view, trust in American politics has evaporated both at home and abroad, which puts China is in a much better position to win the emerging technologies security arms race; a position the Soviet Empire never enjoyed.

However, it is still very much an open race, particularly with regard to quantum capabilities. Scoring particularly high on dimension (v) of the above-mentioned taxonomy, quantum technologies are marked by high degrees of uncertainty and ambiguity that characterise not only basic engineering principles but future applications and impact scenarios even more so. It is this high degree of uncertainty that causes particular trouble for strategists. Nodding to the earlier point that technologies are always embedded and have no intrinsic force that would make them inherently good or bad, some commentators in the domain of strategic stability studies argue that the problem is not emerging technologies as such but how they amplify uncertainties about adversaries' behaviours.

This is a very important point. 'Strategic stability calculations are therefore less about the power and number of weapons', Ronald F. Lehman II writes, 'than they are about anticipating human responses to new, different, and possibly inaccurate information about the circumstances, capabilities, and intent of others and ourselves' (Lehman II 2013, 150). Keeping adversaries in the dark about actual quantum capabilities and intent supports strategic ambiguity and increases uncertainty among strategic rivals.

The way the internet of the future is going to shape up is of ultimate strategic importance as the internet has moved to the core of human meaning-making: 'If strategic technologies are those that most influence change and our responses to it, then the fundamental strategic inventions concern what we know and how we think–languages, alphabets, the printing press, radio, television, the internet' , Lehman notes (p. 149). When it comes to strategic ambitions for internet technologies, the stakes are particularly high. Hence the question, 'How is the quantum internet going to turn out?' is at once a question about technological realities as it is one about influencing adversaries' present-day beliefs about such future realities. This is why, concerning the US–Chinese rivalry over the quantum internet, beliefs about what the quantum internet *can* do will matter just as much as what it is actually going to achieve. While quantum technologies are challenging and indeterminate enough to cause confusion, strategic uncertainty is further amplified by the embeddedness of quantum technologies in AI and ML policy.

On top of the many legal and domestic policy issues they bring up, AI and systems with autonomous capabilities (SACs) amplify the complexities that strategists already face (Krause 2021*b*). Quantum internet technologies can be expected to exacerbate this problem only further. Such an increase in complexification may seriously change the global landscape of deterrence and patronage: 'the supply and demand market for extended deterrence is likely to significantly shift with the inclusion of more capabilities' (Mehta 2021, p. 977). While nuclear weapons have proved the single biggest source of deterrence in the twentieth century, non-proliferation treaties ensured a limited choice of suppliers of patronage, as only a handful of powerful states have access to nuclear weapons. During the Cold War, countries would face a binary choice of alignment between either the US or the USSR. In this regard, strategic choice portfolios were manageable.

Today, however, the picture is much more mixed. Future quantum capabilities will offer non-proliferated states options for offering patronage in exchange for strategic alliances. 'For example, new forms of non-kinetic deterrent capabilities suggest that more actors, whether conventionally superior or nuclear-capable, may serve as patrons of extended deterrence', Rupal N. Mehta continues with a view to drones and hypersonic glide vehicles (ibid.). Strategic alliances with countries that promise access to super-secure QKD encryption, for instance, may suddenly become very attractive. China may be able to offer what could be called *quantum* *patronage* to previously unaligned states.

This prospect invites the serious question of whether quantum internet technologies should, or could, be contained. This problem adds to the whole range of ethical issues that the continuous employment of drones, for instance, already entail in countries that are not officially at war with states that have operational UCAVs in place (Enemark 2022). A secure quantum radar that communicates over quantum channels and masks not just attacks but prevents the very detection of drone employment to non-quantum actors, would add a whole new level to what is already a complicated ethical picture. The quantum internet, particularly if it emerges non-linearly with variable degrees of implementability and interoperability across competing states, may offer new forms of patronage that see established alliances splinter. The question of how the quantum internet is going to shape up, therefore, reaches far beyond immediate concerns about its governance framework.

2.2.1 Official US and Chinese policy positions

In March 2021, US President Joe Biden issued an *Interim National Security Strategic Guidance*, a quick and 'unusual step' (Ashford 2021) taken by the newly incoming administration to distance itself from the previous government. Traditionally, updates to national security strategies are not to be expected until midway through the first term of a new president. The strategy is outspoken about a 'growing rivalry with China' (Government 2021, p. 6). It pays particular attention to emerging technologies. They are mechanisms to not just 'prevail in strategic competition with China' but 'for America to out-compete a more assertive and authoritarian China over the long-term' (p. 20). The Guidance is a strong signal to allies that the US government considers strategic rivalry a much bigger question than the US–Chinese trade war that began under the Trump administration.

Not everyone agrees with the Guidance's hawkish stance. Commentators from established institutions such as the Carnegie Endowment for International Peace identify an unnecessarily charged rhetoric that frames the issue 'as a global contest between democracy and authoritarianism [which] also divides the world into opposing camps, while heating up an already tense relationship between the United States and China' (Chivvis 2021). Attesting to the notion of coproduction, emerging technologies get infused with new dimensions of meaning, they encapsulate ides of freedom and justice in a divided world. 'Such rhetoric', the authors continue, 'tends to reduce the space for diplomacy by adding a moral dimension to this conflict that raises the stakes yet is inherently unresolvable' (ibid.). However, it is no surprise that conservative voices find the strategy insufficiently substantive and not hawkish enough. The Heritage Foundation, for instance, laments too much 'virtue-signalling' and 'political sloganeering [that] seems jarringly out of place in a strategy document' (Spoehr 2021). Either way, the document certainly communicates that the US considers China a strategic rival that must be confronted head-on, particularly in the domain of emerging technologies.

The strategy defines US national security around three broad objectives: to 'protect the security of the American people', 'expand economic prosperity and opportunity', and 'realize and defend the democratic values at the heart of the American way of life' (Government 2021, p. 9). Emerging technologies are considered instrumental to these priorities. Established in 1993 and comprised of cabinet-level councils of advisers, the US National Science and Technology Council (NSTC) identifies technologies 'with the potential to further these objectives' (NSTC 2022, p. 6).

The NSTC serves as the principal body that coordinates science and technology policy across the US government. Its 'Fast Track Action Subcommittee on Critical and Emerging Technologies' maintains a list of critical technologies which are 'a subset of advanced technologies that are potentially significant to U.S. national security' (NSTC 2022, p. 10). On top of established fields such as AI, autonomous systems and robotics, the latest updates to the list saw the inclusion of 'Quantum Information Technologies'.

This strategy recognises the security implications of quantum technologies. It builds on the 2018 NSTC report *National Strategic Overview for Quantum Information Science*, produced by the Subcommittee on Quantum Information Science and published by the Executive Office of the President of the United States Government (2018). The overview holds that quantum information science is 'the next technological revolution' and aims to promote realising its 'national security benefits' (p. 6). With a view to China, export controls are explicitly mentioned: the quantum strategy aims to 'ensure consistent application of existing classification and export control mechanisms to provide the largest amount of information possible to American universities and industry about actions related to QIS [Quantum Information Science] research' (p. 8). This is to 'encourage economic opportunities, protect intellectual property, and defend national-security-relevant applications' (ibid.). Nodding to the Dirac notation practice in quantum physics for describing the superposition state of quantum objects, "$\langle quantum|gov\rangle$" has since been established, the US National Quantum Initiative. It draws funding from the 2019 National Quantum Initiative Act (Smith 2018) that seeks to 'provide for the continued leadership of the United States' in the quantum domain.

In February 2020, the White House National Coordination Office published *A*

Strategic Vision for America's Quantum Networks (US Executive Office of the President of the United States 2020). The document sets out a government initiative to make headway in building a quantum internet; 'a vast network of quantum computers and other quantum devices [which] will catalyze new technologies that accelerate today's internet, improve the security of our communications, and allow dramatic advances in computing' (p. 2). Bearing all the hallmarks of the Trump administration's penchant for rhetoric, it finds that 'America is poised to revolutionize national and financial security, patient privacy, drug discovery, and the design and manufacturing of new materials, while increasing our scientific understanding of the universe' (ibid.). Over the next two decades, 'quantum internet links will leverage networked quantum devices to enable new capabilities not possible with classical technology' (p. 3). The US government has high expectations: although not yet built, the quantum internet is already tasked to achieve a great many new things; even secure the 'American way of life'. Above all, it is expected to defend US dominance against an increasingly assertive China. While perhaps toned down and more nuanced in its language, President Biden has not diverted from this agenda.

In this 'quantum war of words', if you will, also China mobilises a strong rhetoric that is couched in nationalism and patriotism. The Chinese quantum strategy sits within larger strategic technology policy objectives. President Xi Jinping pursues a policy to realise, what is now called, the 'dream of national rejuvenation' (Goldstein 2020, p. 164), which, diplomatically put, involves a 'bolder' approach and the 'clarification' of long-standing international aspirations (ibid.). The Chinese government too holds leverage over emerging technologies the key to global dominance. 'In the eyes of the current Chinese leadership, technological prowess is one of the accoutrements of power' (Schneider-Petsinger et al. 2019, p. 3).

Leveraging future internet technologies is a signal of China's global ambitions. Commentators find a 'strong sense of self-reliance', and a new focus 'on surpassing the US in a broad range of technologies while asserting that China can afford to decouple from the US in terms of pursuing an independent technological development path' (ibid.). Quantum technologies are an opportunity for China to present to the world a genuinely Chinese technology that does not duplicate, imitate or simply copy Western innovation. With a sense of foreboding, *China Daily* confidently claims that the country has become 'a global leader in the fields of 5G, artificial intelligence, big data, internet of things, robotics, quantum computing, and outer space research' to the effect that national rejuvenation is going 'to have a profound impact on [the] world' (Wren 2021).

China's quantum policy has its origins in the early iterations of its 'Big Data Strategy', officially announced in 2014 (Gorman 2021). Upon the adoption of the 13th Five-Year Plan (2016–20), President Xi, addressing the National Congress in October 2017, ordered the provinces to 'promote the deepened integration of Internet, big data, and artificial intelligence with the real economy' (ibid.). The strategy sits alongside the well-known 2015 plan 'Made in China 2025', which aimed for technology leadership in AI and ML by the end of the decade ahead. 'New advanced information technology' and 'Automated machine tools & robotics' were the two biggest priority sectors the plan had particularly emphasised (Kennedy 2015).

Quantum technologies sit at the core of the plan. China's news agency *Xinhua* published an official statement of the '24th Collective Study of the Political Bureau of the Central Committee' in October 2020 in which President Xi 'emphasized a profound understanding of the great significance of advancing the development of quantum science and technology, and strengthened the strategic planning and system layout of quantum science and technology development' (Xinhua.Net 2020). Quantum network technologies are a top priority for the Chinese leadership, which has since repeatedly signalled its quantum ambitions (Kania 2021). President Xi seems personally invested in this.

The ways in which states seek to signal power and ambition is the subject of a large body of research in political science (Crisman-Cox & Gibilisco 2019, Gartzke et al. 2017, Sobel 2009, Whang 2010). Beyond such an instrumentalist interpretation that considers language as a means to an end, discourse itself however seems of particular importance to the Chinese leadership. Elsa Kania draws attention to this under-researched aspect of Chinese ambition: its pursuit of a 'right to speak', or 'discourse power' (*huayuquan*) by which the Chinese leadership seeks to project discursive and norm-setting influence (Kania 2018). In a dedicated politburo session on this topic, President Xi seems to have emphasised, in his own words, the strategic relevance of 'accelerating the promotion of China's global discourse power and rule-making in cyberspace'–China ought to become a 'cyber superpower' (ibid.). For China, standard-setting for the quantum internet of the future is inseparable from technological innovation in this domain. Internet governance and standard-setting are the flipside of quantum internet R&D and must be pursued in tandem.

This is a hugely important point: for the Chinese leadership, actual engineering and technology leadership in quantum technologies and questions regarding their standardisation and governance *are not two separate issues but part and parcel of a comprehensive quantum strategy.* Building the quantum internet requires i) leverage and property rights over key quantum technologies, and ii) 'discourse power' to set standards, norms and governance models that determine who can use this new technology, and how. This establishes a firm link between leverage over technologies (expressed as property rights established by patents) and the domains of governance and standard-finding.

A Chinese-shaped governance model for the quantum internet would be a milestone not just for promoting *huayuquan* but for 'rejuvenating' the nation. It would mean the end of an internet governance and standards model that, over the past 40 years or so, has served Western interests very well. The question of quantum internet standards is one where questions of international security, strategy and cyber dominance intersect. The Chinese leadership is mindful of these intersections, so much so that they have launched a dedicated standards strategy plan that couples patenting activity with standard-finding.

2.2.2 Leveraging patents and standards for strategic ambitions

There is growing interest in the strategic implications of standard-setting at international institutions–a topic that Western alliances have woken up to rather late in the game, as experts interviewed for this thesis suggest (see Chapter 5). China in particular has been busy installing senior executives at such organisations. Over the past ten years, 'the number of committees in the International Organisation for standardisation [sic] where the secretariat is headed by a Chinese national increased by 73 percent', the Council of the European Union finds (ART 2020). China seems to be pursuing a dual strategy. It patents innovation in quantum internet technologies at pace in order to establish property rights and thus have leverage over how the quantum internet is going to be engineered. Parallel to this China seeks to place in key positions influential actors who in the future may decide favourably for Chinese standards.

This is why it is so important to investigate quantum internet governance and patenting activity in tandem. Standards found by the ITU or ISO ‘have great sway over the standards adopted around the world’; as such they can ‘provide enormous economic advantages to companies that hold patents on technologies essential to those standards, known as standard essential patents or SEPs’ (Schaefer & Pletka 2022, p. 2). As Chapter 4 discusses in detail, Chinese quantum internet technologies, in particular in the domain of satellite-based quantum communication, have a strong potential to become SEPs. As far as the quantum internet is concerned, it must be concluded that China is patenting new internet technologies on a large scale while, in parallel, building up ‘soft power’ (Nye 2005, 2019) capabilities across international organisations to increase their chance of adoption as normative engineering principles.

As far as the Chinese leadership is concerned, the long-term objective of ‘national rejuvenation’ requires a strong link between patenting Chinese innovation and pushing for a new Chinese-dominated standard and governance regime. ‘In the eyes of the Chinese leadership, setting the global governance agenda is part of projecting China’s ‘discursive power’, in other words, testing its ability to shape the international norms and widely practised standards’ (Schneider-Petsinger et al. 2019, p. 28). This dual effort is anything but a state secret. The aforementioned ‘Made in China 2025’ strategy is now superseded by ‘China Standards 2035’. The strategy is bold: future standards for internet technology ought to be Chinese. The strategy aims ‘to create a blueprint for the Chinese government and leading tech companies to set global standards for emerging technologies, such as

5G, Internet of Things (IoT), and artificial intelligence (AI)' (Wu 2022). In its official communication, 'China views standardization as a way to strengthen its research and development (R&D) ecosystem by elevating whole-sector capacities, particularly in critical and emerging industries like AI, quantum computing, and biotechnology' (ibid.).

Shared standards increase the economic efficiency of Chinese industries while signalling to the rest of the world that China can offer a comprehensive package deal: not just technological specifications and patents to build a new quantum internet but also the right set of standards to manage and integrate this fascinating new technology. For many countries, this could prove too sweet an offer to resist. In a RUSI talk in May 2022, Dr Ian Levy, Technical Director of the UK's National Cyber Security Centre, expressed concern over the lack of principled engagement of Western alliances in this area. Levy pointed out that it is no longer good enough for the West to simply warn about the adverse security implications of emerging Chinese technologies. Rather, Western powers should try and offer alternatives–how are Western technologies and standards better? Unless bold competing specifications can be found, there is little incentive for countries to not adopt a Chinese system (Levy 2022). As discussed in Chapter 5, interviewees for this research make similar points.

While the West is somewhat stunned by the Chinese *patents + standards* rollout, China proudly points out just how big an advancement it has made at standard-setting organisations. Over the past couple of years, 'China has increased its number of ISO and IEC proposals, reaching an annual growth rate of 20%, which shows China's ambition to shape the world through standard setting' (Mbeba 2021). In particular, Articles 17 to 21 of 'China Standards 2035' make clear just how much

China seeks to extend its influence over international bodies. Control over 'system design and rule-making' offers the chance to establish a 'premium position in the global market' and 'first-mover advantages in key sectors' (Wu 2022). Commentators fear that the 2035 strategy is for China to exercise pressure and eventually lock in 'those developing nations in which China has significant investments' (Gargeyas 2021). This will further increase China's bargaining power at international institutions further. Ultimately, 'these standards serve as China's weapon to eventually displace the West in the high-stakes technology battle' (ibid.).

In particular the ITU has gained notoriety for China-friendly policies since the installation of Houlin Zhao as Secretary-General in January 2015. For instance, Chinese companies ZTE, Dahua and China Telecom have successfully pushed for new facial recognition standards that also cover video monitoring, city and vehicle surveillance (Gross et al. 2019). The speed of adoption of these standards across the world following ITU approval has raised eyebrows among human rights activists. 'African states tend to go along with what is being put forward by China and the ITU as they don't have the resources to develop standards themselves', *The Financial Times* cites Richard Wingfield of Global Partners Digital, an advocacy group. Not only has China's influence at the ITU grown significantly over recent years, but what is more, delegates warn that, increasingly, Chinese corporations themselves, not policy officials, draft standards proposals (ibid.). Chinese interests have taken 'a big seat at the AI governance table' (Ding et al. 2018). It is certainly true to suggest that these days, 'the setting of technology standards becomes more pivotal in the race to economic and technological supremacy' (Schneider-Petsinger et al. 2019, p. 27). Chapter 5 discusses Huawei's recent 'New IP' proposal at the ITU in more detail, a notable attempt by Chinese officials to reshape the internet of the future.

2.3 The international political economy of network standards

Why are internationally recognised standards so important to China? A brief history of internet standards demonstrates their pivotal role in making the network the global success it has become. To better understand China's determination to push for Chinese standards, it is important to realise that current internet standards are Western standards. However, this being the case, they have always been contested. Data packaging standards had already been of great concern at a time when ARPA protocols, which governed the precursor to the internet, the US Department of Defense's ARPANET, were in the exclusive domain of only a handful of elite research networks.

At the time, ARPA's TCP/IP suite of protocols had quickly emerged as the de facto standard for the newly emerging internet. This was not because of any legal barriers to other solutions but thanks to the widespread distribution and early uptake of the protocol in the early 1980s. The US Department of Defense had effectively made the TCP/IP suite of protocols the gold standard of data packaging for the commercial internet when it split ARPANET from its military network applications in 1984 (Cohen-Almagor 2011).

Research sites in the US and Europe were keen to adopt a universal framework, which made TCP/IP particularly appealing. Being of military grade, the protocol suite signalled certainty and reliability (Abbate 2000, Hauben et al. 2007). Universities such as Stanford and University College London in the UK would then follow in adopting it also, thus contributing to the suite's proliferation (Cerf & Aboba 1993). The US government's first-mover advantage in setting the TCP/IP standard at the time allowed an exclusive, restricted-access network technology to become the ‘apparently mundane utility, like mains electricity’ (Naughton 2016, p. 5) that the internet is today. Leverage over a nascent technology made it possible to push for a global standard–a strategy China presently aims to repeat, be it in the domain of ‘New IP’ (see Chapter 5) or, presumably, future quantum networks. Standard-setting is a long-term game and an uphill struggle. IPv6, the update to the Internet Protocol launched in 1995 but not formally ratified until 2017, illustrates the complexities involved in moving between two interoperable standards: several transmission mechanisms had to be designed for switching from IPv4 to its successor (Baker et al. 2011).

The history of the TCP/IP suite is one example of many where domain-specific standards have disseminated across industries and borders and become global de facto standards that support market integration, and ultimately help domestic industries to dominate global markets. The mass adoption of the IBM ‘Personal Computer’ so that the PC would rapidly become the ‘de facto standard microcomputer’ (Zusmann 1982) in the early 1980s is a good case in point. As far as software is concerned, the ubiquity of MS Windows and MS Office over the past three decades has caused regulators on a number of occasions to challenge Microsoft’s business practices; an anti-trust case in the US in 1998 being an early and quite prolific one (Economides 2001).

The success of Adobe’s Portable Document Format (PDF) in becoming the preferred type for filing and printing documents online catapulted it to the status of de jure standard as the International Organization for Standardization’s ISO 19005-1:2005. Similar stories can be told about various connectors and adaptors that are integral to network architectures: RCA, XLR, MIDI, HDMI and USB have emerged not as legal requirements but as winning specifications which, at some point in the diffusion process, users could no longer do without. For network industries and service providers that aim beyond domestic markets, a common standard is critical. A shared standard means (market) power.

With the emergence of the Internet-of-Things (IoT), the strong affinities between political power, commercial success and governance frameworks have only become more pronounced (Čolaković & Hadžialić 2018, Greengard 2015, Mukhopadhyay 2014). The IoT adds to global cybersecurity concerns: with the number of interconnected devices projected to reach 41.5bn by 2025, producing 79.5 zettabytes of data (IDC 2019), the IoT contributes to a vast expansion of the 'attack surface' (Costigan & Lindstrom 2016) for cyber warfare.[2] With the emergence of a 'mega market' (Kramp et al. 2013, p. 1), which crosses homes and buildings, smart portable devices, transport, factories and utility networks, the challenges around compatibility and interoperability are profound. Itself an umbrella term, IoT variously captures some if not all networks in the large set of traditional personal area networks (PAN) such as Bluetooth and WiFi, machine to machine communications (M2M) in various specifications, wireless sensor networks (WSN) and near field communications (NFC) (Al-Fuqaha et al. 2015, Ponnusamy & Rajagopalan 2018).

Numerous domain-specific protocols compete, and a significant number of state-backed as well as industry-sponsored bodies are busy developing frameworks that are hoped to unify IoT standards. Most prominently, these are the Internet Engineering Task Force (IETF)'s IoT Working Groups, the International Telecommunication Union (ITU)'s ITU-T SG20 Study Group, the International Organi-

[2] In cybersecurity, the 'attack surface' is the universe of possible attacks: a collection of all the different ways an attack could unfold. The term 'attack vector' then describes a specific path or route an attacker has chosen to compromise the system.

zation for Standardization (ISO)'s ISO/IEC JTC1 Environment and the Institute of Electrical and Electronics Engineers (IEEE)'s IoT Initiative.

Adding to such regulatory complexities and overlaps, surveys find that businesses and consumers have quite opposing preferences regarding future governance models for the IoT, in particular when it comes to the robustness of privacy and security arrangements (Meddeb 2016). The current regulatory situation is best described as messy 'to the extent that it is often compared to a war' (Meddeb 2016, p. 40). As Chapter 5 discusses in full, given the stakes of these network governance wars, China hopes to drive a wedge into the system and break decades of US dominance.

China recognises as much as the US that communication networks enjoy non-linear economies of scale. The economics of networked services are very different from those of substitution products where the demand for product i is a positive function of the price of product j offered by a competitor: if the price of a good, such as a fizzy drink, rises and a replacement is easily available, the demand curve is likely to shift towards the product that has now become marginally more attractive (Varian 2014). Networks however are peculiar in that they generate network effects, a form of externality 'in which consumers' utility and/or firms' profits are directly affected by the number of consumers and/or producers using the same (or a compatible) technology' (Shy (2011, p. 119), also see Shapiro & Varian (1999a,b)). When the use value of a given technology is a positive function of the user base of a rival firm that offers a compatible service, issues of compatibility quickly turn into non-trivial challenges for regulators.

This is particularly complex when multiple standards, rather than a single one, are likely to yield a welfare-maximising level of output (Farrell & Saloner 1986).

The (at times conflicting) demands towards compatibility standards of network technologies quickly grow with the number of devices, software and apps that are available and which crucially depend, either directly or indirectly, on standards to ensure their viability. The IoT only exacerbates this problem. Networked markets are 'two-sided' (Rochet & Tirole 2003) in that the proprietors of, say, streaming services or food delivery apps need to attract both consumers (viewers, customers) and producers (content providers, participating restaurants) to their platforms. The complexities of cross-substitutions introduce new regulatory trade-offs and challenges due to the fuzziness of tipping points and competitive equilibria (Mortimer 2019). In this rather murky situation, the emergence of quantum technologies will provide state actors with incentives to shift standard-finding towards domestic suppliers. Standards matter a great deal in any industry but have even more significance for networks as they have knock-on effects well beyond standard-bearing firms. Shaping future quantum network standards early on in the game may promises long-term gains within and outside quantum-enabled industries.

As pointed out in the introductory chapter, physical network infrastructures, rather than the user behaviour they afford, are increasingly becoming the object of struggles over control and influence. The aforementioned 'turn to infrastructure' suggests that policymakers are beginning to redirect their attention to 'points of infrastructural control' (Musiani et al. 2015, p. 4). Of course, the question of internet standards has always been a political one (DeNardis 2014*b*). 'Standards are a political issue because they represent a form of control over technology,'– and as such, they can quickly become 'matters of foreign policy', Janet Abbate comments on the evolution of the ARPANET in the early 1980s (Abbate 2000, p. 147-48).

It is because of these entanglements of global power, network technologies and standard that governance wars over the quantum internet should not be considered in isolation from past struggles but rather the next chapter, or evolution, in an ongoing battle between the leading powers for strategic dominance and global reach. Arguably, the stakes are even higher today. Given that the internet, the successor of the ARPANET, is built on rather old technology, what if a new infrastructure is on the horizon that promises unprecedented levels of security and compute resources? Significant changes to internet infrastructure are on the way, quantum-driven or digital, as the 'traditional Internet architecture needs to be revised to match the IoT challenges' (Al-Fuqaha et al. 2015, p. 2348). Even if this were not the case, or the case for a fundamental update of internet infrastructure is overstated, it will be increasingly difficult to resist calls for change. What is more, the advent of a quantum internet, built on a radically different computer architecture, has created an even larger appetite for infrastructural control. The quantum internet is already being framed in security terms well before its arrival.

2.4 The quantum internet and security governance

The discussion so far has established how internet governance (and the standard finding that comes with it) has become a national security concern. Internet governance fora are places where interstate rivalry plays out. In her widely acclaimed study of the history of the internet, published more than two decades ago, Jane Abbate already found that the 'debate over network protocols illustrates how standards can be politics by other means' (Abbate 2000, p. 179). Laura DeNardis considers internet governance to be a ‘dark art’ that raises uneasy questions about the ‘the conditions under which governments should (or could) tamper with communication technologies for national security or law enforcement objectives’ (DeNardis 2014*b*, p. 200). The quantum internet will be tasked to accommodate a wide range of commercial as well as policy interests, many of which will not align easily. The study of these dynamics of alliance-forging, conflict and manoeuvring requires a flexible concept that embraces the fact that security is a multi-layered phenomenon shaped by a great many forces.

In the current debate over whether the internet is likely to fragment ((O’Hara & Hall 2018)), Milton Mueller finds a transnational power struggle over national security and sovereignty that ‘pits global governance and open access against the traditional territorial institutions of government’ (Mueller 2017). China in particular seems to consider the current internet governance framework primarily a vehicle to advance US interests, as ‘the power of the current Internet governance model strengthens the global power of the American example’ (Yannakogeorgos 2012, p. 103). More than any of his predecessors, China’s President Xi is determined to change this. Given how emerging technologies have moved centre-stage in narratives of global power and dominance as of late, as discussed above, it seems right to investigate the evolution of quantum internet governance from a security studies perspective. Any such angle should be mindful of the intersections of interests that co-produce the quantum internet.

The specific *security governance* framework that this thesis adopts recognises that a multitude of competing actors is involved in internet governance and standard finding. Yet it maintains that state actors (or their representatives) are the dominant players, today more than ever. The state enjoys this central position as it remains ‘the principal unit of political organization of the world’s populations’ and ‘the repository of a monopoly of legitimate violence’ (Kolodziej 2005, p. 26), which manifests in bargaining power in international diplomacy.

This position very much acknowledges that private corporations and lobbying groups can be very powerful indeed. This fact is reflected in the ways in which state actors often seek to advance domestic industries by setting industry standards that benefit corporations at home. The private sector lobbies officials to this effect. To say that state actors are the agents in international bargaining games is not to deny the immense power other actors may have; oftentimes state representatives quite openly aggregate and channel corporate interests. The realities of the international political economy of standard finding has always been a part of this debate. For instance, the question of whether ICANN primarily serves US corporate interests stretches back more than twenty years (Weinberg 2000).

The picture only gets muddier given the increasing blurring of institutional boundaries between state and non-state actors today. This is certainly a growing problem in China. For instance, Huawei’s corporate governance model suggests close ties with China’s central government, which complicates drawing well-defined distinctions between public and private sector interests at China’s towering telecommunications corporation (Balding & Clarke 2019). But once again, it would be unfair to single out China in this regard. Western bureaucracies have a significant ‘revolving doors’ problem where public regulators and legislators would oftentimes move between public and private sector jobs with little scrutiny.

For instance, empirical research across 32 OECD countries shows that ‘central bank governors with past experience in the financial sector deregulate significantly more than governors without a background in finance’, a phenomenon the authors label the 'career socialisation hypothesis' (Wirsching 2018). Their results 'also indicate that finance ministers, especially from left-wing parties, are more likely to be hired by financial entities in the future if they please their future employers through deregulatory policies during their time in office' (ibid.). Regarding issues pertaining to internet governance, former UK deputy Prime Minister Nick Clegg's move to a senior lobbying position with Meta highlights that cosy public-private sector relations are certainly not a Chinese issue alone. A security governance perspective must avoid singling out China in this regard.

In response to a surge of foreign media interest in Chinese corporate governance practices and company relationships with the Communist Party, Chinese firms seem to have responded by putting a brake on public communication: today, 'they are acquiring market share under the radar, through small deals' (Weinland 2021). Chinese regulators seem to favour this less visible approach, which avoids the attention-grabbing headline news of the past about trophy acquisitions of Chinese firms, such as Italian football teams (ibid.), and Chinese corporations seem to be playing ball. This is not to suggest that only Party interests would matter in China. Just as everywhere else, state actor interests are interwoven with those of the private sector. Countries differ in terms of how effectively their media, NGOs and advocacy groups can influence state actors, and state-society relations are complex. Despite these involvements, however, this thesis takes the position that state actors ultimately enjoy degrees of freedom in international negotiations that private sector agents do not have, which is why its focus is state-level strategic competition. But how exactly do government, governance models and security interests relate?

2.4.1 Quantum internet governance as security governance

The term ‘governance’ means different things to different people. For the purposes of this thesis, it includes both state and not-state actors in capturing the sway different groups have over the internet. In this sense, government in its broadest form can be considered a ‘subset’ of governance, the latter being a set of ‘processes and institutions, both formal and informal, that guide and restrain the collective activities of a group’ (Keohane 2003, p. 202). As outlined above, this thesis adopts a reading of governance that constructs government as the fundamental but not exclusive source and driver of internet governance regimes.

Thinking of state and non-state couplings in this fashion is an established way of conceptualising how influence manifests in policy. Connections between particular security practices and governance models that saw the emergence of the term ‘security governance’ date back to the early 1990s (Kolodziej 1992). However, the concept did not gain traction until the mid-2000s (Sperling & Webber 2014). While many popular textbooks in security studies in the late noughties did not cover this newly emerging sub-discipline (e.g. (Buzan & Hansen 2009)), it has now become a cornerstone in introductory texts to the security studies discipline (e.g. (Cavelty & Balzacq 2017)). It is a useful heuristic tool and a framing for the analysis of the processes that shape the quantum internet.

As a concept, ‘security governance’ captures the practices that state actors engage in to manage new forms of security threats and risks that require international cooperation across multiple institutions, for example counterterrorism, climate change and public health emergencies. In its early iterations, the concept was construed very broadly and ‘defined as an intentional system of rule [sic] that involves the coordination, management and regulation of issues by multiple and separate authorities, interventions by both public and private actors, formal and informal arrangements, and purposefully directed towards particular policy outcomes' (Kirchner & Sperling 2007, p. 3). This thesis narrows down this maximally wide definition to the analysis of quantum networks.

Applied to the realm of internet governance, *quantum internet security governance*, or QISG in short, would capture that which i) is an object of security concern to state actors, ii) requires an internet policy response in the governance domain and iii) involves actors outside government, such as international standardisation bodies, industries, universities and research institutions. QISG is particularly mindful of how the quantum internet is coproduced not just in a mash-up of domestic interests but also against larger tropes of strategic competition and global reach.

QISG is not so much a theory but a way of analysing the power dynamics at play in internet governance. At present, security governance is usually framed in terms of a 'conceptual framework' or 'heuristic device' that aims to identify the mechanisms by which 'the good of security is sought and obtained within a given geographic or policy domain' (Sperling & Webber 2014, p. 127). The term assumes 'a multi-layered arrangement that involves a wider range of actors, rules, and practices'; it reflects an understanding that the context in which security is organised is a contested one 'wherein power is dispersed and sources of authority are hotly disputed' (Cavelty & Balzacq 2017, p. 29). This statement is certainly appropriate to characterising the flaring of great-power rivalry over future networking and computing standards that involves struggles between the private sector and government interests. Recent scholarship points to the steady complexification of internet governance, for example, regarding the rise of influential Chinese entrepreneurs and tech companies in governance processes who seem to be influencing official Chinese positions (Radu et al. 2021). The Chinese leaderships seems to have responded by clamping down on Chinese big tech's growing influence–'as the Communist Party whips digital platforms into line, trillions of dollars in market value are at stake', *The Economist* fears (Economist 2021). This point will be discussed in more detail in Chapter 5.

The rise in popularity of security studies literature that focuses on governance, rather than governments alone, is grounded on the observation that over the past three decades, multilateralism, globalisation and privatisation have produced various new mechanisms of influence and control. Security is coproduced beyond traditional government domains and in ways that require 'multi-actor and multi-level forms of coordination' (Schroeder 2011, p. 34). China's concerted efforts to extend its influence over international standard bodies is a good example of this phenomenon. The literature points to the emergence of security regimes that reach beyond a purely state-centred, top-down hierarchical system built on coercion. Security regimes and practices have evolved towards a horizontal, networked blending of authority that promotes order by consent, bargaining and diplomatic wrangling (Breslin & Croft 2013).

Yet it is important to note that while there are many more parties at the governance table today, it cannot be assumed that in and of itself, diversity in participation will translate linearly into a diversity of opinion. While in China private corporations may be coerced to follow the official Party line, US positions are oftentimes shaped by the 'big tech' companies' strategic concerns. 'Google, Facebook and others want to set the rules, but without a mandate or oversight [...] technology companies think they should be deciding public policy, not governments', *The Financial Times* grumbles (Schaake 2021). Arguably, governance has become more complex, but as the Chinese case of disciplining domestic big tech industries shows, state actors ultimately retain control and are not shy to exercise their powers.

QISG, then, seeks to highlight the at times affirmative, at times contradictory dynamics in finding a governance principle for the quantum internet. Rather than studying security issues in isolation, as a conceptual framework for 'doing' security studies, QISG seeks to inquire into 'how such arrangements are aggregated in a particular region or issue area involving relationships *between* a multiplicity of actors engaging in common rather than isolated and unconnected acts' (Sperling & Webber 2014, p- 129, emphasis in original). Such a *betweenness* is particularly relevant for the study of a coupling of patents and standardisation policies. For any global actor, the more leverage over innovation, the easier it becomes to argue for a standard, and ultimately a governance principle, which establishes said innovation as the new normal. Thus, QISG seeks to investigate the multi-level processes of interaction by which internet security in the quantum domain is coproduced through patenting and standardisation policies. Both should be considered in tandem, and the next chapter develops a methodology for doing so.

For the chapters that follow, the concept of QISG is best construed as a heuristic tool, a way of thinking about patenting, standard-setting and governance-making in the domain of quantum internet technologies and how these activities relate to questions of power and influence. This is no radical deviation from tradition: 'security governance's main claim to fame is conceptual not theoretical' (Sperling & Webber 2014, p. 128). To highlight, from a security governance perspective, how state actor interests drive practices in quantum internet governance means being mindful of larger and long-term strategic concerns at play in interstate interaction.

While conscious of complexities that are not one-sided, this position maintains that states aggregate and bundle different and at times conflicting domestic interests, and ultimately make political realities happen. While it does not deny the impact that powerful individuals can have in the performance of politics–President Trump taking aim at President Xi serves as an illuminating example–this thesis is, ultimately, curious about how power is coproduced along many axes. As such, it aligns with critical voices in the security studies tradition that point to persistent, structural factors: 'our argument is that security governance has become overly preoccupied with agency and has neglected structure' (Sperling & Webber 2014, p. 127) seems an appropriate comment to make. In this spirit, the empirical analysis in the following chapters should be read as an attempt to integrate broader, multiplex phenomena in a discussion of the forces that shape the quantum internet.

2.5 Main points of Chapter 2

To recap, QISG is about mapping processes of multi-actor involvement in the emergence and control of security and governance practices in quantum networks. As outlined above, this is to be achieved through an enquiry into the aggregation and integration of arrangements that involve a multiplicity of actors across different regions. These practices will not necessarily align. State actors respond to private sector and civil society interests in feedback loops. Bargaining power is differentiated, disputed and non-linear. Various institutions are involved that also differ in terms of reach, clout and legitimacy.

Networks are at the heart of such a framing. ‘When government tasks and authority are delegated downwards (localization), upwards (supranationalization), or sideways (privatization) [. . .] governance in networks becomes important’ (Cavelty & Wenger 2020, p. 12)–in a sense, the architecture of the quantum internet will mirror the structure of powers that seek to exploit it. The governance model for the quantum internet will not be decided in a single top-down effort but rather found in the struggle between the two superpowers. Two factors seem paramount here: technology leadership and leverage, and influence over standard-finding bodies. If either the US or China can offer a reliable deal for quantum internet technologies, many parties will find it hard to say no to the standard that is bundled with it (cf. (Levy 2022)). As it stands, it seems that China is particularly invested in making this happen. The US and its allies are playing catchup.

The above discussion has demonstrated just how much emerging technologies matter in the strategic rivalry between the US and China, and how both countries seek to extend power by maintaining a competitive technological edge. Both rivals consider quantum internet technologies of massive importance to realising their strategic ambitions. One of the key points of the review above is that maintaining a critical edge in emerging technologies, and thus cementing dominance, requires thinking beyond technology leadership and leverage alone. An advantage in engineering terms must be complemented by standards and governance models that support the diffusion of new technology.

China has realised this a while ago: ‘a government-sponsored “patent fever” has led China to file more than any other country in the world’ (Arcesati 2019). The logic seems clear. First, it secures leverage over key quantum technologies. This is established through patenting activities. Then, it seeks control over their implementation and integration by dominating the standard-finding process. Of course, this is what the US has always done, if perhaps in a less centralised, less top-down fashion. Alphabet, Amazon, IBM, Microsoft and Qualcomm own 'standard-essential patent portfolios' (ibid.) that had given them a decisive competitive edge for many years. A critical analysis of Chinese ambition must not ignore that in the eyes of the Chinese leadership, China only wants to excel at a game the West has always played.

The US still enjoys a significant lead. For instance, despite heavy investment into its chipmaking industry, China's reliance on foreign semiconductors is a constant headache for the Chinese Communist Party. China's trade deficit in integrated circuits 'has almost doubled from the equivalent of $135 billion in 2010 to $240 billion in 2020' (Chiang 2022). However such dependencies should be no grounds for Western strategists to relax. After all, it will not be necessary for China to surpass the US along all axes of technology. In the short term, it will suffice to make enough progress so as to compromise and slow down American activity: 'while we often talk of "technological parity," when it comes to these technologies, in many ways it is less important whether their technology is "as good as ours" than whether it is good enough to render our capabilities ineffective' (Carter 2018, p. 6). China has significant potential to disrupt the status quo even if many of its quantum patents will not turn into gold standards for future internet technologies. The next chapter develops a research methodology for this thesis, and Chapter 4 discusses in more detail how China has made considerable progress in many fields of quantum communication–perhaps enough to give it a competitive edge in shaping the quantum internet.

The below collects the major takeaways of this chapter.

Strategic competition and national security

2.a At a time of intensifying great-power rivalry in an increasingly multi-polar world, state actors re-emerge as important drivers of internet governance regimes.

2.b For Chinese and US strategists, national security now has network security at its flipside.

2.c Over the past couple of years, national security agendas have deepened and now include a considerable infrastructural component: the basic infrastructure of the internet has become an object of strategic competition between the leading powers, in particular the US and China.

2.d The quantum internet is part and parcel of a larger emerging tech and security arms race between the US and China.

2.e Quantum internet technologies may present quantum-enabled state actors with new capabilities to offer what could be called 'quantum patronage' in return for a commitment to strategic alignment and alliance-building.

China

2.f China aims high and seeks to offer not just novel internet technologies but standardisation and governance packages alongside them that help lock in participating states and thus slowly erode US dominance.

2.g Quantum technologies are an opportunity for China to present to the world a genuinely Chinese technology that does not imitate or duplicate Western inventions.

2.h For the Chinese leadership, actual engineering and technology leadership in quantum technologies and questions regarding their standardisation and governance are not two separate issues but bundled in a comprehensive quantum strategy.

2.i China has been patenting emerging technologies at scale while, in parallel, it seems to be building up 'soft power' capabilities across international organisations to increase their chance of adoption as normative engineering principles.

Internet standards and governance

2.j Standards matter a great deal in any industry but have even more significance for networks as they have knock-on effects well beyond standard-bearing firms. Shaping future quantum network standards early on in the game promises long-term gains within and outside quantum-enabled industries.

2.k Democratic, multi-stakeholder standard-finding for the next generation of the internet is likely to be a thing of the past.

QISG

2.l Patenting activity and standardisation and governance-finding for the internet should be considered in tandem.

2.m The quantum internet will be 'coproduced' in that it will be shaped by various factors; strategic ambitions for global dominance, market forces, research ecosystems and technological affordances all intersect.

2.n With the above in mind, QISG studies the quantum internet along three axes: i) it being an object of security concern to state actors, ii) as requiring an internet policy response in the governance domain and iii) as a network that involves actors outside government, such as international standardisation bodies, industries, universities and research institutions.

2.o QISG is about mapping processes of multi-actor involvement in the emergence and control of security and governance practices in quantum networks. It is an inquiry into the aggregation and integration of arrangements that involve a multiplicity of actors that have stakes and vested interests in pushing quantum internet technologies.

Chapter 3

Methodology

This chapter explains the choice of methods for this thesis with a view to the qualitative and quantitative character of the subquestions it pursues. It develops a justification for a mixed-method approach to studying issues of power and governance surrounding the emergence of the quantum internet. The literature review chapter has established how novel internet technologies demand new standards and governance regimes for the projection of power. This is particularly true for quantum technologies as reflected in official Chinese communication. 'Hard' quantum capabilities require 'soft' power in the standards domain. Together, they provide opportunities to establish quantum technology leadership and make significant gains in the competition over emerging technologies.

The particular choice of data sources and methods discussed below seems best suited to answer the research questions that Chapter 1 has developed. The data capture the political dynamics to shape standards as well as the technical dimensions of quantum technologies. Aspects of technology as reflected in patenting activity is captured in quantitative analysis, while the somewhat more elusive and less clearly demarcated area of standards policy and strategic competition is captured in interview data. The coupling of methods for studying verbal as well as quantitative data–the qualitative study of a corpus of interviews and the statistical analysis of patenting data–mirrors the subject matter: ownership of quantum internet technologies, and what leverage over them is good for.

The proposed mixed-method framing brings together semi-structured interviews and patent network analysis for pursuing the overarching question, how the strategic competition between the US and China is going to shape the quantum internet. Initially, at the start of this research project, interviews had been considered to be the primary source of data for this thesis. Reflections on conversations with domain experts and output from desk research however changed this perspective towards including a more granular set of data also, and to find a statistically sound approach to inquiring into US and Chinese activity in the quantum domain. The method of interviewing informed the choice of network analysis insofar as it became increasingly obvious during the data gathering process that the debate around US-Chinese competition in emerging technologies would significantly benefit from statistical findings. Coupled, interviews and patent analysis make for a strong set of tools to inquire into the power politics surrounding the emergence of the quantum internet.

Mutual corroboration and complementarity are therefore the two key motives for this choice of methods. While interviews with experts in academia, the UK government, the intelligence community and international organisations provide a high-level summary picture of US-Chinese competition in internet governance, the study of quantum patent data is to provide a detailed and structured analysis of technological progress in building the internet of the future.

The chapter is organised as follows. Section 3.1 makes the case for a multi-method approach in response to the overarching research question and the two subquestions. Section 3.2 provides a justification for interviewing, describes the interview process and approach to analysis, and discusses ethical considerations. Section 3.3 discusses patent analytics. In subsection 3.3.1 it presents examples where patent data provides the evidence base for responding to research agendas in proximity to this project. The section then moves on to discuss in detail in subsection 3.3.2 how the analysis of quantum patent data in particular can respond to the research questions of this project. Subsection 3.3.3 then provides details of the data collection strategy and how quantum patent data has been filtered and checked for consistency and relevance.

The remainder of section 3.3 briefly motivates the computation of some descriptive summary statistics in Chapter 6 of this thesis, followed by a justification of the choice of Exponential Random Graph Models (ERGMs) for representing and studying quantum patent networks. The subsection that follows introduces this class of models in their abstract form and discusses earlier research where an ERGM has been fitted to patent citation data. Section 3.4 concludes and collects the major takeaways of this chapter.

3.1 A mixed-method approach for studying the quantum internet

This project employs a mixed-method approach for building an analytical framework for the study of the emergence of the quantum internet. Broadly construed, Mixed Method Research (MMR) ‘combines elements of qualitative and quantitative research approaches (e.g., use of qualitative and quantitative viewpoints, data collection, analysis, inference techniques) for the broad purposes of breadth and depth of understanding and corroboration' (Johnson et al. 2007, p. 123). A network not yet built, research into the quantum internet is necessarily exploratory and to some degree speculative. Considerable uncertainties about future political developments and the trajectories that quantum engineering may take remain, which exacerbates the problem. Structural difficulties of this kind, intrinsic to this thesis, make the dual aim of understanding and corroboration particularly important.

This thesis considers qualitative and quantitative approaches to be complementary and mutually enriching. As such, MMR provides 'a powerful methods tool that allows for researchers to make their findings more robust' and 'illuminate causal interferences' (Lamont 2015, p. 134). This research follows (Alavi et al. 2018) in assuming a 'reciprocal and dialectic relationship between research and theory' (p. 529) that extends to the choice and application of methods also. This approach is a continuation of the reading of the concept of 'security governance' outlined in the previous chapter, which is at once a theoretical concept and a way of thinking and 'doing' security studies. The concept of securitisation reaches across practices and definitions to provide insight into the processes that frame an object in security terms. A multiplex concept, it lends itself to a mixed-method approach that deliberately crosses the boundaries between qualitative and quantitative research.

While MMR supports the consideration of comprehensive, complementary sources of data input, it can also help maximise the impact of research output thanks to its wider appeal 'to audiences across methodological persuasions' (Thaler 2017,

p. 59). On a very rudimentary level, it makes sense 'to use all the methods at our disposal' (ibid.) to better understand the fallout and repercussions of deep political tensions, and how they are likely to affect how emerging technologies take shape. MMR is driven by the hunch that research would not be as good as it could be if it focused on a single method alone.

In its choice of semi-structured interviews and statistical network analysis as the two principal empirical research methods, this thesis hopes to find readers among methodologically diverse groups of experts in security studies and policy, cybersecurity, internet governance, quantum engineering and technology forecasting. The choice of these two methods is to a large degree pragmatic. As developed in more detail in the sections below, interviews tap into existent expert knowledge while the analysis of patent data generates estimates of technology leadership and competitive advantage. To be pragmatic about research methods does not imply ad hoc arbitrary choices. In their discussions of the usefulness of MMR for political science research, commentators have emphasised the value of pragmatism as an underlying theoretical and philosophical construct that drives the entire research process (Maxcy 2003). Far from inviting sloppiness, pragmatism about methodology means picking research methods which best respond to the research questions at hand.

As developed in the introductory chapter, this project breaks down the overarching research question, how the strategic competition between the US and China is going to influence the trajectories the quantum internet can take, into two subquestions. As developed in Chapter 1, these are:

> **R.1.1** What do domain experts observe regarding US–Chinese competition in internet governance?

and

R.1.2 What do patent data suggest about US and Chinese activity in building the quantum internet?

These two subquestions, in turn, invite further auxiliary queries, responses to which help 'get' to the research questions. Auxiliary queries motivate and guide the collection and interpretation of data. They are:

#	Auxiliary queries
AUX.1	What is a quantum internet?
AUX.2	What does internet governance presently involve?
AUX.3	Can the multi-stakeholder model of internet governance survive?
AUX.4	Who is involved in building a quantum internet?
AUX.5	Does China enjoy a leadership position in quantum internet engineering?
AUX.6	Is there evidence for competing quantum technology clusters developed in the US and China?

Table 3.1: The auxiliary queries that this thesis pursues in response to R.1.1 and R.1.2.

Investigating AUX.1-AUX.6 through a coupling of methods allows for corroboration and the triangulation of findings, which is at the heart of a mixed-method approach. Entangling methods in this way should make for a robust inquiry into plausible future developments of the quantum internet. 'Much of the best social science research', (Brady & Collier 2010, p. 113) note, 'can combine quantitative and qualitative data, precisely because there is no contradiction between the fundamental processes of interference involved in each.' Whether or not this thesis can aim this high, the motivation to combine two distinctly different approaches is grounded in the belief that research methods can complement one another in many meaningful ways.

The sequencing of the presentation of results (Chapters 4-6) matters insofar as this thesis follows a 'general-to-specific' logic. Chapter 4 develops a high-level introduction to the technologies that drive the quantum internet. Since the scope of the interviews is wide, covering general trends in US-Chinese relations and strategic rivalry as well as specifics about competition in internet governance, the interview results chapter, Chapter 5, follows the chapter that discusses the technologies that drive the quantum internet. Chapter 6 then presents the results of the domain-specific statistical analysis of quantum internet technologies.

To sum up: the primary purpose of a mixed-method approach is to complement and mutually corroborate the results from the two methods so chosen. Complementarity strengthens causal inferences while simultaneously supporting the corroboration of findings (Lamont 2015, chapter 7). This is particularly important for exploratory work where uncertainty is a considerable factor. Insights from interviews motivate a quantitative engagement with data; a process which is mutually informative. In the sections that follow, more detail about interviewing and statistical modelling is provided.

3.2 Semi-structured interviews

This thesis incorporates the analysis of a small number of expert interviews in response to the research subquestion

R.1.1 What do domain experts observe regarding US-Chinese competition in internet governance?

Interviews aim to capture how US-Chinese relations impact processes of governance and standards-finding for emerging technologies, and how the internet governance framework is changing due to the intensifying strategic competition between the two countries. In general terms, interviews offer 'political scientists a rich, cost-effective vehicle for generating unique data to investigate the complexities of policy and politics' (Beamer 2002, p. 86). Interviews in empirical international relations research in particular may point to larger intersecting themes and tropes that escape a purely quantitative approach, or are difficult to evidence by statistical means alone (Mosley 2013). Interviews may therefore yield precious insights from domain experts that help put quantitative results into perspective.

This is mainly thanks to the interpretative character of the data so generated. Interviewing enables researchers to study subjects 'in the context of their pasts and the situations in which they find themselves' (Taylor et al. 2016, p. 9). Experts comment against their cultural, political and professional backgrounds and frames, which can make for a more inclusive picture of trends and scenarios that have not yet crystallised in quantitative data.

Importantly, interviews can make for a more nuanced and situated picture of international competition in network governance. Interviewing experts and stakeholders in this area 'has an unrivalled capacity to constitute compelling arguments about *how things work in particular contexts*' (Mason 2002, p. 1, emphasis in original). This project aims to find out how the quantum internet will shape up in the context of deepening political tensions between the US and China.

Interviewing requires the interviewee to take the role of a respondent. Unlike conversations, 'research interviewing involves a "one-way dialogue" with the researcher asking questions' (Brinkmann 2008, p. 470). Interviews provide an opportunity to learn how respondents represent themselves and narrate relevant codes, including but not limited to 'beliefs, ideologies, justifications, motivations, and aspirations' (Boellstorff et al. 2012, p. 93). Due to the non-public character of the format and ensured anonymity, interviewees may also comment insightfully 'behind-the-scenes' on strategic competition in emerging technologies; insights that may not be available through the analysis of material in the public domain alone. For instance, a point developed in full in Chapter 5, sources in Government and at GCHQ have suggested in interviews that the national security implications of QKD are vastly overstated even in prominent academic publications while the implications of a Chinese quantum internet for UK industrial policy are discussed only insufficiently at present. Perspectives and assessments of this kind are difficult to generate by statistical modelling alone.

Interviewing requires some degree of flexibility regarding the actual quality (and order) of the questions being asked. Also, for the purpose of this thesis, participants were encouraged to deviate from the interview guide or follow topics that had developed spontaneously during the interview. Semi-structured interviews therefore seem most appropriate to accommodate this approach (Madden 2010). Some degree of flexibility permits 'an iterative process of refinement, whereby lines of thought identified by earlier interviewees could be taken up and presented to later interviewees' (Beardsworth & Keil 1992, p. 261-262). In the specific context of this research, the quality of interviews improved over time. This was particularly evident in interviews with government officials. The interviews had required the author to first develop the right vocabulary and policy speak to be able to see experts eye to eye in the actual interview process.

Given the exploratory character of elements of this research where it inquires into the likely future evolution of the internet, some degree of flexibility in interviewing was further mandated by the choice of sampling technique. Informants were recruited following the purposive sampling approach (Bryman 2012): potential informants were selected based on their roles and involvement with quantum computing and quantum communication research, national security, intelligence work, regulatory and public policy, or internet governance expertise. Criteria were therefore the role, seniority and professional background of potential informants. The approach to sampling here has been sequential rather than following a fixed sampling strategy (Teddlie & Yu 2007). This is because some relevant informants could not be identified in full or possible to be persuaded prior to the start of the interview process. Rather, new introductions could be made as the investigation evolved, which then generated further opportunities to interview important stakeholders as this research progressed. This is a 'snowballing' sampling technique which 'is able simultaneously to capitalize on and to reveal the connectedness of individuals in networks' (Bryman 2012, p. 424).

In getting at the overarching research question, how the quantum internet is likely to be shaped by rising political conflict over emerging technologies, this thesis invites further auxiliary queries as discussed above. Semi-structured interviews have proved an excellent way to generate insights into competing visions for governing the internet of the future. While there have been differences in opinion as to China's motives, respondents largely converge in their views that China does indeed seek to extend infrastructural control over the internet. The Chinese government seems to want to bring to an end what it considers a long period of Western dominance over network architecture and protocols that have benefitted primarily the US and its allies.

3.2.1 Access to interviewees

Access, here defined as 'the appropriate ethical and academic practices used to gain entry to a given community for the purposes of conducting formal research' (Jensen 2008, p. 2) proved to be a significant challenge. The sensitive nature of questions around great power rivalry in the quantum domain had made it difficult to recruit experts in large numbers. The problem has been twofold: i) access to relevant organisations had to be sought and important gatekeepers convinced of the value of this project; and ii) within each organisation that granted access, informants needed to be persuaded to schedule an interview (Shenton & Hayter 2004).

In recruiting experts for this thesis, the 'known sponsor approach' has been particularly successful, defined here as the tactic to use 'the legitimacy and credibility of another person to establish [one's] own legitimacy and credibility' (Patton 2015, p. 367). The author's three-month placement with the Cabinet Office in the final quarter of 2019, sponsored by Public Policy Southampton, was vital for gaining access to government officials, national security advisers and analysts at GCHQ, the UK's intelligence and cyber agency. Gaining support from senior officials across the Civil Service was important as 'individuals often immediately acquiesce if a superior has granted permission' (Stake 1995, p. 47). In this case, senior officials had acted as gatekeepers who would decide on access to a specific working group in Whitehall. They performed a vital role in endorsing this research project internally and effecting introductions to informants at the National Security Secretariat and the intelligence community (Feldman et al. 2003).

The placement had enabled the author to present himself to potential respondents as an 'insider' or member of an in-group (Dwyer & Buckle 2009). It is safe to assume that without access to internal contact books, an official Cabinet Office email and the job title of 'Policy Adviser', response rates to email invitations for interview would have approached zero. Having obtained official Security Clearance was also immensely helpful as an informant from GCHQ for instance declined to be interviewed over the phone or a video app but instead insisted to meet in a secure conference room in the basement of the Treasury building at 1 Horse Guards Road in Whitehall.

3.2.2 The interview process and interview data processing

In the first round of emails to gauge interest, around 60 potential interviewees were approached. Around 50 percent responded positively, in the end 20 individuals agreed to be interviewed, either by email or over Zoom/Teams calls, once further questions were resolved. From this pool, seven interviews materialised in the end. While some potential informants who had expressed interest initially made the effort to cancel, the majority of those who did not wish to proceed further would stop communication altogether and would not respond to any reminders. Presumably Covid lockdowns at the time did play their part as to why some respondents lost interest or did not have the time to take part after all.

Interviewees were assigned letters, i.e. A-G, for the purpose of anonymisation and identification. The table below provides some detail regarding the background and affiliation of the respondents. Three interviewees are assumed to identify as female, four as male (gender identity was not part of the conversation and was therefore 'read', or assumed).

Respondent	Role	Location
A	Professor of Quantum Communication	Singapore
B	National Security Advisor with the UK Cabinet Office	UK
C	Senior Programme Lead, GCHQ	UK
D	Senior Board Member at an internet standardisation body	USA
E	Lead Researcher in Internet Governance	Switzerland
F	Director of the Asia Programme, Think Tank	Intl.
G	Professor of Internet Governance	USA

Table 3.2: Affiliation and location of research participants.

Full disclosure of the objectives of this research had been provided to all participants prior to interview in the form of a Participant Information Sheet, a Consent Form and a brief summary of the research approach and aims. All informants had been asked to sign a consent form prior to interview. Interviews were 45-

60min long. One interview was face-to-to-face in Singapore, one in London, the remaining five were conducted over Zoom and MS Teams.

The interview schedule for this project was approved in full by the University of Southampton's Faculty of Engineering and Physical Sciences (FEPS) ethics board (ERGO Submission ID 53116). Respondents were asked questions from the below list (not every respondent was able to speak to all questions). The research design was 'flexible, iterative and continuous' (Flick 2008, p. 79) to encourage respondents to deviate from the schedule, e.g. when they wanted to rise an important issue that the interview guide did not cover, or elaborate on a specific point. Flexibility in interviewing gives 'room for the respondent's more spontaneous descriptions and narratives' (Given 2008, p. 470).

Interview guide

Theme 1: personal journey

- Please tell me about your current role here at X? What made you move from your previous post(s) to this one?
- What is your expertise in internet governance? What is the focus of your work and research?
- What is your level of knowledge of quantum computing and communication?
- What was/is your motivation to pursue this line of career?

Theme 2: US-Chinese strategic competition in emerging technologies

- How would you describe the relationship between the US and China?

- Have Chinese policy positions, both internally and externally, moved under President Xi? If so, how?
- What is China's role in international standardisation bodies?
- In your view, does 'big tech' influence official policy positions? If so, how?
- What are the implications of a Chinese leadership position in emerging technology X for the UK/the US/Western alliances?

Theme 3: internet governance

- What does internet governance currently involve?
- How does US-Chinese competition reflect in standards-finding and internet governance?
- What are your views of the current 'multi-stakeholder model'? Is it fit for purpose?
- How will internet governance evolve?

Theme 4: quantum computing and quantum communication

- Who are the main parties in the global pursuit to build quantum computers and quantum communication networks?
- Which country is ahead in which domain?
- What do the US/China hope to gain from a leadership position in quantum tech?
- What, in your view, would be the purpose of a quantum internet?

- What, if any, are the security implications of quantum key distribution?
- Can post-quantum cryptography mitigate the impact of quantum key distribution on cryptography, in particular RSA encryption?
- What are the relative advantages and disadvantages of satellite-based vs ground-to-ground quantum communication?
- What should the Government do about quantum technologies, if anything?

All interviewees agreed to voice recordings of the interview under the condition that recordings be destroyed after transcription. Voice recordings capture not just what people say but the way they say it (Bryman 2012, p. 482). Above all, they help the interviewer focus on the interview process as extensive note-taking during the interview can interrupt the flow of the conversation. The interviews were recorded on a smartphone. Transcriptions were carried out manually and the recording files deleted upon completion of the transcripts.

Transcripts were saved as pdf files, fully anonymised and emailed to participants for sign off and approval that the data so gathered can be included in the final thesis. Participants were informed that they can withdraw their approval at any time. So far no one did. Non-digital, identifiable information, such as signed consent forms, are stored in a secure metal box in a locked cupboard at the author's home address. Anonymised data, such as interview transcript pdfs, are held digitally in a 2FA-protected Google Cloud account.

3.2.3 Coding, thematic analysis and quotations

Following transcription, interview data was divided into in-text blocks, colour-coded, annotated with phrases and terms and finally grouped in separate text files. The annotations served as quick points of reference for easy retrieval and to note down an impressionistic first-glance assessment, such as 'China: standards (AI but not quantum)'. The purpose of coding in this context, i.e. in the qualitative domain, was to 'assign a summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based or visual data' (Saldana 2012, p. 3). While coding precedes analysis proper, in the context of this thesis, coding is also a heuristic tool–the very process of coding already provides insight into the interrelatedness of strategic rivalry, competition over standards and governance models, and novel quantum internet technologies. In this sense, coding interview data for this thesis has been an iterative process that 'leads from the data to the idea' (Richards & Morse 2012, p. 137), and arguably back to the data.

The larger tropes that emerged in coding were used to structure the analysis of responses in the following chapter. Results are therefore being discussed thematically, not individually for each participant separately. Thematic analysis of this kind aims to 'ascertain common topics' (Conaway & Wardrope 2010) and the relationships between them. Grouping interview data around topics makes for a more structured and interesting read than ordering and presenting responses in strict oder following the original interview schedule. Thematic analysis also recognises the interconnectedness of the research questions, and is therefore well suited for a mixed-method approach.

Results Chapter 5 engages with interview data and presents verbatim quotations for the purpose of analysis. There are several reasons for including verbatim quotations that can differ in length. First, although anonymised, they give interviewees the opportunity to 'speak for themselves' in the thesis. As such, verbatim quotations give a voice and illustrate respondents' situatedness and points of view. Readers are in a better position to 'get a feel' for the framings and narratives a respondent may have deployed in the conversation.

Moreover, since interview data are contextualised, analysed and interpreted, it is important to present responses, where applicable, 'as is' to enable the reader to check if the discussion and interpretation that builds on them follow from what had actually been said, and are therefore justified. Verbatim quotations provide an implicit checks-and-balances mechanism for robustness. This is to empower readers so that they can 'make their own judgements about the fairness and accuracy of the analysis' (Corden & Sainsbury 2006, p. 12).

3.2.4 Ethical considerations

Particular ethical challenges due to unexpected interviewee behaviour or strong emotional responses to questions were always unlikely to occur and never did. Similarly, the issue of exploitation, typically arising where 'researchers investigate those who are less powerful than themselves' (Hammersley & Atkinson 2007, p. 217) did not seem to apply. The issue of reactivity, or Hawthorne effect, i.e. the possible behavioural impact on informants in response to the awareness of being questioned or observed (McCambridge et al. 2014) did not seem to occur either. Research suggests that the Hawthorne effect is most pronounced in longer observations over time, in particular in hierarchical settings where the researcher is considered superior in status so that a desire for recognition drives behavioural adjustments (ibid.). Given the author's junior role as a PhD Researcher the Hawthorne effect never seemed likely to manifest. In general terms, the effect seems to emerge in continuous participant observation, not necessarily in one-shot interviews.

The underrepresentation of minority groups in key positions relevant to this thesis unfortunately finds reflection in the interviewee sample pool. One respondent is Asian, one mixed race and five are white. Since access to informants had been very limited from the start the author did not wish to exclude informants on grounds of them being over-represented in the sample pool by markers of ethnicity, hence the overrepresentation.

3.3 Modelling patent networks

In pursuing the research subquestion,

> **R.1.2** What do patent data suggest about US and Chinese activity in building the quantum internet?,

this project builds on Laura DeNardis's observation of a 'turn to infrastructure' (Musiani et al. 2015, DeNardis 2014*a*, 2020, DeNardis et al. 2020) in internet governance, as developed in the literature review chapter. The past decade has witnessed a shift in state actors' attitudes towards controlling the internet to the effect that they seek to extend their influence by means of network architecture, as well as by the implementation of standards. The primary vector of control is no longer restricted to internet policy and the governance of application layers that sit on top of the network, such as the Web (e.g. by limiting which websites can be viewed). Rather, spheres of influence now firmly extend to deeper, infrastructural levels of computer networks, protocols and standards. Controlling the 'hard stuff' that enables global connectivity in the first place puts state actors in a much stronger position to manage who can do what over the network of networks. China's current push for 'New IP', discussed in detail in the next chapter, attests to the extent to which competition in internet governance today revolves around internet architecture and protocols.

This means that the question of governance is now firmly entangled with the issue of infrastructure. The question, who will gain control over the infrastructure of the internet of the future, is therefore also a question about governance. The US and China openly acknowledge this pairing in their strategy papers on emerging technologies. The issue of governance has the problem of network architecture, standards and hardware as its flipside. This prompts the question, who owns critical prototypes that may enable state actors to tighten their infrastructural grip even further? In responding to **R.1.2**, this project collects quantum technology patent data. Patents as they are registered presently have predictive power over the likely winners and losers of the quantum innovation race that will only accelerate over the years to come. And innovation in this space will shape the internet governance model of the future.

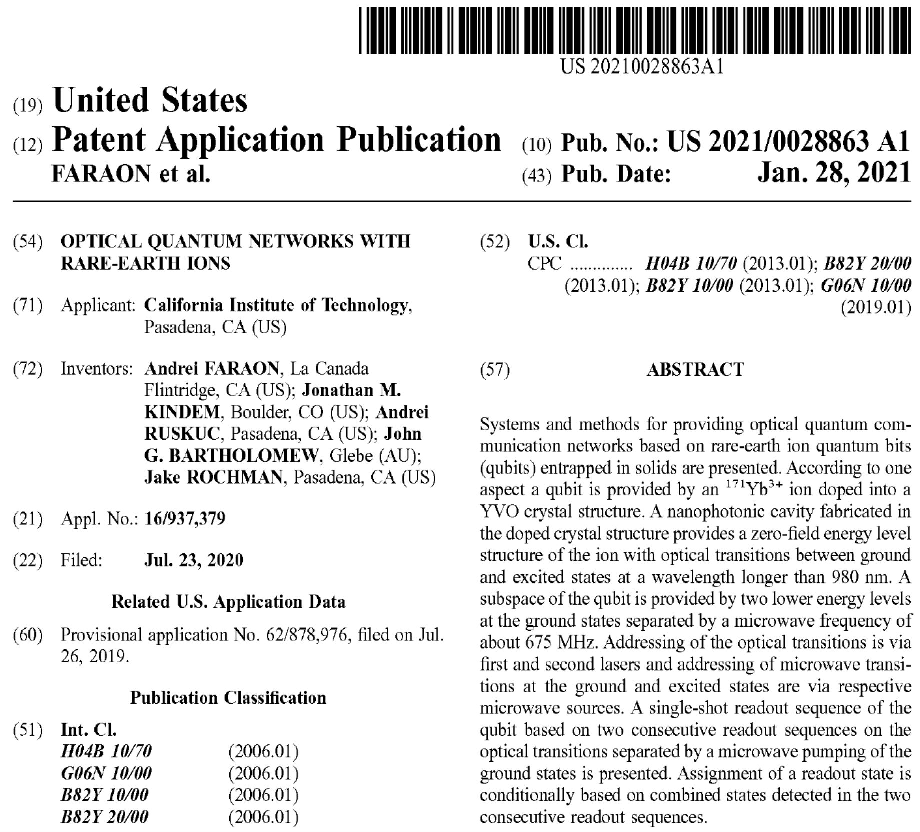
3.3.1 Examples of successful patent analyses

The World Intellectual Property Organization (WIPO), an agency of the United Nations, which serves as the 'global forum for intellectual property (IP) services, policy, information and cooperation', defines patents as 'an exclusive right granted for an invention, which is a product or a process that provides, in general, a new way of doing something, or offers a new technical solution to a problem' (WIPO

2021). Patents incentivise innovation by protecting ideas against exploitation by other parties.

Patents are signals about the future trajectories that novel technologies may take. As ‘indicators of technological emergence [they] promise valuable intelligence’ (Porter et al. 2019). As such, they have formed the empirical base for a great number of studies that forecast how innovation that originates in university research is likely to diffuse and whom it will serve. For instance, (Ahmadpoor & Jones 2017) analyse 4.8 million US patents and 32 million research articles to build distance metrics that measure how quickly academic findings translate into ‘marketplace inventions’. They find that relevant publications in nanotechnology and computer science have the shortest distance to travel until they arrive at a patented invention.

To give an illustrative example of the data that patent offices hold, the image below presents details of a quantum technology patent record.



US 20210028863A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2021/0028863 A1**

FARAON et al. (43) **Pub. Date: Jan. 28, 2021**

(54) **OPTICAL QUANTUM NETWORKS WITH RARE-EARTH IONS**

(71) Applicant: **California Institute of Technology**, Pasadena, CA (US)

(72) Inventors: **Andrei FARAON**, La Canada Flintridge, CA (US); **Jonathan M. KINDEM**, Boulder, CO (US); **Andrei RUSKUC**, Pasadena, CA (US); **John G. BARTHOLOMEW**, Glebe (AU); **Jake ROCHMAN**, Pasadena, CA (US)

(21) Appl. No.: **16/937,379**

(22) Filed: **Jul. 23, 2020**

Related U.S. Application Data

(60) Provisional application No. 62/878,976, filed on Jul. 26, 2019.

Publication Classification

(51) **Int. Cl.**

H04B 10/70	(2006.01)
G06N 10/00	(2006.01)
B82Y 10/00	(2006.01)
B82Y 20/00	(2006.01)

(52) **U.S. Cl.**

CPC ***H04B 10/70*** (2013.01); ***B82Y 20/00*** (2013.01); ***B82Y 10/00*** (2013.01); ***G06N 10/00*** (2019.01)

(57) **ABSTRACT**

Systems and methods for providing optical quantum communication networks based on rare-earth ion quantum bits (qubits) entrapped in solids are presented. According to one aspect a qubit is provided by an $^{171}\mathrm{Yb}^{3+}$ ion doped into a YVO crystal structure. A nanophotonic cavity fabricated in the doped crystal structure provides a zero-field energy level structure of the ion with optical transitions between ground and excited states at a wavelength longer than 980 nm. A subspace of the qubit is provided by two lower energy levels at the ground states separated by a microwave frequency of about 675 MHz. Addressing of the optical transitions is via first and second lasers and addressing of microwave transitions at the ground and excited states are via respective microwave sources. A single-shot readout sequence of the qubit based on two consecutive readout sequences on the optical transitions separated by a microwave pumping of the ground states is presented. Assignment of a readout state is conditionally based on combined states detected in the two consecutive readout sequences.

Figure 3.1: First page of a recent quantum patent application. The bottom left reveals relevant CPC codes while the abstract contains relevant keywords. Source: EPO GPI database.

Early works in patent analysis employed patent statistics to investigate large-scale macroeconomic sectoral changes in response to innovation ((Pavitt 1984), cf. (Marmor et al. 1979, Basberg 1987)). By the 1990s, patent statistics had become a primary data source for economists to investigate the sources of economic growth and technological change on global and national levels (Griliches 1990). This was followed by a surge of works that investigated in more detail the geographies of knowledge production, e.g. by comparing the 'geographic location of patent citations with that of the cited patents, as evidence to the extent to which knowledge spillovers are geographically localized' (Jaffe et al. 1993, p. 577). The authors found that ‘citations to domestic patents are more likely to be domestic, and more likely to come from the same state’ (ibid.), thus providing evidence for the strong ties between patenting, domestic industries and economic growth on country levels.

Over time, the analysis of patent citations in particular–the practice of registering entities to cite other patents as important inputs, similar to academic referencing–‘is a core methodology in the study of knowledge diffusion’ (Alcácer & Gittelman 2006, p. 774). Other early work that involves patent citations studied outward knowledge flows from universities and research laboratories ‘across institutional and national boundaries’ (Jaffe & Trajtenberg 1996). By the early 2000s, a robust number of tools for the analysis of patent citations had been developed (Breitzman & Mogee 2002).

Since then, many academic journals have emerged that focus on the empirical analysis of patent statistics. *World Patent Information*, published by Elsevier, is a journal ‘for intellectual property information and its retrieval, documentation, classification, search, analysis and IP management.’[1] *Technological Forecasting and Social Change* is a forum for the ‘methodology and practice of technological forecasting and future studies as planning tools as they interrelate social, environmental and technological factors.’[2] Since its inception in 1979, Sage’s *Journal of Information Science* has published more than 300 articles that build on the analysis of patent data.[3] *Patent Analytics* is a new open access journal that aims to foster ‘our understanding of patents, advancing methodologies, demonstrating and evaluating effectiveness and efficiency.’[4] The point of this short list is to demon-

[1] https://www.journals.elsevier.com/world-patent-information

[2] https://www.journals.elsevier.com/technological-forecasting-and-social-change

[3] https://journals.sagepub.com/home/jis

[4] https://www.frontiersin.org/journals/research-metrics-and-analytics/sections/patent-analytics

strate that today, patent analytics is an established research method across a vast array of disciplines, topics and locales. Research on quantum internet technology as reflected in patenting activity sits well with this rich tradition in empirical research.

More closely related to the topic of this thesis, research on patent citations registered with China's State Intellectual Property Office (SIPO) suggests that Chinese applicants tend to over-cite domestic technologies relative to external, foreign sources. Moreover, while the absolute number of top-quality patents 'surged in every province', the authors of a 2020 study find that 'high-quality patents remain mainly distributed in four developed areas' (Huang et al. 2020, p. 1), which suggests considerable regional disparities in China in terms of innovation capabilities. Works such as (Choi et al. 2015) build predictive models of technology transfers to better estimate which newly patented technology in particular is likely to become commercially viable. To this end, they use social network analysis to build graphs that show how patents are linked via citation keywords. The authors argue that their methodology can help identify early on some of the most promising patents.

Similarly, (Altuntas et al. 2015) design a model of 'patent power' and 'expansion potential' that builds on patent data in order to make statistically more robust predictions about core technologies of the US electronics industry. In a study of the global automobile industry, (Lin et al. 2011) use patent citations to identify several 'backbone technologies' that should be considered the main accelerators of innovation in this industry. They employ network analysis to find important subnetworks and technology clusters that drive the commercial success of the entire sector. The quantum patent data model developed in this thesis seeks to contribute to this class of literature.

The recent boom in big data analytics, AI and machine learning has also brought about novel ways of text-mining and aggregating patent datasets for developing novel tools for technology forecasting. There has been such a steady output of work in this area over the past ten years that several authors have taken to the task of building patent analytics taxonomies ((Abbas et al. 2014, Aristodemou & Tietze 2018)). There is, of course, also a large number of commercial patent analytics research and consultancy services, mainly for the purpose of identifying investment opportunities for corporate clients. While projections from the consultancy industry should not necessarily be taken at face value, a recent estimate values the 2019 commercial patent analytics market at $660 million (Insights 2020).

The rise of patent analytics research correlates with a jump in patent applications themselves. Over the past twenty years, patent registrations worldwide have increased sharply in number, which attests to the growing status of patents in corporate planning and management. There is now widespread agreement that patent data provide insight into the diffusion and propagation of early technologies and prototypes that have not yet reached maturity. ‘Although there is more to invention than patenting, patents are primary indicators of invention, providing valuable technological and geographic detail’, the US National Science Foundation sums up the consensus (NSF 2020). This thesis follows this line of argument and considers quantum patent data signals of probable technology futures.

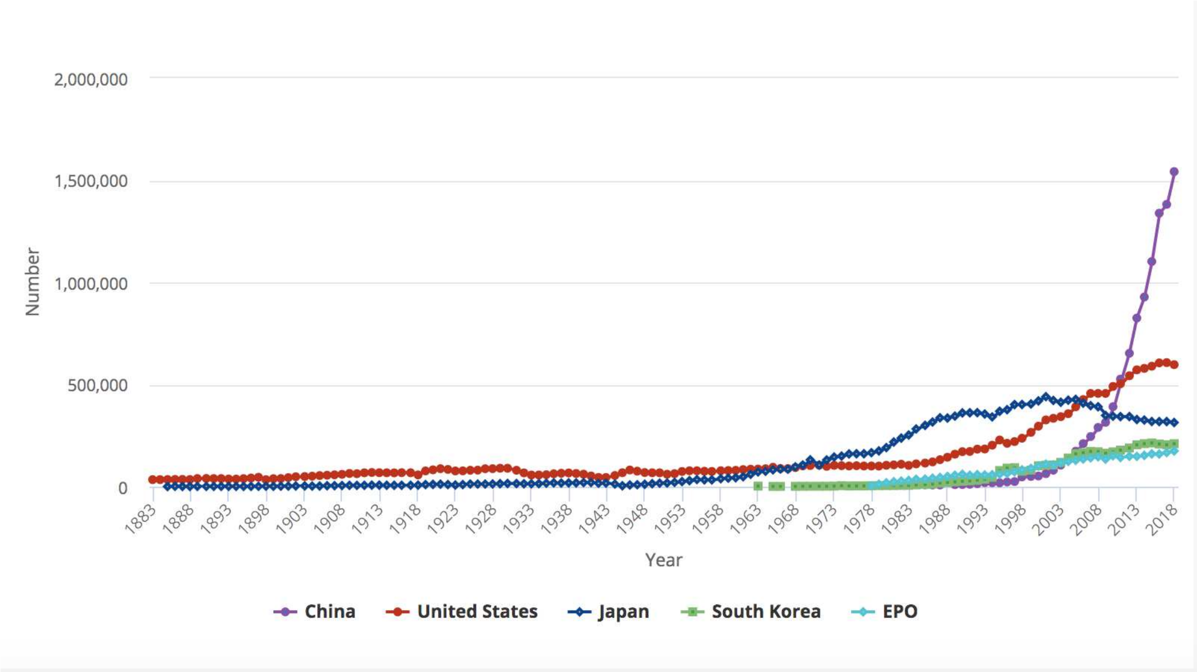


Figure 3.2: WIPO patent applications to the top 5 patenting offices worldwide: 1883–2018.
Source: (Robbins et al. 2020).

3.3.2 Why quantum patent data?

State actors could be reluctant to patent novel quantum technologies in an attempt to keep these technologies secret. This would make patents an unreliable source of data on quantum innovation. It seems very reasonable to suggest that not all government-sponsored research activity, in particular where it pertains to questions of national security, will be patented. However, while it is true that in the past, disruptive military technologies were developed at classified government facilities, military innovation today is largely driven by private sector corporations.

The US Department of Defense (DOD) and the Ministry of Defence (MOD) in the UK routinely express concern that they do not have the in-house capabilities to develop AI-powered vehicles or autonomous weapon systems independently to the degree they would like (Feickert et al. 2018, MOD Developments, Concepts and Doctrine Centre 2018, NATO Allied Command Transformation 2016). In the updated Integrated Review and the Defence and Security Industrial Strategy, the UK Government outlines how it seeks to extend collaboration with the private sector even further for building critical national infrastructure and developing cyber resilience (HM Government 2021*b*,*a*). Both the DOD and the MOD have established units and working groups that are tasked to design better processes for collaboration with the private sector.[5]

Private companies consider their patenting activities signals of robustness and profitability to financial markets. Studies find strong positive correlations between firms' IPO performance (the amount of money they can raise when going public on stock markets) and prior patenting activity (Useche 2014). A great many studies suggest an overall positive correlation between patent data, R&D activity and financial performance on the level of firms (see (Lerner & Seru 2017) for an overview).

At present, the human and financial resources required to fully develop relevant quantum technologies in-house and at scale are beyond what even the most generous funding increase for the Armed Forces would be able to achieve near-term–attracting top level engineers is one issue of many, as clearly demonstrated by the threat of Google researchers in 2018 to walk out if the parent company Alphabet would not cancel its contracts with the Pentagon (Shane & Wakabayashi 2018). To realise quantum technologies without any private sector involvement at all, in par-

[5] Examples of such offices in the UK are Defence Digital at Strategic Command, Jhub at Joint Forces Command, or the British Army Innovation Team. There are several others.

ticular where they need to link up with legacy network systems at enormous scale, would most likely be an uphill struggle of considerable proportions to any government. Where the private sector is involved however there are strong incentives to patent innovation for future commercial exploitation. If anything, today patent data have only become stronger signals of trends in emerging technologies.

Beyond the research cited in the above sections, governments too routinely analyse patent data for the purpose of internal reporting. For instance, the UK Government's Intellectual Property Office has developed several toolkits 'to be applied to science-intensive technologies which are visible to horizon-scanning, but not yet widely developed such that opportunities for application and commercialisation may still be unclear'. The toolkits can be used to 'produce an output score indicative of disruptive potential' (Buchanan & Corken 2010, p. 1). The indicator aggregates, among others, patent application filings over time and the portfolio sizes of registering entities. The UK's Intellectual Property Office confirms the US National Science Foundation's view that patent data have considerable predictive power over technology futures.

In the field of quantum technologies, so far there has been only one study that collects some high-level quantum patent data: a report published by the European Commission's Joint Research Centre provides some basic descriptive statistics about quantum patent applications held in the European Patent Office's Global Patent Index database (Travagnin 2019). While other studies that draw on quantum patent data exist, as the authors of the European Commission's research paper explain in the appendix to their study, they have been assembled with commercial interests in mind, e.g. by tech consultancies that aim to stir up interest in consultancy services among industry partners. This puts a big question mark on the validity of these efforts.

3.3.3 Data collection and filtering

The source of patent data for this project is the Global Patent Index (GPI), a patent database maintained by the European Patent Office (EPO), which includes registered worldwide and UK patents and patent applications. The UK Government recommends retrieving data directly from the EPO for searching UK data.[6] The GPI pulls records from EPO's worldwide bibliographic, legal event and full-text patent databases. Holding more than 130 million patent records in total, the GPI is the most comprehensive patent databases available.[7]

For this thesis, data were retrieved via the GPI Web interface following a combined classification and keyword search strategy. Each patent record held in GPI is classified with at least one CPC (Cooperative Patent Classification) or IPC (International Patent Classification) entry. For instance, 'G06N 10/00' captures 'Quantum computers, i.e. computer systems based on quantum-mechanical phenomena'. In principle, relevant data can be retrieved by specifying appropriate CPC and IPC entries only.

However, the CPC classification tree alone is divided into nine sections, which in turn are divided further into classes, sub-classes, groups and sub-groups, totalling approximately 250,000 classification entries.[8] While it is fairly straightforward to automate data retrieval following a classifier approach, it must be assumed that a significant number of patents may sit in fringe subgroups that are difficult to

[6] https://www.gov.uk/search-for-patent

[7] https://www.epo.org/news-events/news/2021/20210609.html

[8] https://www.epo.org/searching-for-patents/helpful-resources/first-time-here/classification/cpc.html

anticipate. Over-reliance on classification codes is likely to produce vast numbers of irrelevant data while missing a lot of others in the process. This is particularly pertinent regarding the oftentimes fuzzy framing and wording of nascent quantum technologies, as the above mentioned study in this domain indicates (Travagnin 2019).

Instead, for the purpose of data generation, the CPC/IPC code search was combined with a keyword filtering approach in order to retrieve relevant patent families. The EPO defines a patent family as ‘a collection of patent applications covering the same or similar technical content’.[9] This grouping is necessary when an inventor registers patents that are either very similar in character and quality, or registers the same patent across multiple countries and jurisdictions. In order to avoid multiple countings of essentially the same invention, only quantum patent families have been collected for the purpose of this thesis. The relevant CPC codes were identified following the search strategies the EPO recommends in its GPI user manual.[10] Thanks to a previous professional role of managing a library database, class-marking system and classification tree at the British Library of Political and Economic Science at the London School of Economics, the author was sufficiently qualified to select the relevant CPC entries without further external validation.

The search was then divided into two separate stages in order to make the process more manageable and keep in line with the fact that the relevant technologies which will contribute to the infrastructure of a quantum internet, i.e. i) quantum computing and ii) quantum communication technologies, largely constitute two separate research fields. The following tables give an overview of the search

[9] https://www.epo.org/searching-for-patents/helpful-resources/first-time-here/patent-families.html

[10] https://www.epo.org/searching-for-patents/technical/espacenet/gpi.html

strategy.

For the domain of quantum computing, the following CPC codes have been used for retrieval.

CPC code	Description
G06N10/00	‘Quantum computers, i.e. computer systems based on quantum-mechanical phenomena’
B82B	‘Manufacture or treatment of nanostructures’
B82Y10/00	‘Nanotechnology for information processing, storage or transmission, e.g. quantum computing or single electron logic’
G06E3/00	‘Optical computing devices for processing non-digital data’
H01L39/00	‘Devices using superconductivity’

Table 3.3: The most relevant CPC codes in the domain of quantum computing for retrieving GPI data.

The same procedure was applied to the domain of quantum communication, which proved an even more crowded marketplace of ideas. The relevant CPC subgroups are as follows.

CPC code	Description
B82Y20/00	'Nanooptics, e.g. quantum optics or photonic crystals'
H01L31/00	'Semiconductor devices sensitive to infra-red radiation, light, electromagnetic radiation of shorter wavelength or corpuscular radiation and specially adapted either for the conversion of the energy of such radiation into electrical energy or for the control of electrical energy by such radiation...'
H04L 9/00	'Cryptographic mechanisms or cryptographic arrangements for secret or secure communication'
H01L 33/00	'Semiconductor devices with at least one potential-jump barrier or surface barrier specially adapted for light emission'
H04B 10/00	'Transmission systems employing electromagnetic waves other than radio-waves, e.g. infrared, visible or ultraviolet light, or employing corpuscular radiation, e.g. quantum communication'
H04B10/70	'Photonic quantum communication'
H04W 12/00	'Security arrangements; Authentication; Protecting privacy or anonymity'
G02F 1/00	'Devices or arrangements for the control of the intensity, colour, phase, polarisation or direction of light arriving from an independent light source, e.g. switching, gating or modulating; Non-linear optics'
H04J 7/00	'Multiplex systems in which the amplitudes or durations of the signals in individual channels are characteristic of those channels'

Table 3.4: The most relevant CPC codes in the domain of quantum communication for retrieving GPI data.

To check for consistency and robustness, the resultant dataset was manually reviewed by the author. In a somewhat tedious process, titles and abstracts of patents were double-checked for relevance. For instance, a patent on 'quantum game theory', arguably falsely classified, was removed upon inspection. This manual filtering approach requires a sound understanding of quantum computing and quantum communication. To this end, in preparation for data collection, the author had pursued a six-month accredited course on quantum computing, quantum communication and quantum algorithms with the Massachusetts Institute of Technology's computer science department. The course was funded by the University of Southampton's Web Science CDT. Further details of the combined classifier and keyword search strategy, and the output of the searches, are presented in Chapter 6.

3.3.4 Descriptive statistics

Chapter 6 first presents some high-level descriptive statistics that describe the US and Chinese quantum technology patent networks, such as counts of the countries where applying entities are based. This is to demonstrate empirically that the number of patent applications for technologies relevant to the quantum internet has been rising significantly since 2015. The section develops a range of insightful statistics such as degree distribution or the k-core (concepts which are explained in full in Chapter 6), which allow the reader to get a quick overview of the scale, distribution and quality of relevant quantum patents in this area.

3.3.5 A quantum Exponential Random Graph Model

Strategic competition over emerging technologies implies that quantum patenting is a patterned activity, i.e. the emergence of a new quantum patent is not an independent event but dependent, in some way, on some other patenting activity in the past and/or different domain. To see why this should be the case, even prior to analysis, assume the reverse, i.e. independence. In statistical terms, independence of events would imply that no invention out there has ever been informed by any other but has emerged in complete isolation: statistically, independence requires that no patent application has predictive power over any other. However, the very fact that inventors must cite other relevant patents that have shaped their work, similar to academics who cite relevant literature to situate their research, shows that the global patent landscape is indeed a network, both in cross-sectional and longitudinal terms. It is not a collection of independent events.

This project aims to identify some fundamental characteristics of this global quantum patent network. This raises the question which approach to modelling and estimating the network is the right one. The interdependence of patent events entails that standard regression models (which assume independence of observations, which allow for established procedures such as t-tests and ANOVAs), do not apply. To analyse quantum patent data from a network perspective requires finding models that do not require observations to be independent. Secondly, a statistical patent network model should provide insight into the how dynamics evolve over time. The model should make for a better understanding of the leading registering entities, where they are located, how they are connected and the pace at which progress is being made in building the infrastructure for the quantum internet of tomorrow.

Chapter 6 develops a model that meets these requirements–an exponential random graph model (ERGM).[11] EGRMs are a class of established statistical models developed for the analysis of social networks. For the purpose of this thesis, a quantum patent ERGM is designed to test for the structural characteristics of the global quantum patents network. The model achieves this by studying local network structures in sub-graphs in order to build up a more complete picture of the network in its totality (Lusher et al. 2012*b*).

In general terms, ERGMs are a class of autoregressive models that allow for statistical inferences about overlapping network structures and interdependencies (Lusher et al. 2012*a*, Chakraborty et al. 2020, Ward et al. 2011). The point of building an ERGM is to generate a representation of the structural processes at work that have led to the characteristic tie formations among clusters of quantum patents as observed in the data. Ties, or edges, between patents emerge when they cite other patents, or are being cited. Strong ties among Chinese applicants for instance would point to the formation of local clusters. Should the number of China-to-China ties have increased steadily over time the data provides evidence for the formation of strong local clusters, which would suggest progress towards technological independence.

More precisely, the ERGM developed in Chapter 6 tests if a given network, such as the empirically observed patent application network as selected from the GPI database, is a random network where the ties (citations) between registered patents (nodes) follow a random walk. If the null hypothesis of randomness is rejected, the network reveals structural characteristics e.g. in terms of location and registering entities–clusters that shape how successfully a patent citation can propagate

[11] It would be more appropriate to speak of 'exponential family random graph models'. However, for convenience the term 'family' has been dropped in most of the recent literature.

through a subnetwork. An ERGM reveals network features such as cluster dominance and centrality measures in procedural estimates. The outcome is a pattern that reveals regional clusters and estimates of variables that shape quantum internet technologies.

In statistical terms, the general form of the ERGM can be expressed as follows. The probability $\mathcal{P}_\theta$ of observing the network as constituted by the GPI data, i.e. the graph (G), $\mathcal{P}_\theta(G)$, is defined as:

$$\mathcal{P}_\theta(G) = \frac{\exp\big(\theta^T \cdot \Gamma(G)\big)}{\sum_{G^* \in \mathcal{G}(N)} \exp(\theta^T \cdot \Gamma(G^*))} \tag{3.1}$$

where $\theta, \theta \in \mathbb{R}^q$, is a q-dimensional vector of parameters, $\Gamma : \mathcal{G}(N) \to \mathbb{R}^q$ projects $\mathcal{G}(N)$ into $\mathbb{R}^q$, $G \to (\Gamma_1(G), ..., \Gamma_q(G))^T$ is a collection (of functions) of network statistics, such as homophily and transitivity and is as such q-dimensional, and finally,

$$c(\theta) := \sum_{G^* \in \mathcal{G}(N)} \exp\big(\theta^T \cdot \Gamma(G^*)\big) \tag{3.2}$$

is a vast normalisation constant that is expensive to compute, if possible at all (Schmid & Desmarais 2017). For a quantum patent network of around 5,000 nodes, as is the case for this thesis (see Chapter 6), the true constant c cannot be calculated in polynomial time and therefore requires approximation. Essentially, $c(\theta)$ is the sum of (a simulation of) all possible configurations of the network (G). Dividing the statistic for the observed network by the sum of all possible networks gives the probability of the observed network to emerge ‘in nature’. The model is developed in full, with attention to the theoretical background of ERGMs, in

So far there has been only one academic publication that fits an ERGM to patent citations (Chakraborty et al. 2020). The authors model the patenting activities of Europe's 20 largest companies. They find strong empirical evidence that patents are much more likely to cite other patents if they were registered in the same country and filed in the same language, which attests to strong homophily in R&D activity among Europe's biggest multi-national enterprises. There are large disparities in the numbers of outward and inward citations however, meaning that a small number of firms are significantly more influential than others in pushing novel technologies.

Below is an illustrative example of the network visualisations that their ERGM produces. The authors claim to be delivering 'a deeper analysis into the "prestige" network of top applicants' (p. 23), thus providing insights into patenting dynamics that are not available through standard regression analysis. They confirm that 'ERGMs help us model network mechanisms directly, instead of acting as a proxy for unspecified dependence and relationships among the observations' (p. 1). This thesis aims to extend this line of work to the study of quantum technologies. This is in order to get a sense of the internet governance challenges in the years to come, which unfold against the backdrop of rising political tension between the two competing superpowers.

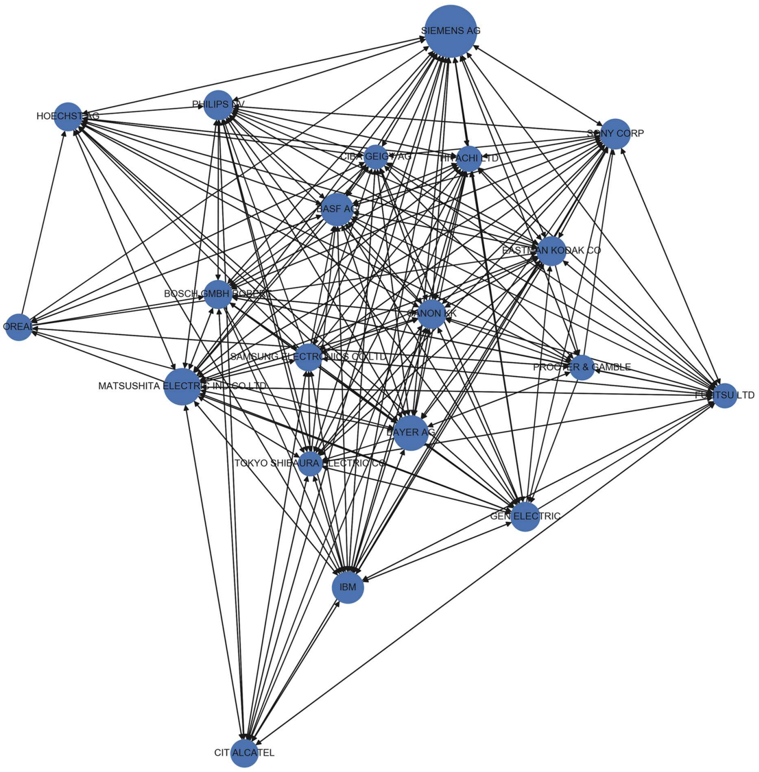


Figure 3.3: Example output from an ERGM: the citation network of Europe's top-20 prolific companies.
Source: (Chakraborty et al. 2020, p. 21).

3.4 Main points of Chapter 3

This chapter has proposed a mixed-method approach in response to the research question, how rivalry and the strategic competition between the US and China impacts the possible growth trajectories of the quantum internet. The question reaches into plausible scenarios of regime-finding for a new internet in a world of deepening political tensions, most notably between the US and China. Future internet governance regimes will largely depend on how state actors position themselves, how much value they place on an open, non-fragmented internet, or if they believe that an open network can only bring about strategic disadvantage.

Questions about the political and strategic dimensions of internet governance invite a qualitative perspective. As section 3.3 above hopes to have demonstrated, it makes sense to reach out to experts in this domain and ask about their views and assessment of the issue. Semi-structured interviews are an established way to sample opinions in this area. Interviews yield a rich set of data about how the internet governance community, as well as policymakers and security officials on the fringes, consider internet governance to evolve over the coming years.

However, political manoeuvring and political strategy will be conditional upon, at least partially, actual technological progress in building a quantum internet. It can be assumed that either of the two superpowers will give their efforts to shape the quantum internet governance model a big push if and when quantum technologies developed at home afford a more aggressive stance. The question if there is sufficient progress in building the elements for a quantum internet is an empirical one. It does reach beyond what expert interviews can possibly reveal.

For this reason, this chapter has proposed a second, quantitative angle to the study of the quantum internet. In section 3.4 above, it has made a case for employing quantum patent data as signals of probable technology futures. In ERGMs it finds a rich technique for modelling patent dynamics. ERGMs deliver insights in response to subquestions about technology leadership and geographical clusters. They help reveal the degree to which state actors' rhetoric must be considered empty talk or if it is indeed backed by a nascent technology that promises to revolutionise networked computing.

Following on from the above discussion, the major takeaways of this chapter are:

3.a The literature review chapter explains how ‘hard’ quantum capabilities are best studied in tandem with ‘soft’ power in leveraging standards. The choice of methods for this project reflects this entanglement.

3.b Research into the political and governance issues surrounding the emergence of the quantum internet is necessarily exploratory and speculative in places. Large degrees of uncertainty should guide the choice of methods available.

3.c A mixed-method approach (MMR) brings together complementary approaches to the study of the inevitably fuzzy variables that will shape the quantum internet. MMR reaches beyond methodological siloes and appeals to a larger body of readers than any strictly separated method alone. To this end, pragmatism as a guiding principle is an established way for selecting the most appropriate sets of methods.

3.d Interviews in empirical international relations research support the identification of larger intersecting themes and tropes that escape a purely quantitative approach, or are difficult to evidence by statistical means alone.

3.e Patent analysis is an established research field that investigates the diffusion of knowledge as well as the scale and the pace at which innovation translates into novel products and processes.

3.f Patent citation networks can provide valuable insights into the dynamics by which innovation diffuses in national research programmes.

3.g The analysis of patent citation networks requires a dedicated class of statistical models. ERGMs are a sophisticated class of models that estimate the entire network in one step, thus avoiding untestable assumptions not backed by further evidence or theory.

Chapter 4

The quantum internet

Far from being a specialist project that would only excite network enthusiasts, the quantum internet has entered mainstream reporting. *The Washington Post* is eager to reveal that the US 'hatches [a] plan to build a quantum Internet that might be unhackable' (Whalen 2020). For *The New York Times*, the project 'inches closer' and is going to connect computers which 'will make today's machines look like toys' (Metz 2022). Here in the UK, *The Times* raises the possibility of 'unbreakable codes' that could be exchanged over the internet (Blakely 2022). And, perhaps unsurprisingly, *The Daily Mail* finds that it is thanks to British scientists that an "unhackable' internet moves a step closer after 'game-changing' quantum breakthrough paves way for safer online communication' (Chadwick 2020).

But what is a quantum internet exactly? In its simplest form, a rudimentary quantum internet will connect some basic quantum computers, i.e. quantum nodes, over a secure quantum communication channel. But for what purpose? And what is a quantum computer, and what is quantum communication? This chapter presents a high-level introduction to these topics and provides an overview of US and Chinese efforts in this space. This is to prepare the grounds for the empirical analysis that follows in Chapters 5-7.

The chapter is organised as follows. Section 4.1 covers the essentials of quantum computing. Large, stand-alone and fault-tolerant quantum computers that could be useful at solving complex tasks are difficult to build and still many years away–to work around this, a quantum internet would connect basic devices with limited functionality to essentially build a distributed system of quantum compute resources.

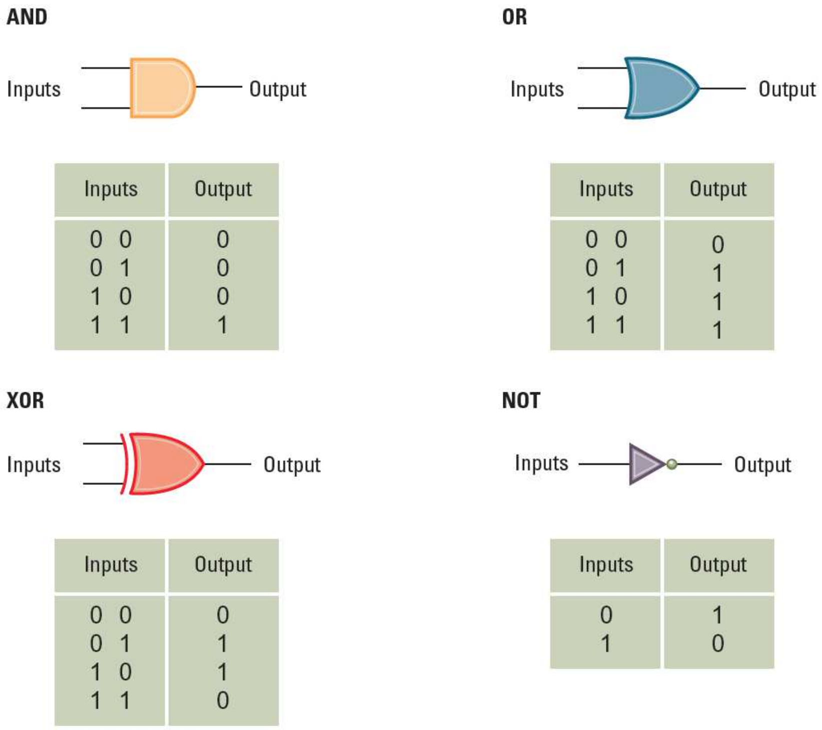
For this to be possible, quantum computers need to be connected over appropriate channels. Section 4.2 discusses how this could work in practice. Section 4.3 then considers the principles of quantum networks and provides an introduction to the architecture of a quantum internet that connects nodes via quantum repeaters–one of the most pressing engineering challenge in this domain. The section also discusses how China has established a significant leadership position in this area. It is the only country to have experimented successfully with satellite-to-ground quantum communication, the chief enabling technology for a global quantum internet. Section 4.4 concludes and presents the major takeaways of this chapter.

4.1 Quantum computing

The major difference between quantum computing and digital, or 'classical', computing is that quantum machines are not binary. All the computing devices that exist today, from smartphone to tablet, to PC and to supercomputer are binary in the sense that at any given time, their fundamental computational components are in one of two states. This is because for any program to be able to run, no matter how complex, ultimately information must be encoded on the level of hardware. This means it must be stored physically, i.e. inside a laptop or on a cloud server.

At this level, however, options are limited. The principal component of a computer system is the micro-transistor to which a charge can be applied. This is a world in which the transistor can only ever be ‘on’ (the charge is applied so that electrons flow through it), or it is not so that no electrons may travel through the transistor, in which case it is ‘off’. While there are no ontological grounds to label these states ‘0’ and ‘1’, it is convenient to use the binary system of counting (i.e. a numerical system to base 2) as it obviously matches the two available states a transistor can find itself in. To keep things logical, it makes sense to label the off-state ‘0’, meaning the voltage level is zero while ‘1’ means the transistor is ‘on’ because there is voltage so that electrons flow through the system.

The beauty of these (micro)transistors is that they can be linked together to build more complex logic gates that return the output of Boolean operations. Applying charges selectively to specific transistors in the chain (i.e. flipping them between on and off) makes it possible to engineer controlled sequences of currents that flow through the system: some transistors are on, then off, then on etc. Essentially, a transistor acts as a gate for electronic signals (Brookshear & Brylow 2020). This back-and-forth of applying a charge on the circuit level–depending on the Boolean operation so desired–is the literal encoding of information on machine level. These (oftentimes very long) lists of on/off combinations are then abstractly represented by strings of zeros and ones, which, in turn, can be aggregated to represent human-readable information such as letters and numbers in ASCII code. The same principle applies to exciting pixels on a screen surface so that information can be represented visually. Figure 4.1 below provides an illustration of the most fundamental gate operations in digital computing.



Inputs	Output
0 0	0
0 1	0
1 0	0
1 1	1

Inputs	Output
0 0	0
0 1	1
1 0	1
1 1	1

Inputs	Output
0 0	0
0 1	1
1 0	1
1 1	0

Inputs	Output
0	1
1	0

Figure 4.1: Representation of the AND, OR, XOR and NOT gates in classical computing. Source: (Brookshear & Brylow 2020, p. 43).

A binary computer executes commands sequentially, i.e. on a first-come-first-served basis, very much like humans read a page in a book line by line, page by page. While binary computers are limited to a two-dimensional state space (on or off), more transistors however quickly turn into more processing power as they allow for more parallel operations, better caching and better control. So in principle, more transistors mean better performance–today, top-end chips can contain billions of micro-transistors. The relationship between the number of transistors on a chip and the efficiency of a computer has come to be known as *Moore's Law.*

In 1965, the co-founder of Intel, Gordon Moore, famously predicted that advances in engineering will lead to a doubling of the number of transistors in integrated circuits about every two years or so (Moore 1965). While Moore's Law has proved remarkably accurate over the years (Flamm 2018), all good things must come to an end: there is a natural limit as to how many micro-transistors can be placed on a chip without creating noise and interference. It seems that the growth potential of building ever more efficient and dense conventional microchips is drawing to a close. 'It's over. This year that became really clear', Charles Leiserson from the MIT claimed in an interview in 2020 (Rotman 2020). For Erica Fuchs at Carnegie Mellon University, 'there are really smart people in AI who aren't aware of the hardware constraints facing long-term advances in computing' (ibid.). The future development of large-language models with billions of parameters may very well be compromised by literal hardware constraints.

This frontier to binary computing is one of the key motives to find a radically new and different computer architecture that need not worry about such limitations. Quantum computing is one of these approaches. The concept as such is not new; it celebrated its 40th birthday in 2021. In May 1981, star physicist Richard Feynman presented his vision of a future computer at the 'Simulating physics with computers' conference at the MIT (Feynman 1982).

Feynman's starting point was that the complex behaviour of molecules is impossible to simulate on a digital machine. This is because of the exponential growth of the possible number of states the system can evolve into thanks to the intractably large number of possible quantum effects. For Feynman, it would only be logical to build a new kind of computer the architecture of which mirrors the object of study: a quantum computer that harnesses the potential of quantum mechanics to simulate quantum effects on the subatomic level (Preskill 2021).

The genius of Feynman's proposal rests on the curious behaviour of (sub)atomic particles. The aforementioned indivisible unit of classical computing, the bit, is commonly instantiated physically on a silicon chip. As discussed, its binary notation is an abstraction from its physical state (voltage yes or no). The basic unit of a quantum computer is called a *qubit* (for 'quantum bit'). It can be instantiated in many different ways; as electrons, ions, even photons (Aaronson 2018, Bellac 2006, Bokulich & Jaeger 2010, Deutsch 1997, Lo et al. 2000, Nielsen & Chuang 2010). Presently, a great number of research programmes in this area compete to find the winning specification (the following subsection discusses this in more detail). In quantum computing, too, the concept of the qubit is an abstraction from its physical state.

A classical bit appears in either of the two (abstracted) states 0 and 1. Qubits too can have state spaces $|0\rangle$ and $|1\rangle$ in a complex two-dimensional Hilbert space where $|0\rangle = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ and $|1\rangle = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$.[1] The 'state' of the qubit can be its spin if it is an electron, or, in case of a photon, its polarisation Mermin (2007), Nielsen & Chuang (2010). Regardless of their physical particularity, the important point about states is that they define qubit behaviour, and this behaviour can be manipulated. Electrons, for instance, can be excited such that their spin, somewhat akin to their angular momentum, can point upwards or downwards in space.

The computational potential of a qubit resides in the fact that, unlike the classical bit, it can be brought into a combined state where it displays properties of *both* states simultaneously. This state is called *superposition.* This is achieved by manipulating a qubit with laser beams or microwaves to change its spin. The

[1] This is shorthand 'Dirac', or 'bra–ket' notation. $|0\rangle$ is pronounced 'ket 0' and $|1\rangle$ is 'ket 1'.

behaviour of qubits is best described in terms of basic linear algebra. A qubit has two mutually orthogonal basis states, as noted above: $|0\rangle$ and $|1\rangle$. In superposition, it achieves a linear combination of these two states (Wright & Ding 2015):

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}, \ \alpha, \beta \in \mathbb{C}, \ |\alpha|^2 + |\beta|^2 = 1. \tag{4.1}$$

While the bit can only represent two states, the qubit can, in principle, have an infinite number of states. Colloquially speaking, it can be 0 or 1 just like a bit (and indeed it collapses to either 0 or 1 in the act of measurement) or it is 'a little bit' of 0 while also being 'a little bit' of 1. It is convention to visualise this behaviour on a so-called Bloch sphere:

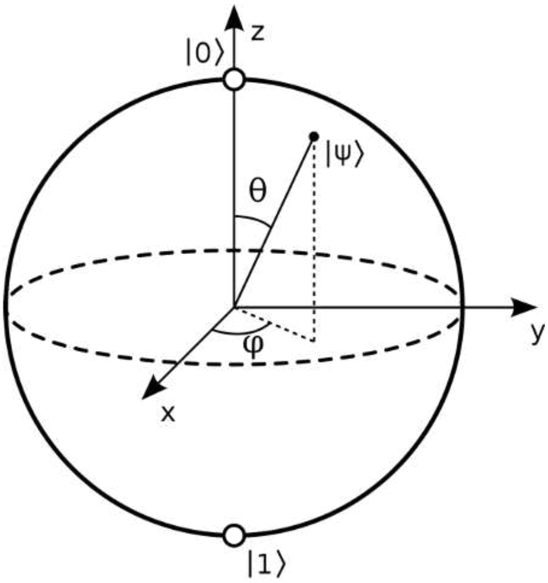


Figure 4.2: A Bloch sphere represents the possible states a superimposed qubit can assume. Source: Wikipedia.

A classical bit can only occupy the polar axes of the sphere, i.e. the 'North' and 'South' poles $|0\rangle$ and $|1\rangle$; the rest of the sphere is not accessible. The state of the qubit can sit anywhere on the sphere, however. While a classical bit is limited to a very narrow choice of either of the two poles, the qubit can travel freely across the globe and choose to rest anywhere on the sphere. In the figure above, it is fully determined by angles φ and θ.[2] In the example figure above, $|\psi\rangle$ sits considerably north of the equator towards $|0\rangle$. But it does not sit at either of the poles and so it is 'both' 0 and 1 at the same time, albeit to different degree. Even if somewhat inexact, it is not incorrect to say that the superimposed qubit is both 0 and 1 at the same time. This is Schrödinger's cat, at once dead and alive (Gerry & Bruno 2016).

So the first important point to note is that compared to a classical bit, a qubit has more degrees of freedom to choose its state-space. The figure below presents a direct comparison–the classical bit can only choose extreme (and icy!) conditions at either of the poles (since the Bloch sphere is symmetrical, the choice which pole is 0 or 1 is arbitrary). In a sense, the bit is a special case of a qubit that is in state $|0\rangle$ or $|1\rangle$.

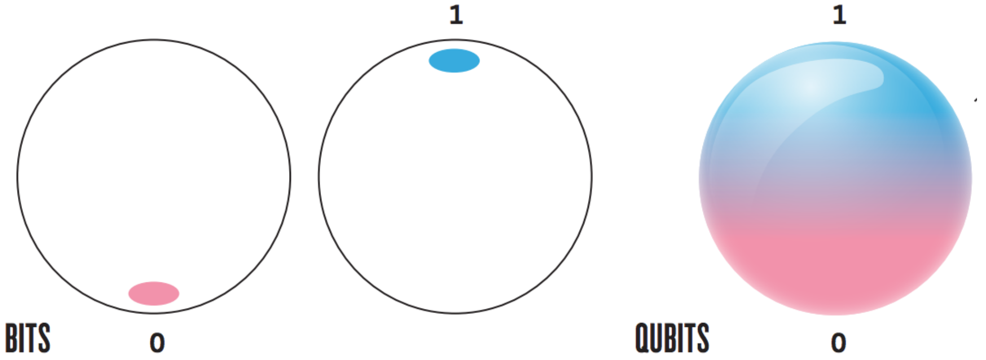


Figure 4.3: The possible states of a classical bit compared to a qubit that can occupy any point on the surface. Reprinted with permission from Springer Nature Customer Service Centre GmbH. Springer Nature: Nature, 'Quantum leaps, bit by bit', Andreas Trabesinger, ©2017.

[2] The probability amplitudes of the parameters are $\alpha = \cos\left(\frac{\theta}{2}\right)$ and $\beta = e^{i\varphi}\sin\left(\frac{\theta}{2}\right)$.

While this behaviour is surely interesting, it is not of much computational interest. The potential of a quantum computer becomes more obvious when more than a single qubit is assumed. Consider a two-state system. There are four different states a classical 2-bit computer can represent: $(00), (01), (10), (11)$. Put differently, the system is ‘off/off’, ‘off/on’, ‘on/off’ or ‘on/on’. The equivalent quantum machine would be made up of two qubits x and y such that

$$\begin{aligned} |x\rangle &= \alpha_0|0\rangle + \alpha_1|1\rangle, \\ |y\rangle &= \beta_0|0\rangle + \beta_1|1\rangle. \end{aligned} \tag{4.2}$$

Just as for the single qubit case, the joint state of this system is a linear product of its four basis states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Now, importantly, this system can be transformed as follows (Wright & Ding 2015).

$$|x\rangle \otimes |y\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix} \otimes \begin{bmatrix} \beta_0 \\ \beta_1 \end{bmatrix} = \begin{bmatrix} \alpha_0 \begin{bmatrix} \beta_0 \\ \beta_1 \end{bmatrix} \\ \alpha_1 \begin{bmatrix} \beta_0 \\ \beta_1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{bmatrix} \tag{4.3}$$

where

$$00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad 01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \quad 10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \quad 11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}. \tag{4.4}$$

This joint state can no longer be represented on a 2-dimensional Bloch sphere but the principle is still the same. In the single qubit case, the superimposed qubit is, to some degree, both 0 and 1 at the same time. In the 2-qubit case, the two superimposed qubits are, to some degree, at once $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ at the same time, meaning they are in $2^2 = 4$ different states at the same time.

This is a hugely significant point: because each state can be made to represent a basic unit of information, the 2-qubit system can hold, and thereby encode, and thus ultimately represent, all the four states that it is composed of *at the same time*. This is not the same but somewhat akin to parallelism. Importantly, while the number of basis states are the same as in the classical world (there are four possible states for the 2-bit digital system also), the quantum machine can hold these four states 'in parallel' while its classical counterpart must make a choice which of the four states it wants to adopt. For instance, it could not perform, at the same time, both operations 'voltage on/on' and 'voltage on/off'. It could do this sequentially, sure, but not at the same time.

With each additional bit in the chain, the binary computer has a better choice to represent *one single* state. For instance, the 2-bit system in this example can represent four different states, from 0 up to $2^0 + 2^1 = 3$. A 3-bit system can represent one out of eight states, from zero to $2^0 + 2^1 + 2^2 = 7$ etc.

The advantage of a quantum computer is that the number of states it can hold simultaneously scales exponentially. While the 3-bit system has to choose *one* out of eight states, its 3-qubit cousin can hold *all* eight states. In general terms, *n classical bits can store exactly one number between 0 and $2^n - 1$ while n qubits can store all the numbers from 0 up to $2^n - 1$* (XQ 2020).

For this to happen, however, the qubits must be brought into a special relationship quantum physicists call *entanglement* (Preskill 2021). Entanglement is a special kind of correlation that cannot be expressed as the linear tensor product of basis states as characterised above. Put differently, qubits that are entangled are expressed as a linear combination that cannot be reduced, or separated further. Out of all possible linear combinations that characterise superposition, there is a subset of special entangled superpositions that will not reduce mathematically. The most common example of such a state is

$$|\psi\rangle = \frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle. \tag{4.5}$$

This linear combination cannot be expressed as the tensor product of two other states, hence the term 'entanglement' that suggests a solid connection. The two qubits are correlated and always in the same state (cf. (Wright & Ding 2015)). This quality gives entangled qubits the power to behave as a computational unit which can hold all these different states at the same time.

How do computations on qubits actually work? In the classical world, logic gates engineer the flow of electrons in circuits in such a way that they yield results of Boolean operations. In the domain of quantum computing, computation is achieved by rotating states on Bloch spheres around in such a way that they yield AND, OR, and NOT operations. Essentially, this is achieved by matrix calculations over the entangled superimposed states. For instance, the so-called Pauli-X gate

$$X = NOT = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{4.6}$$

flips the qubit over as it maps $|0\rangle$ to $|1\rangle$ and vice versa (Nielsen & Chuang 2010). This is the quantum computing equivalent to a NOT gate in binary computing. The design of quantum logic gates is certainly a non-trivial task and beyond the scope of this illustrative section. Good introductions and overviews of the topic can be found in (Aaronson 2018, Preskill 2004). The most important point for the purpose of this thesis is that quantum logic gates manipulate the state space of (entangled) qubits, expressed formally as rewriting the linear combination of states. They are the equivalent to classical logic gates, as the image below illustrates.

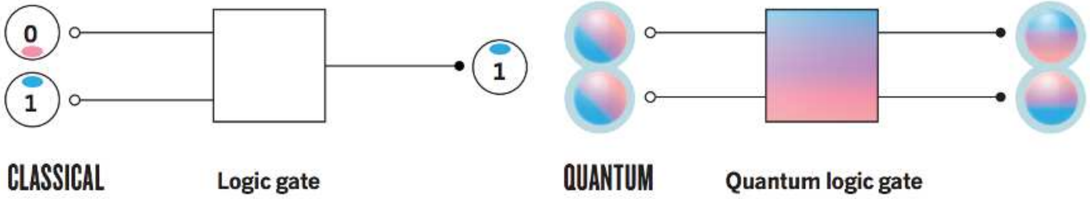


Figure 4.4: Classical vs quantum logic gates. Reprinted with permission from Springer Nature Customer Service Centre GmbH. Springer Nature: Nature, 'Quantum leaps, bit by bit', Andreas Trabesinger, ©2017.

Thanks to the exponential rise in the number of possible entangled state-spaces when more qubits are added to the system, superposition and entanglement can yield, at least conceptually, compute resources of unimaginable scale. A theoretical quantum computer of 300 logical qubits[3] could perform $2^{300} \approx 10^{90}$ operations at the same time. This is a figure larger than the number of *all* atoms in the universe, according to calculations that astrophysicists provide (Preskill 2021). It is safe to assume that such a machine will never be built, but it is a neat illustration that gives a sense of scale and a rationale as to why both the US and China are

[3] In reality, it will need thousands if not millions more qubits as they decohere rapidly, and many are lost to inference and noise. 'Logical' here means the equivalent to perfectly stable imaginary qubits that work reliably. For instance, if a quantum computer has 1,000 qubits but only 1 in 10 survives computation, it would only contain 100 logical qubits.

determined to develop robust computers of this kind.

Besides the massive increase in compute resources, quantum computers are hoped to run certain classes of algorithms that are intractable even for the best digital supercomputer that exists today. The most prominent example is ‘Shor’s Algorithm’, named after Prof Peter Shor from the MIT (Shor 1994, 1997). It finds the prime factors of large integers in polynomial time, meaning efficiently enough so that it makes sense to run the algorithm in the first place. This is bad news for much of online encryption. While a classical computer finds it easy to calculate the product of two prime numbers, even very large ones, the reverse is not the case. This is the foundation of so-called RSA encryption named after their three inventors (Rivest et al. 1978, Nordrum 2016).[4]

For instance, John Preskill from the California Institute of Technology gives the following example. It would take a classical computer of below-average clock speed of 2.2 GHz more than 10^{12} years to factor a 500-digit number; this is longer than the age of the universe (Preskill 2013). A theoretical quantum computer of the same clock speed would be able to perform this task in about two seconds however (ibid.). RSA and similar cryptography systems will no longer be of much use once quantum computers have arrived, which has opened a new chapter of encryption research, that of post-quantum cryptography.

At present, the single biggest obstacle to realising even a modest quantum computer is error correction (Devitt et al. 2013, Roffe 2019). While compute resources scale exponentially for each additional qubit that is added to the system, the same is true for errors, interference and noise. Exposure to even minuscule forces or magnetic fields will cause the qubits to lose their entangled state, collapse to

[4] In fact, GCHQ had developed this algorithm a couple of years prior to the American computer scientists but would keep it classified until after the publication of (Rivest et al. 1978).

their basis states instead and thus lose all calculations.

Announcements of doubtlessly impressive engineering successes of 50+ qubits rightly make headline news and get YouTubers excited. Experts, however, say 'it's generally accepted that we'll need roughly a million qubits before we can error-correct enough qubits to perform useful calculations' (Timmer 2021). This is a long way to go. Large-scale and fault-tolerant quantum computers are many years away, which makes building smaller mid-range devices a much more realistic project. As the introductory section of this chapter notes, this matters to building the quantum internet as it is going to be the key mechanism to provide and distribute entanglement at scale. The following subsection discusses the progress the US and China have made in building quantum computers, and the engineering approaches that compete.

4.1.1 Current progress and engineering principles

While the basic principles of quantum computing as outlined above apply to all platform designs, quantum computing in reality should be considered an umbrella term for a wide range of competing engineering approaches. With this nascent technology, nothing is settled. Some approaches seem more promising than others, but it would be premature to make a call on any specification. This is an important difference to classical computing where the fundamental principles of manufacturing are not subject to debate: wafers, slices of crystalline silicon, serve as semiconductors from which computer chips are built (Laplante 2018).

The most important choice for quantum engineers to make in the first instance is which particle should be crowned qubit. Electrons are a popular modality. Using microwaves, the spin of an electron can be manipulated as outlined above. The major selling point of electrons is that, if implemented as so-called ‘quantum dots’, they can leverage existing silicon fabrication technology, i.e. they can be manufactured at existing chip production factories with little modification to production machinery and infrastructure. This keeps investment in auxiliary machinery significantly lower compared to other approaches. Quantum dots also require relatively small areas for implementation, which makes them interesting for developers with commercial applications in mind (William & Chuang 2021).

A promising qubit candidate based on electron spins is the phosphorus atom placed on silicon–the outermost electron of the phosphorus atom serves as the qubit. As this approach employs existing silicon production systems, coherence times and fidelity rates seem to outperform alternative approaches (Gnidenko et al. 2021). However the phosphorus atoms need to sit within 10 nanometers of each other on a silicon board, which makes implementation and scaling a significant challenge. Research in this domain is still largely experimental (He et al. 2019) with some indication that the US is ahead in this area (Parker et al. 2022).

The first generation of quantum computers will be extremely expensive to build, service and maintain due to the high cost of auxiliary infrastructure such as cooling devices. One of the few qubits that can be manipulated at room temperature utilises the lattice structure of diamonds. Researchers pick ‘faulty’ diamonds that lack carbon atoms in their lattice structure and inject a nitrogen atom into it, which creates a ‘carbon vacancy’, and most importantly, an extra pair of electrons that can be used as a qubit. This approach seems particularly popular with researchers in Europe.[5]

[5] QuTech at TU Delft is a leading research lab for this modality.

However most universities and laboratories that publish quantum research seem to prefer the trapped ion method (Ladd et al. 2010). Charged atomic particles are suspended in an electromagnetic field and then manipulated by lasers to move between different energy levels, which is the physical realisation of the qubit (Gibney 2020). Since its inception in 1995 ((Cirac & Zoller 1995)), this method has been largely confined to experimental work at research labs. However, in June 2020, US conglomerate Honeywell, headquartered in Charlotte NC, has made headline news when it presented a 'functioning' quantum computer it had quietly been working on for over a decade. The company claimed that their trapped ion-machine outperforms even the most powerful quantum computer by any competitor if the somewhat nebulous metric of 'quantum volume' is applied (Gibney 2020).[6]

[6] 'Quantum volume' is a composite indicator that considers error rates and connectivity also and not just the number of qubits alone. However it has not gained much traction as it is 'still a rather coarse metric' (Gibney 2020).

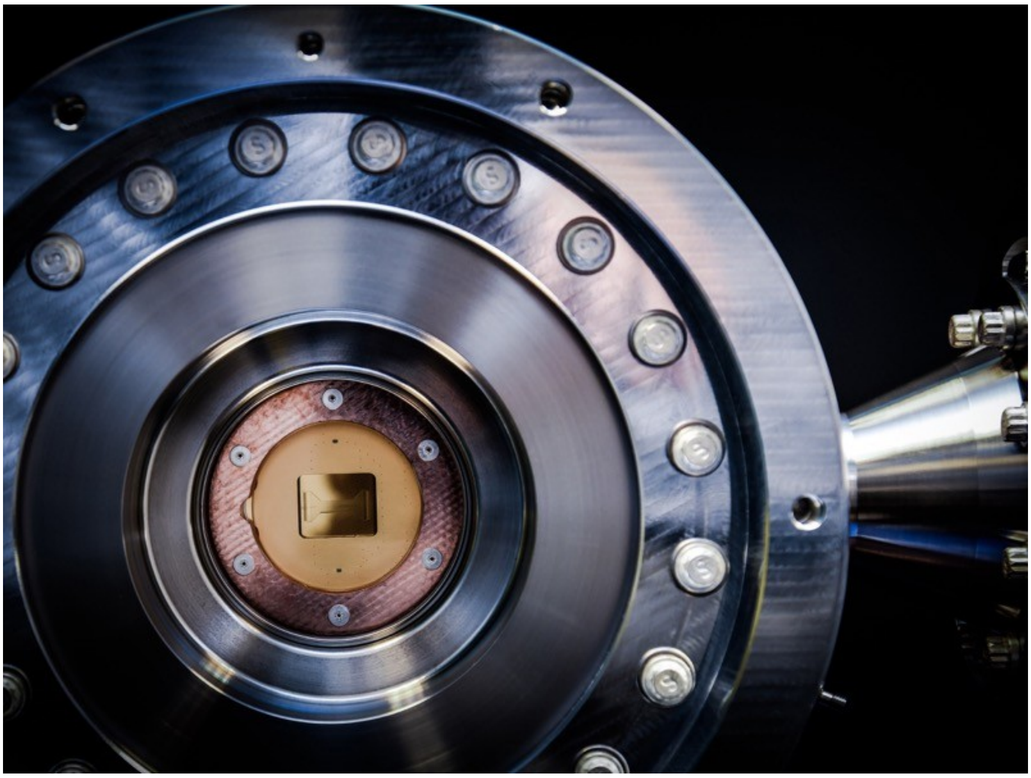


Figure 4.5: Honeywell's trapped ion computer core housed inside a vacuum chamber. ©Honeywell. Source: (Gibney 2020).

The choice of trapped ions over alternative qubit candidates is informed by the particular research ecosystems that university labs can draw on. At universities, there is usually a lot of expertise in atomic physics that make collaborative work between physics and computer science departments possible–oftentimes, large private corporations however do not have this breadth of expertise at their disposal (Hui 2019). Unlike interdisciplinary labs at physics departments, on the other hand, large companies do have a lot of expertise and experience in manufacturing semiconductors, and, importantly, knowhow on scaling up. Expertise and areas of specialisation then reflect in the choice of qubits, and explain why university research in quantum computing would oftentimes choose qubit modalities different from large private corporations.

The difference in access to expertise seems one of the reasons why the likes of Alphabet, Amazon, IBM and Meta bet on superconducting devices as their qubits of choice. Superconductors require massive cooling efforts down to temperatures of just above absolute zero. At this level, metals such as aluminium display the curious property of superconductivity: its conductivity is infinite. If a current is applied, it will not dissipate but flow indefinitely. These currents can be manipulated with inductors such as the Josephson Junction to manage energy levels. The system then behaves as a qubit (Centre for Quantum Technologies 2021, Hui 2019). These devices are typically housed in large refrigerators and have become the stereotypical representation of quantum computing in the media, as illustrated by the image below:

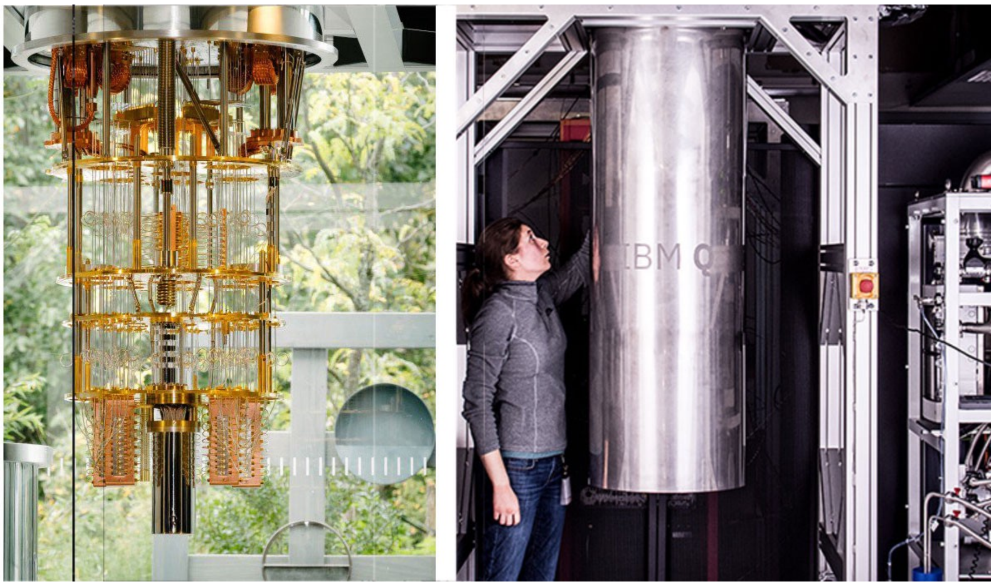


Figure 4.6: An illustration of IBM's quantum computer that utilises superconducting circuits. ©IBM. Source: (Hui 2019).

In November 2021, IBM announced a new quantum processor named *Eagle* that holds 127 qubits on a superconducting transmon architecture (IBM 2022). The company claims that the 'arrival of the 'Eagle' processor is a major step towards the day when quantum computers can outperform classical computers at meaningful levels' (Pires 2021). IBM hopes to extend *Eagle*'s capabilities to 1,123 qubits by 2023.

For Microsoft, on the other hand, none of this will be good enough to generate genuine quantum advantage, i.e. the point where quantum computers are 'better' than digital computers in the sense that they can solve relevant problems more efficiently, or new classes of problems entirely. Microsoft has proved an outlier in that they do not pursue quantum computing with superconducting circuits. Unlike other tech giants, they place their bet on 'topological' qubits, a mathematical abstraction of qubits that yet has to make it from the chalkboard into the lab– topological qubits remain a theoretical concept.

The elusive 'Majorana' particle, named after an Italian physicist of the 1930s who first proposed its existence, would serve as a scaleable qubit. Microsoft believes that neither superconducting techniques nor trapped ions will prove scaleable enough to actually build fault-tolerant computers. While a Microsoft-led team created headline news in 2018 when they claimed to have found evidence for the existence of the Majorana particle, in what was nothing short of a PR disaster they had to retract the paper 'for insufficient scientific rigour' in March 2021 (Godwin & Clayton 2021). The world of quantum engineering still awaits a breakthrough from Microsoft's rather exotic approach.

The high levels of uncertainty as to which qubit modality should make the race to the top means the rudimentary machines that are already available are not exactly sellout items. In a 2021 survey of 300 senior managers at large multinational companies from nine countries, about 50 percent of respondents cited the 'complexity of integrating quantum computing with their existing IT stack' as the major obstacle to adopting quantum computing at their organisation. This was closely followed by 'security concerns' (38 percent) and 'concerns over vendor lock-in' (38 percent) (Alsop 2022). Quantum computing has not yet reached a sufficient level of maturity to find consideration in corporate planning.

At present, the US is largely considered leading in terms of research output and experimental progress in the domain of quantum computing 'but this lead is tentative' (Parker et al. 2022, p. 1-2). In 2020, the US dominated patenting activity to a large extent–the analysis in Chapter 6 however yields a more nuanced picture, with China making considerable progress. What makes the US quantum ecosystem so successful is the fact that it is characterised by a fair number of highly productive collaborations between universities, industry, and government bodies. Many joint bodies and working groups have formed since the Quantum Initiative Act (discussed in Chapter 2) was passed in 2018. Examples include the Quantum Economic Development Consortium, a joint initiative of IBM, several startups and government departments that is funded by NIST, NASA and Google's Quantum AI Lab, and the Alliance for Quantum Technologies, initiated by Caltech and AT&T.

The US government has invested about $ 1.7B into quantum technology research in the three years 2019-2021(Parker et al. 2022, p. 42). This figure does not include funding for classified research projects. As far as China is concerned, it is difficult to obtain reliable figures on public investment. Government-sanctioned research publications such as (Zhang et al. 2019), one of the very few papers on this topic, state that the Chinese leadership had injected about $100 million annually into quantum technology research programmes in the decade up to 2019. The US Congress however estimates this figure to be significantly higher. It arrived at around $250 million for 2018 alone. A 2018 US research paper ((Costello & Kania 2018)) identified claims in Chinese-language media about government plans, albeit unconfirmed, to increase funding for quantum R&D for the period 2017-2022 to around $ 3B per year. Given how the strategic competition between the US and China has accelerated since 2019, it can be assumed that this is a better estimate.

Despite the opacity of public-facing communication in China, one observation seems solid: China is concentrating its efforts on advancing its leadership position in quantum communication (cf. (Parker et al. 2022, p. vi)), the topic of the following section, while the US is cementing its competitive edge in quantum computing. This is mainly explained by strong government *and* private sector funding in the US while research in China is largely funded by public investment: 'U.S. private industry is primarily focused on quantum computing, with almost half of the companies and nearly all of the VC investment going toward that domain' (Parker et al. 2022, p. vi). On the other hand, the Chinese leadership seems particularly keen to make quantum communication a radically new and genuinely Chinese innovation.

4.2 Quantum communication

Quantum communication is the application of superposition and entanglement for the encryption of messages over significant distances. It builds mainly on a final important qubit modality: photons. Photons have the property that they are both wavelength and particle, which make them excellent qubit candidates. By definition, they move at light speed. While this makes them difficult to control, it also makes communication with photons extremely fast.

Quantum communication exploits a fundamental principle of quantum mechanics: the 'no cloning' property of prepared qubits.[7] If the state the qubit has been prepared in is unknown, it cannot be copied. Imagine for a moment there was a way to copy the unknown state of a qubit. This would mean there exists a unitary cloning operator U^*_{clone} such that

$$U^*_{clone}|0\rangle \rightarrow |0\rangle|0\rangle, \;\; U^*_{clone}|1\rangle \rightarrow |1\rangle|1\rangle. \tag{4.7}$$

Then, this cloning operator could be applied to the equal superposition state (the unknown state the entangled qubit is in). This would yield

$$U^*_{clone}\left(\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\right) \longrightarrow \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right). \tag{4.8}$$

This, however, would entail a contradiction because

$$\frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right) \;\neq\; \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right). \tag{4.9}$$

There is no way for this unitary operator to exist, hence unknown superposition states cannot be copied (William & Chuang 2021).[8] This property can be utilised for encryption purposes.

The most popular approach in this domain is Quantum Key Distribution (QKD).

[7] 'Prepared' in the sense that the qubits are entangled and in superposition.

[8] It should be emphasised that if the state *is* known, the second qubit can, of course, be prepared in an identical way.

Two parties share random key pairs over a secure quantum channel. This private key is used to encrypt and decrypt the actual message so transmitted.[9] If Alice and Bob communicate over a secure quantum channel, eavesdropper Eve would be unable to tune in without having to take a measurement of the photons being sent around. As she cannot copy and replace the photons she is reading out, as per the no-cloning principle, her intrusion would collapse the quantum channel and raise an alarm. The key pair would be discarded:

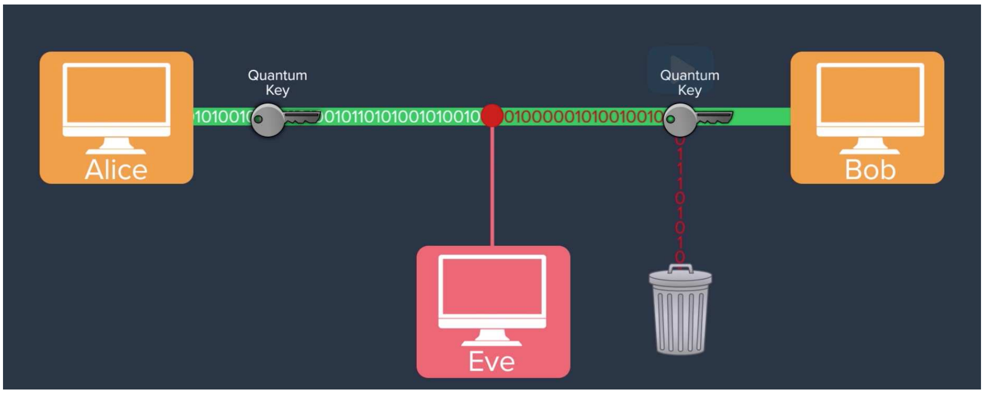


Figure 4.7: Secure exchange of random key pairs over a quantum channel. Should an eavesdropper tune in, the key is being automatically discarded. Source: (William & Chuang 2021).

For Eve to actually be able to decode the key pair deciphered as strings of prepared photons sent around, she would have to perform a measurement on them. The act of measurement however collapses the superposition state, the most basic principle in quantum mechanics. Given that photons, by definition, travel at light speed, there is no mechanism in the known universe for Eve to measure quickly enough, replace, and feed newly prepared qubits back into the channel. As QKD exploits this basic feature of quantum physics, many advocates of this protocol offer variations of the claim, 'QKD as a cryptographic primitive offers security

[9] It is important to say that the quantum channel only encrypts the exchange of key pairs, not the message itself. Unsurprisingly, this creates vulnerabilities.

that is guaranteed by the laws of physics' (Campagna et al. 2015, p. 18).

This claim is disputed on several grounds (Bernstein 2018, Bernstein & Lange 2017). In practice, QKD is expensive both in computational and infrastructural terms as it requires a quantum channel for the exchange of private key pairs plus a classical communication channel for exchanging the actual message. While the principles of quantum communication may indeed be secured by the laws of nature, in reality quantum hackers have already exploited hardware weaknesses at the endpoints of the channel, e.g. by reading off the most minuscule temperature differences of the photon pulses, which enabled them work out the key chain (Pang et al. 2020, Pereira et al. 2019). A fair number of such vulnerabilities need to be overcome to make secure quantum communication a reality.

While the principle of non-cloning gives quantum communication its unrivalled security, in conceptual terms anyway, it is, at the same time, a big obstacle to realising a communication channel over significant distances. Unknown quantum signals cannot be amplified. Unless quantum signals are being transmitted in a perfect vacuum (i.e. in space) they will require quantum repeaters on the way, which creates considerable technological challenges to their implementation. Repeaters are therefore a critical technology for realising the quantum internet. As it stands, China enjoys a considerable edge in this domain.

4.3 Quantum networks

A network that connects at least some quantum computers (nodes) with either classical computers or other quantum machines over a secure quantum communication channel is called a quantum internet (Kimble 2008). A rudimentary quantum network of this kind allows transporting the states of qubits across the network. Assuming sufficient fidelity, it thus distributes entanglement (and hence computational resources) over the network at large. In providing 'entanglement on demand', it can supply quantum compute resources when needed.

Given the notorious difficulties in building large-scale fault-tolerant quantum computers as discussed above, the quantum internet emerges as a neat solution to engineering challenges. Essentially a distributed system, it provides entanglement at scale. 'History is repeating itself, and the internet is about to be born, except this time with quantum bits', the Technical University of Delft's QuTech research outfit confidently claims (Academy 2022).

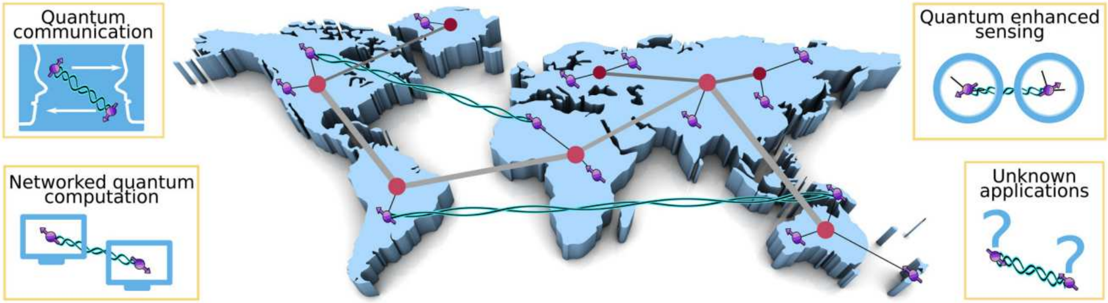


Figure 4.8: Schematic representation of a future quantum internet that connects quantum computing devices over quantum networks, as envisioned by researchers at the MIT and TU Delft. Source: (Ruf et al. 2021, p. 130).

Quite contrary to the frenzy in the media, the quantum internet will not make the classical internet obsolete.[10] Rather, it will extend it and 'add new and special functionality', Stephanie Wehner, one of the leading researchers in this domain, clarifies (Wehner 2019). The first and foremost application of the quantum inter-

[10] The *Daily Express* for instance casts a future of the quantum internet as one that 'will truly blow your mind' as the new internet will create 'unhackable' networks, and be of 'unimaginable' speed and 'infinite' capabilities.

net will be to provide information security such that subnetworks can be protected against eavesdropping and espionage, even if adversaries have powerful quantum computers at their disposal. The second is distributed entanglement to simulate quantum systems–instrumental for any field where the behaviour of large stochastic systems must be modelled, be it in (astro)physics, meteorology and climate science, or medical and pharmaceutical research. A third application scenario is blind cloud computing such that service providers have no access to the algorithms being run, which makes a quantum internet a useful resource for commercial, proprietary R&D research that is plagued with foreign government-sponsored industrial espionage.

1. Information security.

The most commonly discussed impact of quantum computing resources provided over a quantum internet is the threat to standard encryption models such as RSA, as outlined above. RSA does not provide principled security but works in practice because factorisation of very large integers is too tedious and time-consuming a task for digital computers. Shor's algorithm however would factor large primes in polynomial (i.e. not exponential) time:

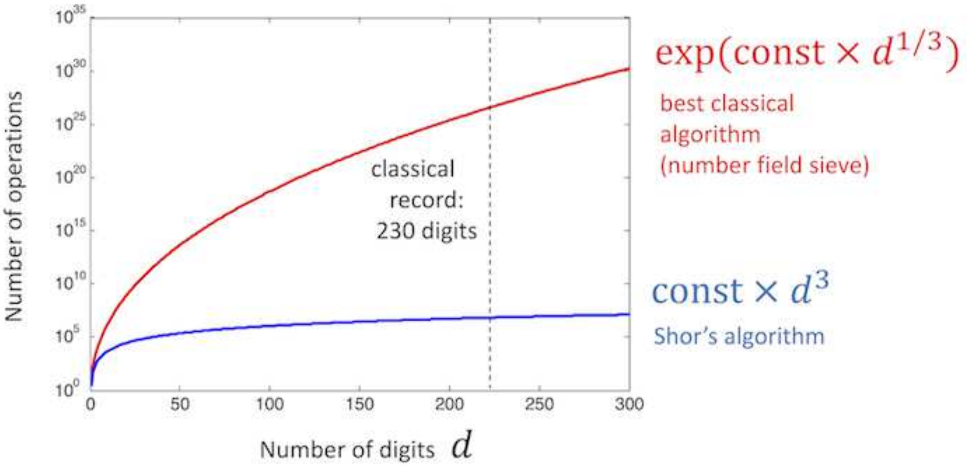


Figure 4.9: The computational costs of factorising large prime numbers. They rise exponentially in the number of digits for classical computers while only polynomially so for quantum computers. Source: (Kitaev 2022) at IBM.

However, if practical issues around its implementation can be overcome, Shor's algorithm, even run from the most powerful quantum computer, is toothless against QKD. QKD is a principled, information-theoretically secure way to encrypt data regardless of the functionality and capabilities of an adversary's computational arsenal. A quantum internet implements quantum communication protocols as discussed in section 4.3 above to offset the advantages of a quantum computer as per section 4.2: a quantum internet provides effective security, a protective shield, against quantum capabilities. The best response to quantum attack is quantum defence. 'To counter this threat', a NATO strategist rightly concludes, 'we will have to completely upgrade all our secure digital infrastructure using cryptography that is 'quantum-resistant', i.e. secure against both quantum and classical computers' (van Amerongen 2021).

One obvious way to do this is to implement QKD. However, as it stands, QKD development has not reached a level of maturity that it would make it reach military grade, or any convincing standard for that matter. This is why GCHQ cannot recommend UK businesses to invest in a highly volatile technology that is likely to see a great number of iterations until it is market-ready. As it stands, GCHQ 'does not endorse the use of QKD for any government or military applications, and cautions against sole reliance on QKD for business-critical networks, especially in Critical National Infrastructure sectors' (NCSC 2020).

Waiting for QKD to mature is not an option either however. If quantum computing development surpasses efforts to engineer trusted and reliable QKD, quantum advantage is likely to present significant dangers to other countries that are playing catchup. To offset the challenges of quantum computing, much work has been done lately in the domain of so-called 'post-quantum cryptography'. The aim of this research is to develop encryption systems that are sufficiently difficult so that not even a quantum computer will be able to break them, let alone a classical system.

In July 2022, NIST announced the winners of an international competition to select the best post-quantum encryption algorithm to become a future standard (NIST 2022). The winner for general web-based online traffic is CRYSTALS-Kyber, a lattice-based encryption algorithm. Lattices are point structures on n-dimensional coordinate systems that create intricate mathematical problems, such as finding the shortest vectors between any two points (Chi et al. 2015). Encryption models then build on these problems that are hard to solve even for a quantum computer, and are thus said to be quantum-proof.

However there is no formal proof that these problems, doubtlessly harder to solve than factoring tasks, are intractable in principle. While they are computationally challenging and will protect against early generations of quantum computers, post-quantum cryptography is quantum-proof by assumption; it is not an information-theoretically secure encryption model. For the quantum internet to be secure ‘by the laws of physics’ some QKD-style encryption model will need to be implemented further down the line.

2. Entanglement as a resource

Arguably the most exciting promise of a quantum internet is to provide entanglement at scale. Large-scale fault-tolerant quantum computers are difficult to build, as section 4.2 above has described. Connecting smaller devices over a quantum internet effectively creates a multi-node quantum computer. The quantum internet then distributes computational resources. The hope is that a system of only a handful of quantum computers smaller than 10 qubits but connected over a quantum channel is significantly easier to build than, say, a stand-alone quantum computer of 100 or more logical qubits. ‘[B]eyond that, the only way to do this is use this modular approach, involving quantum communications’, Mikhail Lukin, from Harvard University says (Castelvecchi 2018, p. 290). A quantum internet would be able to supply entanglement for quantum advantage, the tipping point where quantum computing can solve meaningful tasks better than its classical counterpart, as discussed in section 4.2.

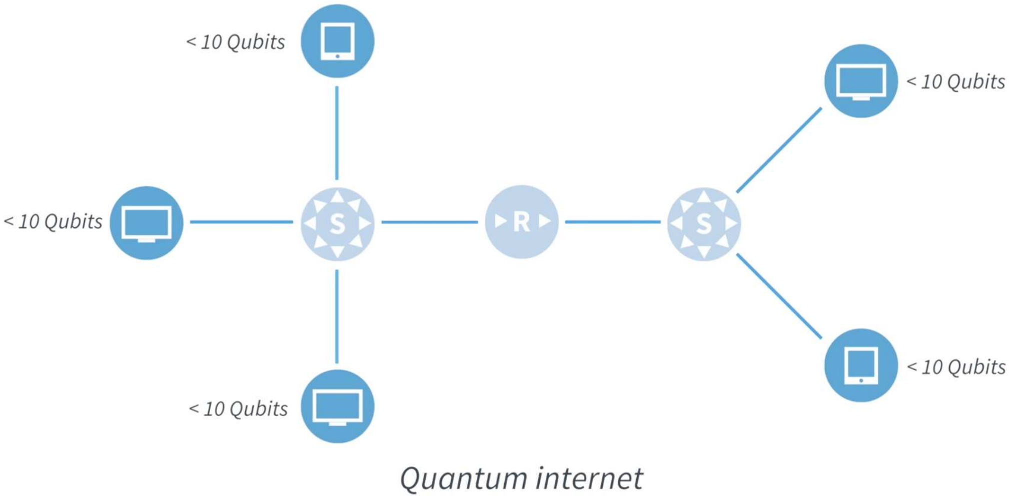


Figure 4.10: A quantum internet with small quantum computers as endnotes, as envisioned by researchers at the TU Delft. Source: (*What Is a Quantum Internet?* 2020).

With each additional qubit available for entanglement, the computational offerings of a quantum internet rise exponentially. In a sense, the quantum internet will reverse the evolutionary logic of computing. As far as the history of the internet goes, useful stand-alone computers were primary. The task then was to link them in such a way that meaningful tasks could be performed over the network. The improvements would be incremental whilst the computational power of the nodes increased steadily. With the quantum internet, however, the network is primary in the sense that the weak-ish nodes it connects will be of little use outside their network function. This is certainly a curious observation with regards to the philosophy of computer science.

3. Blind quantum cloud computing

Most likely, the early quantum internet will be an expensive specialist resource for research-heavy organisations and institutions. Households and individual endusers may benefit from it at a later date, most likely in terms of cloud services (Fitzsimons 2017, Grover 1996).

Cloud services have quickly become critical infrastructure for many businesses and consumers. The term ‘cloud’ comprises three delivery segments: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Global overall spending on cloud services was over $400B in 2021 (Statista 2022*b*).[11] The market is dominated by three US companies (Amazon Web Services (AWS), Microsoft Azure and Google Cloud) that are also heavily involved in efforts to build quantum computers. If they succeed, the market power of these companies introduces system-critical dependencies on a small number of suppliers which establishes long-term, structural risks to China in particular.

If a future quantum internet is QKD-secured, it can offer blind cloud services. ‘People at the server are unable to know what kind of program you’re running and the data you have’, Ronald Hanson from TU Delft claims (Castelvecchi 2018, p. 291). If true, besides its obvious advantages, blind computing would create a whole set of new problems for intelligence services and law enforcement. Cybercriminals that are currently operating on the Dark Web would probably want to move into mainstream network systems if the chance of detection is low. An internet hybrid, partly quantum and partly classical, would considerably widen the attack surface for ransomware, online fraud and data thefts, and thus makes regular users of online services and participants on digital markets that are not quantum-protected more vulnerable. This would effectively split the internet into a quantum fast lane and some second-tier digital legacy infrastructure.

Moreover, the quantum internet is likely to amplify market distorting forces in

[11] The cloud computing market in the UK was around $16B with 44% of the UK population using cloud storage.

an already uneven playing field that is the cloud computing services market. US dominance in this domain must be expected to cement unless China manages to move ahead. Large corporations such as Google dominate both the apps and cloud services markets. This allows them to realise substantial network effects. A hardening of their leadership position in the quantum domain via a quantum internet may further solidify their stronghold in apps, platforms and social media markets. This may have considerable repercussions for consumers worldwide–the US-Chinese quantum race will have global repercussions.

But there are considerable benefits too. Personal and sensitive information, such as health and tax records, could be held securely with great levels of confidence against cyberattacks for many decades to come. With cyberattacks on public bodies significantly on the rise,[12] a quantum internet would support long-term compliance with privacy regulation.

Banks and financial services are likely to move to secure quantum communication networks for transaction and clearance purposes, and the storage of customer data (Dietz et al. 2020). The chances of third-party hacking into retail banking accounts would be low, with the potential to make the requirement for Multi-Factor-Authentication (MFA) obsolete. Many businesses incur significant financial damages due to industrial espionage–for the UK alone, the figure is the equivalent of about 3% of GDP annually, the UK's Intellectual Property Office estimates (Searle 2021). With any cyber-physical system only being as strong as its weakest link, running corporate R&D programmes on a secure quantum cloud service will provide protection against the theft of intellectual property.

The Web has certainly turned out differently than its inventor had hoped (Berners-

[12] CSIS publishes regular updates to its 'Significant Cyber Incidents' log of attacks on public institutions.

Lee 2019, Bridge 2018, Solon 2017). Technology is indeterministic. For this reason, the three obvious areas of application of a quantum internet are unlikely to characterise it in full, when it arrives. A fully developed quantum internet may be quite different from what is imaginable today. A few things seem certain however. While a quantum internet requires quantum computers as critical nodes, not every node in the system need be a quantum computer. This makes the integration with legacy internet infrastructure likely. The emergence of an entirely separate quantum internet that would sit parallel to the internet as it exists now is an implausible scenario. So what are the major obstacles in achieving this integration?

4.3.1 The compulsion to repeat

At the beginning of the twentieth century, telephony suffered a considerable problem: calls over long distances were impossible to make due to the scaling of noise such that conversations with parties outside city borders would quickly become impossible. What was missing 'was a satisfactory telephone repeater', AT&T realised (Gertner 2013). In response, Bell Laboratories began incorporating Lee de Forest's 1906 invention of the 'Audion' vacuum tube for the purpose of telephony, which enabled the first coast-to-coast long-distance call from New York City to San Francisco in 1915.

The quantum internet faces similar challenges. As outlined above, quantum signals cannot be boosted or amplified. They decohere and die out quickly due to atmospheric interferences; the maximum range on Earth for a single photon shot is about 100km (Azuma et al. 2015, Briegel et al. 1999). As a way of illustration, if the distance between two quantum nodes in two cities were 1,000km, and no repeaters installed, a constant stream of photons would need to be fired at a rate of 10GHz, and still the receiver would need to wait many years for only a single photon to come through all the way–such is the loss rate of optical fibre (Flagship 2022). For internet applications, this is obviously hopelessly inadequate.

For a truly global quantum internet, quantum repeaters are required that work against the exponential decay of quantum signals. Consider two quantum nodes A and B. The specific quantum state of a photon is to be transmitted between A and B but the nodes are too far apart so a repeater node R is placed equidistant between them. Then, A prepares a pair of entangled photons. It holds onto one of them and transmits the other one to R. This move preserves the state of entanglement. At the other end, B also prepares a pair of entangled photons. It also holds onto one of them (stored in a quantum memory device) and sends the other one over to R. Here too the state of entanglement is preserved.

The repeater node now holds two photons, one coming from A, the other one from B, each still entangled with their source. The repeater node R now performs a specific measurement on the two qubits it holds. The nature of quantum mechanics is such that this act of measurement reveals a state that is identical between all four photons in the chain. R now discards the two photons it had stored. This leaves both A and B with a qubit each, both of them in the same state. A has effectively transferred quantum information, i.e. the state of the qubit, to B. This process is called 'entanglement swapping', it effectively means that the state of the origin qubit at A is 'teleported' over to B. If necessary, this process can be repeated several times across n repeater nodes $R_1, R_2, ..., R_n$ in the chain (Bouwmeester et al. 2013, Hermans et al. 2022, Niemietz et al. 2021, Zeilinger 2010).

The non-trivial obstacle to realising the quantum internet is therefore to build a chain of quantum repeaters that can be connected via existing optical fibre networks. The QuTech team at TU Delft hopes to connect four Dutch cities over a rudimentary quantum internet by 2023; it would leverage the Netherlands's existing telecoms infrastructure (Pompili et al. 2021).

Not surprisingly, China aims bigger. A vast country, distances to be overcome are of a different scale. China is the only nation that has so far successfully demonstrated an alternative approach to quantum teleportation over optical fibre: satellite communication. In what must be considered an extraordinary engineering feat that has rightly gained international praise, in 2016 China launched *Micius*, the first ever quantum satellite (Liao et al. 2017, 2018). Named 'Quantum Experiments at Space Scale', or QUESS, the satellite is a collaboration between the Austrian and Chinese Academies of Science. In 2017, the research team managed to quantum-secure a short video call between China and Austria where the satellite acted as a trusted repeater (Liao et al. 2018, 2017, Yin et al. 2020).

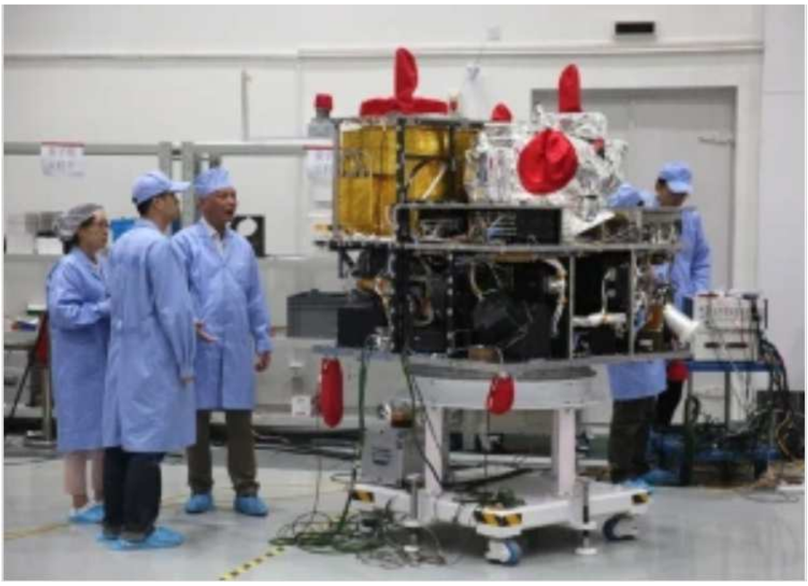


Figure 4.11: China's 600kg *Micius* satellite before it was fitted to the launch rocket. Credit: Cai Yang/Xinhua via ZUMA Wire. Source: (Gibney 2016).

From an international security perspective, it is worth noting that the Principal Investigator of the Austrian research team, Prof Anton Zeilinger, had originally pitched the idea of a quantum satellite to the European Union–only to be rejected. In 2001, Zeilinger tried to convince the European Space Agency of the value of QKD for secure communication but the pitch fell on deaf ears (Peyman 2018, p. 314). It can be assumed that the EU has come to regret this decision. One of Zeilinger's students was Pan Jianwei, who had quickly risen to the top of China's elite quantum research group, and secured funding for *Micius* from the Chinese Academy of Science in the region of $100m. Pan then got Zeilinger involved. Since then, Zeilinger has advised China on quantum affairs. In 2019, he was awarded the 'Micius Prize' by the Chinese Micius Quantum Foundation for 'outstanding application-oriented research in quantum physics' (Austrian Academy of Science 2019).

The satellite acts as a quantum repeater. In space, photons can travel farther than on Earth where atmospheric interferences cause photons to die out relatively quickly. Relayed over the satellite, Chinese researchers have so far managed to distribute entanglement over distances of up to 1,200km (Yin et al. 2020). The caveat, as with ground-to-ground repeaters, is that the satellite must be 'trusted' in the sense that it must be ensured it will not leak information to third parties. In the original experiment, for instance, the satellite needed to hold the quantum states it had received from China and then wait and hold on to them for some while en route to Austria. This waiting period creates additional vulnerabilities.

Once in sufficient proximity to Vienna, the satellite emitted photon pairs to the ground station there. Travel time in space from Asia to Europe makes the satellite vulnerable to attack. For it to be a trusted repeater, several separate protocols must be in place that ensure it had not been compromised. Thus a secure quantum channel in space still very much requires communication security in classical terms and is best considered a layered concept. For both ground-to-ground and satellite-to-ground quantum communication, significant engineering challenges remain.

The error rates of satellite QKD are considerable, and *Micius* can only operate at night to minimise interference. Still, the satellite is a considerable reputational asset for China and a very significant achievement. The US or the EU have yet to launch their own satellites for such purposes, and it is not obvious if they will. China seems determined to push ahead in quantum communication, which is less a concern for the US. Research commissioned by the DoD confirms that 'several independent lines of evidence indicate that Chinese R&D is focused much more on quantum communications than [the] U.S.' (Parker et al. 2022, p. vii). It almost seems as if Western alliances have resigned to the fact that China is too far ahead in this domain.

The US seems to have decided to focus on quantum computing instead. Its military command holds the obstacles to realising QKD too significant for it to have any practical value in the field (see graph below). This is echoed by GCHQ, as discussed in the following chapter. But this view may prove shortsighted.

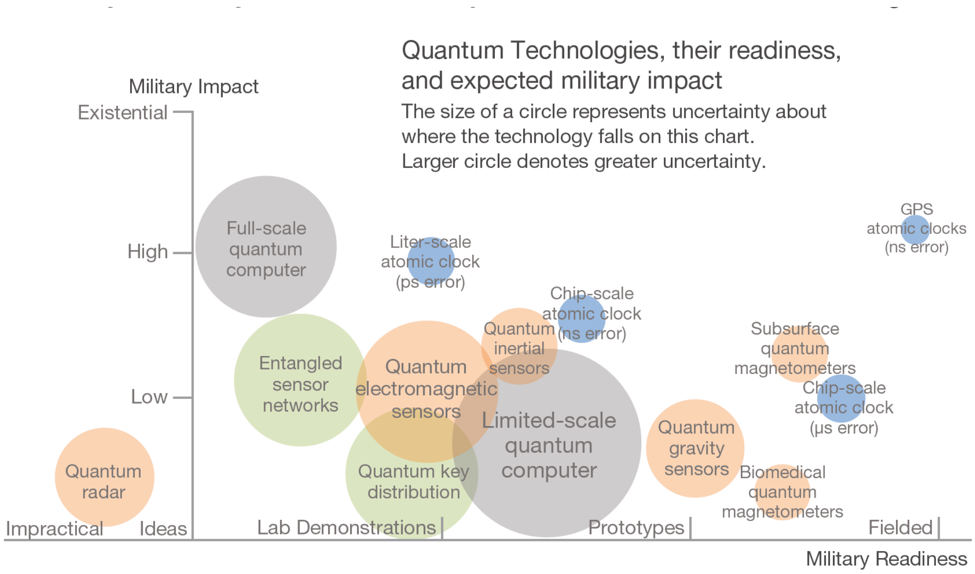


Figure 4.12: The US Department of Defense's 2021 assessment of the potential military impact of nascent quantum technologies. Source: (Parker et al. 2022, p. 13).

For a global quantum internet to work a reliable quantum communication protocol is indispensable. In light of China's efforts in this domain it must be concluded that the Chinese leadership has a much stronger interest in building a network of this kind. This conclusion is corroborated by the high-quality research output in the areas of satellite- as well ground-based quantum repeaters. And it helps explain the big push for Chinese standards and governance models that international organisations have witnessed over the past five years. China, it seems, is determined to shape significantly the quantum internet of the future. Even if QKD is not of military interest primarily, it will support a Chinese power base. Western alliances seem remarkably relaxed about this outlook.

4.4 Main points of Chapter 4

The major take-aways of this chapter are as follows:

Quantum fundamentals

4.a Computationally expensive programs in AI and ML will soon run into hardware problems. This is because digital (or 'classical') computing built on micro-transistors placed on silicon chips has reached a natural limit to its growth.

4.b A classical bit can only ever be in one of two states, usually labelled 0 and 1. These two states are physically realised on a micro-transistor to which voltage can be applied (0 = no, 1 = yes). This binary system determines the number of operations a digital computer can perform.

4.c A qubit has considerably more degrees of freedom and can choose state spaces between 0 and 1 such that, colloquially speaking, it is both 0 and 1 at the same time. This state is called 'superposition'.

4.d Two or more qubits can be superimposed. Their combined state-spaces are a linear combination of their individual states. These combinations can represent information.

4.e Within this set of superimposed states there exists a class of special qubit-to-qubit relationships that cannot be reduced. Qubits in this special state are said to be 'entangled'.

4.f With each additional qubit so entangled, the number of operations a quantum computer can hold at any one time rises exponentially. In classical computing, the growth rate is only linear for each additional bit. In principle, this makes quantum computing exponentially faster than traditional, digital computing.

4.g Quantum logic gates manipulate the state-spaces of entangled qubits, e.g. by flipping the spin of an electron. This is achieved by laser beams and microwaves.

4.h In addition to the massive increase in compute resources, quantum computers are hoped to be able to run certain classes of algorithms that are intractable even for the best digital supercomputer. The most prominent example is 'Shor's Algorithm' for factoring large integers, which poses a considerable threat to RSA encryption models.

4.i The single biggest obstacle to realising even a modest quantum computer is error correction. While computate resources scale exponentially for each additional qubit, the same is true for errors, interference and noise.

4.j University research centres in quantum computing can oftentimes leverage relationships with physics departments in order to build new experimental devices. Private corporations do not usually have this expertise easily available. This explains the difference in choice of qubit modalities among private sector corporations and publicly-funded research.

4.k Established companies as well as start-ups begin to register quantum patents at scale.

4.l The US is largely considered leading in terms of research output and experimental progress in the domain of quantum computing. What makes the US quantum ecosystem so successful is the fact that it is characterised by highly productive collaborations between universities, industry, and government bodies.

The quantum internet

4.m Commentators suggest that China is concentrating its efforts on advancing its leadership position in quantum communication while the US seems determined to cement its competitive edge in quantum computing.

4.n Quantum communication is the application of superposition and entanglement for the encryption of messages over significant distances. It builds mainly on an important qubit modality: photons.

4.o A network that connects at least some quantum computers (nodes) with either classical computers or other quantum machines over a secure quantum communication channel is called a quantum internet. Essentially a distributed system, it provides entanglement at scale.

4.p Quantum signals cannot be amplified or copied. Unless quantum signals are being transmitted in a perfect vacuum (i.e. in space) they will require quantum repeaters on the way. Repeaters are therefore a critical technology for realising the quantum internet.

4.q The quantum internet will not make the classical internet obsolete but add new capabilities to it.

4.r There are several important applications and use cases for a quantum internet, the most important ones being information security, the provision of compute resources over a quantum network, the modelling of complex systems and the provision of secure cloud services.

4.s A quantum internet is hoped to provide effective security, a protective shield, against the quantum capabilities of adversaries. The best response to quantum attack is quantum defence.

4.t While lattice-based post-quantum cryptography is computationally challenging and will protect against early generations of quantum computers, post-quantum cryptography is quantum-proof by assumption; it is not an information-theoretically secure encryption model. For the quantum internet to be secure 'by the laws of physics', some QKD-style encryption model will need to be implemented.

4.u Households and individual users may benefit from the quantum internet in terms of cloud services. At present the cloud services market is dominated by three US companies that are also heavily involved in building quantum computers. If they succeed, the market power of these companies introduces system-critical dependencies on a small number of US suppliers.

4.v An internet hybrid, partly quantum and partly classical, could widen the attack surface for ransomware, online fraud and data thefts, and thus make regular users of online services and participants on digital markets that are not quantum-protected more vulnerable. This would effectively split the internet into a fast lane and some second-tier digital legacy infrastructure, adding to the ‘fragmentation’ debate.

4.w Quantum-protected personal and sensitive information, however, such as health and tax records, could be held securely for many decades to come with great levels of confidence against cyberattacks. Running corporate R&D programmes on a secure quantum cloud service will provide protection against the (state-sponsored) theft of intellectual property.

4.x China is the only nation that has so far successfully demonstrated an alternative approach to quantum teleportation over optical fibre: satellite communication. The quantum satellite *Micius* distributes entanglement over distances of up to 1,200km compared to 100km or so over ground-to-ground repeaters. But travel time in space makes the satellite vulnerable to attack.

Chapter 5

Internet governance in the 2020s

The previous chapter has developed an overview of key quantum technologies that are required to build a quantum internet: noisy, mid-range quantum computers, quantum communication protocols such as QKD, and an infrastructure to connect quantum hardware via ground- or satellite-based repeaters. The chapter has found that early quantum networks will add capabilities to the existing internet rather than replace it–premium services that are likely come at considerable extra costs to end users. Above all, a new quantum infrastructure promises the great powers a major advantage in the global emerging technology race that chapter 2 has discussed. Chapter 3 has made the case for pairing interview data with quantitative analysis: **R.1.1** asks, what do domain experts observe regarding US-Chinese competition in internet governance? What does internet governance presently involve, and how is it going to evolve in the years to come?

In pursuing these subquestions, Section 5.1 of this chapter discusses larger political tropes against which the rivalry over the internet of the future unfolds. It discusses how China has grown considerably more assertive, and now seeks to dominate important standardisation bodies. Quantum communication, and QKD in particular, emerge as key technologies for China to push globally for Chinese internet and telecommunications standards. This move, the Chinese leadership hopes, helps the Party to sustain its role as 'data sovereign' while also to increase trust among the general population. Chinese QKD must be considered a direct threat to Western economic and security interests.

The chapter then moves on to discuss Chinese activity at international bodies in more detail, in particular around 'New IP', Huawei's recent proposal for a total redesign of basic internet architecture and protocols. 'New IP' has generated deep scepticism among interviewees for its inbuilt capabilities for near-perfect surveillance and control. As obviously problematic as the proposals may be, informants argue that it will be increasingly difficult for Western alliances to keep rejecting Chinese ideas unless they are willing to present genuine alternatives–of which none are on the horizon.

Section 5.2 then explores the implications of the current governance conflict for the quantum internet. Two major themes emerge here. Chinese quantum internet technologies are likely to provide China with significant reputational gains while providing a considerable economic boost also. With a view to the West, US big tech companies are asymmetrically more likely to benefit from quantum internet technologies in comparison to smaller businesses. This would increase economic concentration in the West and present additional regulatory headache.

While the direct security threats of Chinese QKD should prove manageable, respondents from GCHQ and the UK Cabinet Office warn of economic repercussions for economies such as the UK that may get drawn into a spiralling internet governance conflict. The protection of British intellectual property emerges as a chief concern, amplified by the observation that the very object of internet governance will only increase in magnitude. The informant at the United Nations points out that internet governance over the coming years will be impossible to separate from other regulatory concerns, which provides China with an even bigger opportunity space to shape not just the internet of tomorrow but large parts of Western policy. Section 5.3 concludes and presents the major takeaways of this chapter.

5.1 Internet governance and strategic competition

Chapters 2 and 4 have established that quantum internet technologies, and wrangling over internet governance frameworks, are at the heart of the strategic competition between the US and China. The dynamics of the complicated relationship between the two superpowers will shape the quantum internet to no small degree. In this section, with an eye to US-Chinese competition, respondents provide some broader framing and background for their views on how the internet of the future is likely to be governed. For informant F, despite what British, European and Australian leaders may think, the game for global dominance is very much a US-Chinese one–in the eyes of China anyway.

> ‘The worldview in China is that it’s China versus the US. That’s the hierarchy level. And then everything else has to be slotted into those categories, friend or foe, with us or against us. This idea that there is this kind of non-aligned neutral mass, that’s something that the

> Chinese have dealt with for a long time. That was their belief for a long time, and I think that is one of the fundamental things that have changed. They have slotted us in, slotted Europe in, they have decided that in case they go to war with the United States the Europeans will be on the side of the Americans [...]' (F)

In this view, China no longer accepts neutrality. According to the respondent, China's strategic outlook has changed dramatically under President Xi. While (geo)political non-alignment of trading partners used to be respected, or rather bracketed, the Chinese leadership now seems to consider most countries antagonistic. The informant continues:

> 'The strategic environment has decoupled. Let's not forget, they only have very few treaty allies. North Korea. The best buddies are North Korea and Pakistan. And a couple of African states, and that's not a coalition to win a war with, you know, it doesn't work that way. *So they need to make sure that the alliance between the Americans and the Europeans is at least weakened. So while we [Europe] are slotted in there, we can be an enhancing factor for the Americans, or we can become a drag on their capabilities, and that's what China would like to see us become: a drag on the Americans, like them being very busy with our transatlantic relationship.*
>
> That's why AUKUS[1] was so great. Seeing the French being completely angry at the Americans and backstabbing the UK and the Australians laughing on the other side of the ocean and you know this, this whole

[1] Announced in September 2021, AUKUS is a security agreement between Australia, the US and the UK. While the pact sets out a wide range of collaborations, including AI and quantum technologies for the purpose of intelligence sharing across the Five Eyes, the most significant agreement, to the anger of China, is for Australia to acquire US nuclear submarine technology.

> ordeal. I mean there'll be nuclear-powered submarines in like 20 years in Australia, that doesn't bother the Chinese military planners so much right now. . . ' (F, emphasis added)

The respondent talked in detail about Chinese efforts to drive a wedge between US and European partnerships just to keep US planners and strategists occupied. In F's view, Europe is only of little strategic interest to China; it is sufficient for the Chinese leadership to cultivate disunity among European leaders for Europe to become paralysed and unable to speak with a unified voice. Quite unlike the fanfare in the press, AUKUS then is not quite the success it was portrayed to be–in its aftermath, divisions in Europe have only become more visible. According to the informant, China now considers Europe's institutions 'hopeless' to the point that the European Union is not being taken seriously in terms of geopolitical and strategic considerations. With regard to internet governance in particular, there is little, if any, Chinese appetite to engage with European proposals, the informant said.

Shifting the conversation towards the US, what has brought about the intense deterioration of the US-Chinese relationship? While media commentators often point to the Trump administration's initiating a trade war, for F, the US position had not changed dramatically at all. If anything, it was China that decided to change course radically under President Xi.

> 'I think that's something that is often overlooked. It wasn't a decision by the US or by Europe or whatever, we would have been very happy to continue to do exactly what we've been doing, it was fantastic! China as an open market, China as a participant in the global economy is hugely beneficial to all of the other market economies, it's fantastic to

> have another great market with huge potential, with a lot of capital, with an entrepreneurial spirit that is wide open to innovation, open to adopting new things, so that used to be great, but then things changed in China, and things have changed so rapidly that it is really hard for businesses and for politicians to keep up.
>
> So if you ask me, now, today, what the opportunities are for engaging with China on emerging technologies, I would say they're probably near zero, because the environment that is being created in China is one that is not conducive to cooperation anymore, it is one where *the Chinese are kind of waiting out their time until they have a strategic advantage, and then capitalising on that, it is not intended to be cooperative, it is not intended to be win-win. If anything, it has tended to be a kind of the Chinese win-win version where China wins twice.*' (F, emphasis added)

The informant was adamant in their views that the fault for the hardening of positions rests with a considerably more assertive China that had decided to change strategy and play a waiting game, and watch from afar how Western alliances crumble. In particular Europe has been guilty of considering China something akin of a blank canvas, a large market yet with no real political aspirations, a place of endless opportunity where Chinese consumers would never cease to demand European goods. A grave error. This game, it seems, is over.

What is the rest of the world to do in light of a more robust and confident China that openly pursues its national interest? Respondent E points out that a small number of countries do not wish to get drawn further into this accelerating US-Chinese rivalry. Instead, at international institutions such as the United

Nations, they seem to try and forge new alliances to escape the vortex that is great-competition. However, E is pessimistic about such prospects.

> 'There are very few countries that are deliberately acting to change that [dependence on either the US or China]. I know India has created the public infrastructure that is open source to run governmental services but it's really an exception. If you look at who is actually running government services [in practice], you're going to find the same usual suspects. The same companies that we've seen operating everywhere. So it's really a question of finding that third way, which is not the public-private partnership because they still have the same dynamics but a real alternative to what we currently have.' (E)

While there is growing discontent with such dependencies, or where they become more obvious, there is no genuine alternative for other countries to take. The sheer degree of leverage that the US and China enjoy over emerging technologies in particular makes it difficult to avoid siding with either of the two superpowers. According to E, regarding the governance model for the internet of the future, there is no way to circumvent the US-Chinese conflict.

> 'This is a hard conversation to have, because we've seen it a lot in the UN system at least where some of the discussions that I was following are very much focused on this huge geopolitical divide. You have the US on the one side and the European partners and then you have, China, Russia, and the rest of the world.
>
> But many of the developing countries are now saying, I don't want to be in any of those camps, we actually want to put forward our

> own agenda, some of our own issues, and that's more related to the development of technology and questions of ownership. It's still very hard because at the end of the day, the technology in Africa is still mostly provided by the Chinese and in Asia, there's a bit of a fight over American versus Chinese dominance. But yeah, at the end of the day, *crafting a completely new form of governance that doesn't have all these strings attached is probably impossible.*' (E, emphasis added)

Many countries, it seems, realise that they are locked into an international relations conflict that demands they take sides. Internet governance is no exception. Against this backdrop, it is safe to assume that the emergence of the quantum internet will be shaped significantly by US-Chinese rivalry. But what exactly is China's game?

5.1.1 Chinese ambition: quantum communication

China's efforts for infrastructural control over the internet of the future are very much a continuation of Maoist principles, respondent F finds.

> 'The state is fundamentally not just about individuals. China is not so worried about the individual blogger, they take them out if they think that they create a problem, but that's not necessarily the immediate aim. It's more to create a structure that allows for as much control as possible at all levels, and that's something that is not new. If you look at the Mao days in the 1940s, 50s, and 60s you have, in China, a government system that is running down to the level, down to the work unit or down to the housing block that you live in. Today, it's a

> surveillance and control system that had previously been undertaken by people. Now, the classic "Blockwart"[2] is something that is just so inherent in the Chinese system that it probably feels freer to have that done by technology today than by people.' (F)

This is certainly a curious take. If surveillance and control cannot be avoided either way, people may be more accepting of emerging technology as it will not judge. So for the Chinese state, according to the informant, internet governance and cybersecurity policy are about control and the dystopia of near total surveillance. But these technologies are also about managing new forms of risk to Party power that emerge today, primarily from domestic industries, not necessarily foreign adversaries. F continues:

> 'There are so many things that are so deeply ingrained and deeply embedded and controlling big tech at the moment is important, not just because they have accumulated a lot of money but because of the destabilising potential that they have on the entire Chinese economy.' (F)

F here confirms recent articles in Western news outlets, in particular *The Economist*, that report how the Party is reining in on corporate power. The move has seen some founders and CEOs arrested while others have had to pay significant fines, or saw their IPOs postponed indefinitely (Economist 2021, Weinland 2021). For F, any new technology that somehow relates to the internet is of particular concern to the Chinese leadership.

> 'I think that Evergrande [the large Chinese property developer] was a

[2] The "Blockwart" in Nazi Germany, a neighbourhood guard, would usually be a civilian; a housing officer and resident at a block of flats who would report subversive or otherwise un-German behaviour of fellow tenants to the Gestapo.

> good example of that, when you have companies that grow so powerful that they can tank your growth, that they can tank your economy so you have to bail them out, and that they are in a position that they control data that you don't have, well that is problematic. *So for the Chinese Communist Party, it is important to maintain a kind of data sovereignty over everyone else and have the prerogative of the state and the party inbuilt into technology development* [...]
>
> Xi Jinping says, there needs to be a blockchain with Chinese characteristics, there needs to be like a blockchain controlled by the Communist Party. That, to me, inherently, that's a problematic thought, it doesn't really work that way. *But from a Chinese perspective, that seems a logical application of the technology that you say blockchain works on that level where it creates trust, and obviously above that is the Chinese Communist Party.* It's not designed to be that way but that doesn't mean it can't be that way right? (F, emphasis added)

Several issues emerge at this point. Party officials are apprehensive about domestic Chinese big tech where such firms as they may establish themselves as internal rivals. In particular social media and e-commerce companies hold data on a vast part of the population, their preferences and proclivities, and these data must not be beyond the reach of the state. There can be no private sector data sovereign, the informant finds, no data authority above the Party. New internet technologies must therefore be designed in a way that enables the state to siphon off any data it desires.

However, new internet technologies must also be trustworthy. The Chinese leadership wants internet technologies to be trusted so that people are disincentivised to find offline workarounds, or find different channels for communication and payment clearance purposes that would upset the Chinese economy and power structures alike. A genuinely Chinese internet technology may meet this dual objective: trusted by the Chinese people as well as their leadership. Once again, on top of that trust pyramid there must be no room for anyone other than the Party. This leaves China's big tech companies struggling–perhaps for good reasons, as F points out.

> ‘Company [redacted], a state-owned enterprise, it's a big conglomerate that does all sorts of different things. So I met their representative and asked, how you do you want to do data governance in the future? She was very gracious, in her mid-30s, internationally educated, and she was saying how they are in this problematic situation in China, where a lot of really crucial data is stored with private companies–and that's not safe, she said. I mean, you would rather want the state to control your data, right, rather than a private company?, she asked me.
>
> So there are fundamentally different ways of approaching this. They say, I have a huge level of trust in the state, or at least I should have a huge level of trust in the state. They're coming at this from that angle. So, I think, rather than to say, this is all strategic and all driven by the Party and they would enhance their influence here and they want to enhance their influence there–that is, to a degree true, but all this is also driven by this grappling with problems and complications that digitalisation brings about for China, that the leap-frogging on a number of these issues has made things like early adaptation of technologies, particularly in FinTech, not a problem in China.

> But then how do you make that safe, how do you make that secure? *It's not that the Chinese Communist Party fundamentally has the worst for the Chinese people in mind, that's not the point. That's not what they're trying to do, but they obviously have a different set of priorities and getting that right from our perspective is I think the difficult task.* This is where we have to navigate properly.' (F, emphasis added)

It seems that China's laissez-faire attitude towards big tech, pursued to counter US economic dominance, has come to bite the leadership as China's big tech companies have now emerged as internal, domestic rivals to Party control. These companies hold vast assets, financial and data that contains vital intelligence about the Chinese population. The Chinese leadership must limit their influence yet a harsh clampdown may have negative effects on economic performance and public opinion. The Party needs to manage public trust carefully.

So it should not come as a surprise that the Chinese leadership demands a technology, applicable to internet commerce and blockchain, that extends trustworthiness downwards to the general population but can also be trusted by Party officials to do the job. Only a genuinely Chinese technology may achieve this. For China, QKD is the perfect technology to deliver this dual objective. Trustworthy by design and delivered by Chinese scientists and engineers, it promises an encryption protocol untainted by Western meddling. The 'laws of physics' that quantum engineers oftentimes solicit to sell QKD extend to Beijing in that they guarantee the US will be unable to extract signals.

The GCHQ informant very much corroborates this view.

> 'Let me talk about QKD. So yeah, the Chinese are very much ad-

> vocating the use of this and are building long distance networks and technical devices, putting satellites up and all sorts of things. And that's very different from what's happening in the UK and the US. I'll refer to 'us' as the West for shorthand. We are sceptical about the actual value of QKD, what actually does it buy? You actually can't use it a lot. It's just a complicated, expensive way of doing something that we already do, effectively [...] But nonetheless, China and other countries are investing heavily in this now. What I think, there's different reasons. *One is obviously the Chinese sort of distrust of the West and maybe the US corporations in particular.*' (C, emphasis added)

In line with the 'Made in China 2025' plan, GCHQ confirms, the Chinese leadership seems to have decided to not trust foreign technologies in principle. If state control sits at the top of the aforementioned trust pyramid, foreign technology must be excluded. The GCHQ informant continues:

> 'Information was leaked in the Snowden revelations a few years ago that have alarmed some countries about that they might not be able to trust US security services entirely. So again, it's not all true, don't believe everything you read in the press. But some countries, in particular China, Russia, more paranoid countries don't like to trust security services in the West as much. There's a lot of Chinese investment across the board. In IT, they have a programme where by 2025, they'd like to source everything from within China, making the chips to the software stacks and operating systems and all of that to be made in China rather than relying on Microsoft.' (F)

It is not entirely clear from the conversation why China and Russia should be ‘paranoid’ for not trusting Western security services; arguably it would be foolish if they did. To be fair, China trusts Western technologies just as little as the US trusts Chinese systems, as the recent ban of Huawei and ZTE shows. And in terms of rhetorics, China’s ambition here is not very different from the European Commission’s repeated call for ‘technological sovereignty’ (Bauer & Erixon 2020) and independence–the chief difference being that China has the industrial policy and infrastructure in place to be able to achieve it.

In addition, GCHQ identifies potentially huge reputational gains for China.

> ‘Another element is, it’s like a first man-on-the-moon-thing, trying to launch a large-scale QKD network or QKD satellite ahead of the West, that’s for national pride purposes, that’s big and you know, countries like China and Russia are still operating in that way. Whereas I think certainly the UK doesn’t tend to do this anymore. But if you can just think of this, first-man-on-the-moon or Mars or that sort of thing, that’d be a big publicity thing.’ (C)

While this is certainly true, it should be added that based on the discussion above, Chinese ambition is not just about signalling technology leadership to Western powers. *Micius* and QKD are just as much about *internal* signalling: showing domestic industries and the population that China is able to build a trustworthy internet infrastructure that makes Western dependencies a thing of the past. With China’s ambition so characterised, how big a threat to the West is QKD, and how will it shape the quantum internet?

5.1.2 Quantum communication and Western security interests

The UK Cabinet Office and GCHQ consider the fallout of Chinese QKD containable and manageable. The bigger issue arises from intellectual property rights and the significant economic gains that China could make thanks to quantum-encrypted satellite-to-ground communication. The informant at the Cabinet Office says:

> ‘When you talk to people about quantum communications, they tend to panic [laughs], ‘Oh God, this is bad’, but when you talk about some of the details and all the caveats that must be considered people worry less that tomorrow someone is able to teleport a piece of information from A to B because there are all these extra caveats that need to be worked out and things like that. I think the main concern at the moment is the protection of IPR [intellectual property rights] rather than anything else but we haven’t brought this up with Ministers yet.’ (B)

The notable lack of urgency is likely due to GCHQ’s deep scepticism about QKD:

> ‘My organisation worries about protecting government networks from phishing attacks, malware, ransomware, all that. So that is absolutely where the cyber security action is these days, that is our focus. Old-fashioned military cryptographers, those are the people that might have some use for QKD. QKD just doesn’t address 90 percent of the actual problem space for government.’ (C)

This is in stark contrast with the Chinese position and attests to very different views about the role of government-controlled cybersecurity in internet governance. Arguably, 'old-fashioned military cryptographers' will have a significant voice in internal Chinese affairs. Smaller states on the periphery of Chinese influence also take QKD more seriously, perhaps because the nature of the threat is closer, both geographically and politically.

Singapore enjoys a particularly curious status in US-Chinese competition thanks to its strategic alignment with the US, which makes the 'special relationship' with China 'awkward' (Peng Er 2021). For informant A, QKD emerges as a key technology that will make Singapore a global player in this technology.

> 'We are trying to extend that range [of QKD] globally. We have looked in Singapore to have a shorter radius of fibre. But we're going to do that globally. What they're doing in Delft in the Netherlands with these quantum repeaters, it does make sense but we as a community we feel that even if some of the challenges with quantum repeaters are overcome you're not going to be able to link up the whole world with quantum repeaters for quite some time. There is no alternative to satellites [...] So we also want a satellite.' (A)

Statements of this kind are evidence for a self-sustaining and self-propelling quantum security arms race. If China has a satellite, other countries are likely to wish to keep up with China and build a satellite also.

Singapore is very keen on implementing QKD in the near future and recognises China's leadership position.

> 'The West is leading in quantum science, but when it comes to QKD

> it's more complicated, I'd say China because they have invested so much money in developing this capability [...] That would be a game changer and give the state new power [...] if they have it and you don't, your signal quality will drop. You haven't kept up with the game, and there's no way you can fix it. But, you know, the US is a bit funny about encryption as it falls under the purview of the NSA.' (A)

Informant A implies that not all US research on QKD may be in the public domain. If this is true, it would have to be assumed that QKD is much more of a concern to the West than openly acknowledged. The participant from GCHQ however stands firm.

> 'I have to come back to looking at the systems perspective. So this claim that quantum communication, QKD, is secure, guaranteed by the laws of physics, only applies in this situation where you got A talking to B either over optical fibre or through free space such as a satellite or however you want to think of it, and there's nothing else in between.
>
> So as soon as you put any sort of repeater node in the middle, that claim that is protected by the laws of physics goes away, because obviously, that node could be corrupted, it could just break on its own or degrade over time or an adversary could jump on it and do a denial-of-service attack. Or if you're going into space, you could imagine trying to block the signal that's going into space. . . ' (C)

The respondent is certainly right to point up all the challenges that QKD presents but what if they can be overcome? When it comes to QKD, GCHQ expresses significant trust in NIST and expects standards bodies to do the right thing when the time comes.

> 'We're quite sceptical about QKD and we're recommending businesses and government users and critical national networks: wait until this next generation of mathematical software algorithms becomes available and standardised, which will happen over the next three to five years and to upgrade your systems at that point because we think that people panic and upgrade too quickly. They might pick something that either doesn't work or something that doesn't get standardised. And so you've got to change twice. That's with all the cost, and whatever [...] *We recommend, do not panic, wait for the scientists to do their job and say, we now recommend this new set of algorithms for quantum systems, then the standards will start to appear from global standards bodies that control the internet and telecoms networks, and then to migrate*' (C, emphasis added).

The final sentence in this response highlights just how much GCHQ relies on standards bodies to find a standard that is not orthogonal to Western interests. This level of trust however may prove problematic. Do internet standards really just 'appear'? The sentiment here seems that standards bodies can be trusted to find frameworks that are 'good' from a Western perspective. This requires these bodies to hold up against Chinese influence. The following subsection discusses that this could prove a myopic view. There is little ground to assume that GCHQ-approved standards will naturally 'appear': China now holds considerable influence over some of the standardisation bodies that GCHQ wants to rely on.

5.1.3 Loci of US-Chinese competition: internet standardisation bodies and big tech

It is being recognised in the literature that internet standardisation bodies have become a central place where great-power rivalry plays out (Carr 2015, DeNardis 2014*a*, 2020, Radu 2019, Weinberg 2000). Many commentators fear that the current 'multi-stakeholder model' for managing the internet, which invites governments as well as industry and civil society representatives to the table, is unlikely to survive. Curiously, for the informant at the internet standardisation body, the move towards multi-stakeholderism many years ago was already an attempt to contain China.

> 'The way the internet was originally designed was that it was community based. So if China wanted to do one thing and we wanted to do something different, that's okay as long as we use IP [Internet Protocol] and we can talk to each other, as long as the infrastructure talks.' (D)

Moving away, however, from a radically flat and egalitarian community model that was the exclusive domain of internet technologists towards multi-stakeholderism helped deal with China, the informant says:

> 'You go to China, and you go to a Chinese official, and you say we represent a community organisation and they're going to go: we don't care, goodbye. But if you come in and you say, well, we're a multi-stakeholder, you know, a big organisation and we want to hear your view as the Chinese government then you're gonna get a lot more attention and you're going to make a lot more headway.' (D)

This is a very different view from histories of internet governance, discussed in some detail in Chapter 2, which consider multi-stakeholderism the apex of inclusion and democratic control. In its official communication, the United Nations for instance characterises multi-stakeholderism as follows: ‘the multistakeholder governance framework is informed by three components: a) opened-ended unleashed innovation (infrastructure), b) decentralized governance institutions (governance) and, c) open and inclusive processes (human)’ (UNODC 2016). This makes the internet ‘open, distributed, interconnected, and transnational’; an approach that ‘has grown from the Internet’s own DNA and is what allows it to thrive’ (ibid.). Respondent D however points to a more colourful history that is marked by political manoeuvring and strategic concerns throughout.

The respondents align in their views that China has managed to extend significantly its influence over internet standardisation bodies. Informant E finds that the issue is intensifying: the struggle over future internet standards is on.

> ‘I guess we should also talk about institutional fragmentation. I think it’s not too far-fetched to say that right now we have a preference for certain institutions so political interests can play out on different levels. And for sure, we have now seen that particular actors, and they are not just state actors, prefer certain venues for, you know vocalising their concerns, or simply for bringing forward their positions.
>
> There are countries that never engaged with certain fora and there are others that are present everywhere and trying to push for the same point, the same way they’d accomplished to come up with their own multi-stakeholder forum to discuss these issues. So institutionally, there is no harmonisation of initiatives. *We’re really in the middle of*

> *a fight to occupy this space and have as many supporters on one side as possible.*' (E, emphasis added)

In particular China's increasingly assertive display of norm-leveraging has contributed to the *securitisation* of internet governance (the concept of 'securitisation' is introduced in Chapter 2). Respondent F argues:

> 'I think it is important to understand the real Chinese environment around this, where it is. *It is a very military driven process.* We see that in the United States as well. It's very different in Europe in a way, but it is all part of technical nationalism, and techno nationalism is something that has just been very present in China since the Mao days. *It's the idea that through technology and through mastering it you actually gain the power not only to control your own citizens but also to control your space in the world. And by not being autonomous in that area you have dependencies that are more problematic than other dependencies that exist* [...] anything that relates to semiconductors, or to telecommunications technology or AI developments, I think [mistrust] will be even greater. There are barriers coming up on each side.' (F, emphasis added)

Both respondents provide evidence that struggles over the governance model for the internet are intensifying. Military planning and strategy gain more weight–it could be too quick to dismiss 'old-fashioned military cryptographers', as GCHQ does. Spaces for collaboration and compromise seem to be diminishing.

Informants suggest that the Chinese government is increasingly assertive in seeking to shape the internet of the future. Parallel to this, the influence of large technology corporations, big tech, is also on the rise. Corporate influencing of this kind is of special concern to the respondent at the internet standardisation body. In their view, the multi-stakeholder model, usually celebrated for its inclusivity and democratic principles, was already a move away from a truly community-based governance model in that 'multi-stakeholderism' has proved much more accommodating not just for China but for big tech also. For the informant, multi-stakeholderism in itself was already shaped by large companies and skewed towards their preferences.

> '[Back then] there just wasn't this concept that there would be somebody like Facebook, that would dominate the world of social media, or Google, that would dominate the world of search and social media, by the way, or Amazon that would dominate retail [...] there was no concept of that, the concept was, you would have some little guy in Greenland who hand-carved whale tails at a local rock, and he was able to sell those on the internet, equally with the people from Amazon, right, that was the general concept.
>
> Yeah, and I think *when the Internet Society kind of caved as it were, to the what they call the multi-stakeholder model, where they started saying, oh no, it's never really going to be that way, what's really going to happen is we have these huge stakeholders, and we've got to be bilateral among these stakeholders, and the Internet Society kind of lost its mojo at that point.* And it's been very difficult for them [...] and I know why they did it, they did it because they were struggling to talk to governments, right, again, I totally get it.' (D, emphasis added)

This response underlines just how much state actors matter, and always have, even if their influence is somewhat hidden behind a multi-stakeholder approach. The evidence here supports the particular perspective on securitisation adopted in Chapter 2: while internet governance is certainly not just about state actors, they remain the most critical actor due to their reach and bargaining power.

Throughout the conversation, D reiterated how multi-stakeholderism, for them, is simply short for accommodating US big tech. Informant F draws attention to the fact that US corporate power however is not just a problem for Western democracies but for authoritarian regimes as well–China has its own reasons why it would object to Amazon and Meta enjoying undue influence over internet governance fora.

> ‘The interesting thing is that it always becomes particularly problematic for us when the Chinese identify a problem and there's actually a genuine problem and their proposal is different from the one that we would like for it. So that's a lot of what is happening right now in terms of the "red reforms" that are taking place on the Chinese side as well. If you look at big technology companies and big platforms etc, they present an alternative source of power. We from a democratic angle say that's hugely problematic if Facebook has that much power, because that is something that challenges our democratic structures.
>
> *The fact is though that obviously it challenges the authoritarian structures just as much, so the impact on our power structures is something that is a deep concern to the Chinese Communist Party. So the objective is regulating big tech because they challenge the way we govern ourselves.* That's a similar objective in our society and in the Chinese society, they just come at it from very different angles, and that's

> always problematic for us.' (F, emphasis added)

When civil society groups in the West protest that Meta and Google have too much power, the Chinese leadership would certainly agree. However, their reasoning and objective is a very different one. A complexification of Western power structures regarding the internet of the future means a larger, and more diverse and complicated, set of actors that China has to reckon with, and would be forced to try and dominate. China's interest in reining in on US big tech is that better regulation and control would shift back loci of power to US state officials that China may find easier to deal with. This is an area it has experience with; the erratic behaviours of eccentric big tech billionaires could prove much more difficult for China to factor into policy-making–better the devil you know. Besides, the fewer actors it has to handle the more effectively China can influence internet governance models in the years to come.

Respondent E has a wealth of experience working at UN bodies where such dynamics play out. They echo the above points and talk in more detail about the complex relationships between corporations and state officials at standardisation bodies as well as tech entrepreneurs that try to influence both.

> 'They [private and public interests] operate in parallel. I mean, obviously we've seen initiatives coming from many non-state actors bidding for generally formalising their own norms. We've seen that a lot from non-state actors and maybe they even got more visibility than state actors do but there's a parallel move among states too, there's a little bit of competition, obviously, but there's a parallel move as well to be an entrepreneurial state [...] *Individuals play a role because you might have these influential people that go from one sector to the other, you*

> *know, go through all the chaos and achieve what they want to achieve, independent of public or private sector affiliation.*' (E, emphasis added)

Informant E makes this point to emphasise just how important it is to have smart officials in place who know how to play the game well. Standards don't really 'appear' as such but are the outcome of significant wrangling over oftentimes very detailed issues. Actors with experience in both public and private sector roles are particularly well equipped to shape internet standards. Relationships are multi-directional; state actors seek to influence entrepreneurs and representatives from big tech and vice versa. This is true for both China and the US.

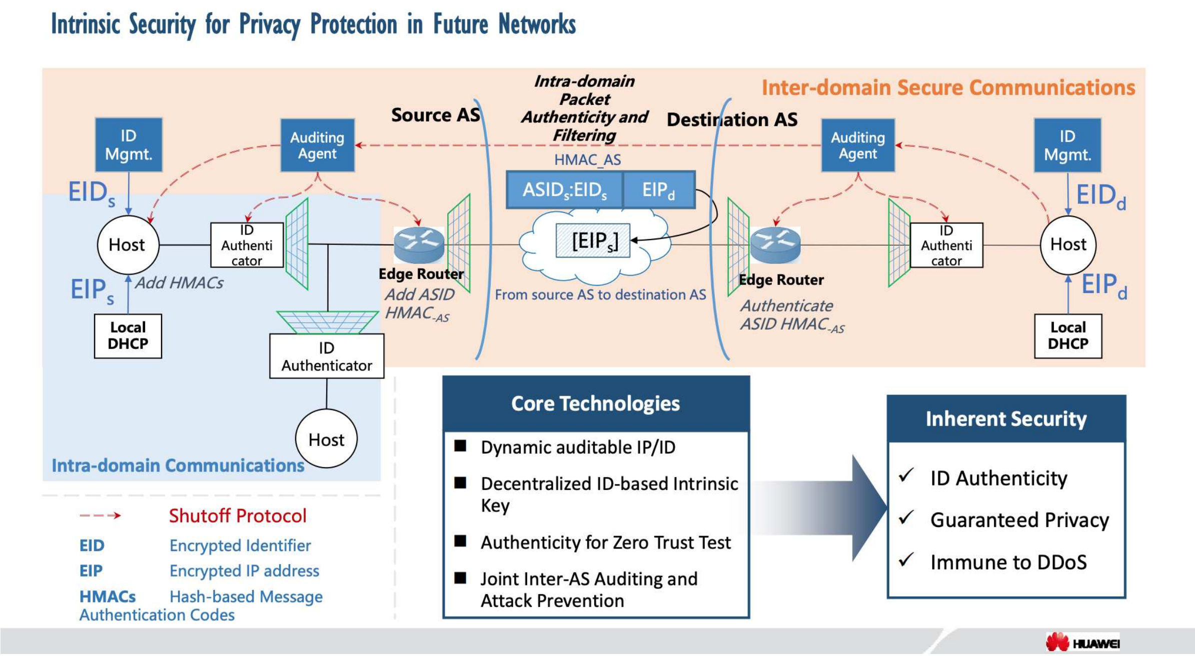
> 'Everyone kind of aspires to coming up with a global solution or a global technology that would then take over, which obviously would mean from the state perspective, a lot more control at the global level. It's a little bit what China is trying to do right now. *It's not only about developing the technology or controlling it within its own borders but about projecting that power globally and even getting the trust of the global community around certain matters.*
>
> It's not easy to do that, obviously, and it takes both entrepreneurship and, yeah, a lot of public support to get there. So I see this happening in parallel, obviously, states can also act via proxies and they do that a lot. Whether it's the US, having the big companies, lobbying very hard for things to happen or not to happen. We can say with China it's either the state, pushing for a set of things to be implemented by the private sector, or even the other way around. *Globally we have some very successful private entrepreneurs, influencing state behaviour.*' (E, emphasis added)

In internet governance games, there is a complex mix of interests, a lot of cross-influencing and acting via proxies. The findings presented in this chapter very much align with the view argued for in Chapter 2, i.e. the position that a focus on state actors is not to deny the paramount role of other agents that operate more or less transparently. Rather, state actors differ in term of the degrees of freedom they enjoy. True, their position will be shaped by corporate (and civil society) interests. Yet their position remains special since, ultimately, they are the actors that ratify changes at a level that is enforceable. It is worth noting just how often the notion of 'trust' would surface in conversations about China's aim and objectives. The leadership seems keen to present an internet technology that is trusted at home and abroad. However, if the fallout of 'New IP' is anything to go by, this will prove an uphill struggle for China.

5.1.4 'New IP'

The current debate over 'New IP' illustrates the above points regarding the increasing complexification and blending of corporate and state interests. Huawei has been pushing for its 'New IP' model, more a general outline of ideas rather than a workable proposal, which ultimately seeks to update internet protocols so that they better accommodate IoT requirements. Since late 2019, in several rounds of presentations at the ITU, then headed by Secretary-General Houlin Zhao, representatives of Huawei, China Mobile, China Unicom, and the China Ministry of Industry and Information Technology have been proposing to do away with TCP/IP. Similar presentations were made at other bodies (Durand 2020).

'New IP' covers a range of proposals to variable levels of maturity, most notably the idea of 'Many Nets' that would replace a unified internet architecture with a large number of subnets connected over gateways so that they could be managed more effectively–or switched off if and when required. Lin Han and Sheng Jiang of Fururewei, a subsidiary of Huawei, describe this network model as one that comes with 'intrinsic security', and introduces a new 'contract' layer for ID identification, among many other features.



Intrinsic Security for Privacy Protection in Future Networks

Shutoff Protocol

EID	Encrypted Identifier
EIP	Encrypted IP address
HMACs	Hash-based Message Authentication Codes

Core Technologies

- Dynamic auditable IP/ID
- Decentralized ID-based Intrinsic Key
- Authenticity for Zero Trust Test
- Joint Inter-AS Auditing and Attack Prevention

Inherent Security

✓ ID Authenticity
✓ Guaranteed Privacy
✓ Immune to DDoS

HUAWEI

Figure 5.1: Slide from Huawei's ITU presentation on 'New IP'.
Source: (Jiang 2019, 17).

The exact specifications are not entirely clear at the time of writing. Proponents of 'New IP' argue that 'intrinsic security' features of this sort are indispensable for the further development of autonomous vehicles and many applications in the IoT-domain (Han 2020). Experts at the Internet Society however call the proposals 'concerning' (Sharp & Kolkman 2020). And the Chief Technology Officer at ICANN writes:

> 'At a high level, New IP architecture introduces variable length ad-

> dresses; reintroduces circuit-switched-like principles in what is dubbed "better than best effort networking"; suggests an approach to enable packets to embed contracts to be enforced by intermediary network elements in a way that is reminiscent of active networks where packets contain code to be executed by routers and switches; and presents the concept of "ManyNets" where instead of a single network, the Internet would become a patchwork of networks loosely interconnected via gateways.
>
> New IP advances the idea of a strong regulatory binding between an IP address and a user. If deployed, such techniques could make pervasive monitoring much easier because it would allow any intermediary element (router, switch, and so on) to have full access to exactly which user is doing what. Similarly, content providers would have access to the identity of every user connecting to them. This could dramatically increase the oversight of published content' (Durand 2020, p. 3).

Respondent D is heavily involved in institutional debates over 'New IP'. D considers 'New IP' an existential threat to the internet as it is today.

> 'So I'm actually within a little group of people who have been trying to stop 'New IP'; we've had conversations with high level diplomats in London, Washington and in Canada [...] We are trying to inform them about this and there's actually a white paper that's not public, and a presentation that's not public, that have been written on this topic, but essentially the biggest danger that I see in 'New IP' is to the internet itself.

> ‘New IP’ would add to complexity from the lower levels up which makes everything more, much more difficult to manage. You’d have, basically, a kind of competition between the two transport protocols stacks. Which one should I use, and why should I use it? And so it adds complexity. And it also threatens a bifurcation in the network, certain nodes won’t be able to talk to other nodes any longer.’ (D)

In response to the question, what would be the point of ‘New IP’ anyway, the informant at the internet standardisation body finds it difficult to identify real value in ‘New IP’. They find a ‘technical’ and a ‘political’ dimension to the new protocol advanced by Huawei. While the respondent was happy to explain why ‘New IP’ would not deliver much in terms of technical innovation, they were extremely reluctant to address the political dimension at all.

> ‘Well there are two things going on, there’s a political thing going on there, as always. And then there’s a technical thing going on. *The technical thing is that a lot of the old line telco guys are still around and are still fussing because they cannot charge packet by packet based on quality of service, and they want to be able to charge on that stuff.* And there are other people who are saying, well, you can’t do real time over IP, and we need real time networks.
>
> Well, some of their examples, all the examples I’ve seen actually are pretty silly [...] There are other things that they talked about with sensor networks and factories and stuff. But a lot of that can also be solved with current IP anyway: with protocols on top of current IP. So that’s kind of the technology side of things that they’re getting at. *The political thing is, hmm I don’t know if I should tell you this.*’ (D,

> emphasis added)

Critical reviewers of 'New IP' such as Respondent D consider the proposals primarily a technology for realising profits based on discriminatory packet charging. This would be the first step towards a dual-lane internet; a fast lane for premium customers that pay premium prices, and a retail lane for everyone else where speed and connectivity drop. As far as the political dimensions to this proposal are concerned, it must be assumed that themes around surveillance and control are not entirely unrelated to what informant D says they cannot reveal.

For informant F, the problem is that the West is not in a particularly strong position to offer an alternative to 'New IP'. With rapid advancements in autonomous systems design, wearables and IoT applications more generally, the narrative of 'old' internet protocols and infrastructures that are not 'future-proof' or 'fit for purpose' will be increasingly difficult to reject.

> 'New IP, I think the other issue here is, we're probably running into a situation where the structures that we have created around the internet or how it was built are running into limitations at a certain stage and we will have to rethink them. But if we rethink them, do we want China to rethink them, or do we like to do it ourselves?
>
> That's the fundamental problem that we have with China at the moment, it's that all of the structures that we have created are fundamentally not running well. Be it government, including our democracy now, including saying our economy isn't going so well. We couldn't handle the pandemic super well. *And we keep standing there and waving the flag and saying, but we are democratic and it's great. And it's*

> *not in the end helping us so much.*' (D, emphasis added)

On this view, much more must be done to counter China, in particular with a view to their 'Standards 2035' agenda. The last quotation illustrates well how the future of internet architectures and system design is about so much more than technical specifications. It is fundamentally a competition of political systems engaged in a signalling game: which one is more agile and better equipped to deliver the technologies for the future? As far as respondent F is concerned, the West rests too much on its laurels. Ultimately, the struggle over IP is also a struggle over values and ideas of what makes a good society.

5.2 Governance futures: the quantum internet

In light of the discussion above, what is next for internet governance? Respondent E does not see much room for future collaboration. The US and China are at loggerheads.

> 'So how do you deal with the fact that the Chinese come forward with a solution like 'New IP' and don't, you know, push it away and say, no, that's silly because you're an authoritarian state and you can't have these ideas, but rather to admit, we have a problem here, we may need a solution, and trying to get that to a technical conversation.
>
> I would say under the current geostrategic circumstances that's impossible. And that's an important lesson I think for everyone who works in your field, is that there are sensible technological solutions for a lot of this, that you could agree on and you could find rules, and that you

> could then, you know, abide by. *But on the US side there's a huge level of distrust and it's very ideologically laden, and on the Chinese side, there's an enormous level of mistrust and there is absolutely zero willingness to adhere to rules.* They're more like an actor that says, I may apply these rules, or I may not. And so that makes technical solutions to technical problems really problematic.' (F, emphasis added)

The implicit case for an interdisciplinary programme such as Web Science aside, one that aims higher than finding technical solutions to technical problems only, informant F finds an increasing unwillingness among Chinese officials to abide by rules. This is certainly a headache for standardisation bodies–what to do if a powerful actor is unwilling to stick to the rules of the game? However it would be unfair to single out China in this context. The Trump administration had made it their hallmark to not stick to established ways of doing things. Either way, the evidence presented so far does not bode well for an inclusory and transparent multi-stakeholder model of internet governance. For respondent G, quantum technologies are likely to amplify the issue of US-Chinese competition.

> 'Quantum would probably complicate things greatly, although widespread applications of that to networking are so far away we are being purely speculative here [...] But the short answer is that the problem and direction of internet governance are pretty much going to be set by the US-China rivalry, with a dash of Europe thrown in.' (G)

Technology can generate some normative pull out of this gridlock. Quantum internet technologies may help set technological facts that shape standards and governance models that follow. Such a perspective helps explain the current patenting frenzy of internet technologies. If the future of internet governance is up for grabs, there is genuine normative power in technology. Respondent E considers this a self-perpetuating dynamic that is the product of the success of the internet itself.

> ‘Much of this [patenting activity] comes from the history of the internet, you know, after two decades it became the global network for communication. The fact that it was commercialised immediately actually meant to let go of its initial creations, kind of, well, let universities have it and then five years later, no actually let the whole world have it and build companies around this.
>
> So I think that’s the model that people have in mind when they think about future technologies. Nobody thinks, oh, AI should be actually, you know, under strict military control, nobody thinks that. But the perspective is always, there’s going to be private sector dominance, which, again, some countries are challenging. I mean, not everybody’s necessarily in agreement over this.’ (E)

A Chinese leadership position in quantum communication, whether or not it meets all requirements for encryption that intelligence services such as GCHQ demand, promise the opportunity to set de facto standards. If China continues offering proposals for internet reform that respond to genuine issues, it will be difficult to keep saying no. ‘New IP’ need not be perfect, as it is sufficient for China to signal that they are a serious player that has practical solutions to offer. Over time, actors, both public and private, will want to listen.

The official at the UK Cabinet Office expresses concern in particular about protecting British intellectual property amidst the scramble for the internet of tomorrow.

> ‘There is a sort of general consensus that we need to be wary of China but also other countries possibly as well. It’s not necessarily about China in particular but more around making sure that we need to protect the UK’s intellectual property, particularly with quantum. A number of UK-based university spin-outs are doing some really great research so it’s more about protecting these assets and IPR, this might end up being the focus for us.’ (B)

It seems the UK government worries to get locked into a governance conflict that yields them no advantage. The official continues:

> ‘We can’t say we’re banning all foreign investment from hostile state X because we don’t want it and we’re scared about it when in actual fact this would leave the UK behind in terms of progressing with technology X because we’re not getting any investment from certain countries so I think we’re definitely aware of the balance here but we just have to make sure that everyone else is too.’ (B)

For GCHQ too, the quantum threat is about economic growth.

> ‘It would be a security concern to the UK if China had a large-scale working quantum computer well ahead of the West. The direct security threat is if you can factor these numbers or, or do some data science, AI, or modelling chemicals and material science, you could potentially do things the West couldn’t.
>
> So that’s in some sense a direct security threat if they can do things

> we can't, but more to the point, it's an economic threat as much as it's a security threat because they would attract a lot of investment and sales and all that. So trying to get ahead of the West would be a concern [...] if you balance that direct threat of what they might be able to do with economic and technology developments, you might have a problem.' (C).

The quantum internet emerges as a dual threat. It may provide an adversary with new capabilities for surveillance and espionage, as well as R &D, but also a lucrative source for attracting foreign investment and commerce, and thus contributing to economic power in the long run. The Cabinet Office official is mindful that the UK's resources and reach are limited–Britain would not be able to sustain a more aggressive stance of the kind the US is pursuing.

> 'We'll have to remember that the US have a lot more people, and a lot more money than we do and are probably able to keep things in-house where we can possibly not. So that's one of the key differences' (B).

Effectively, the UK is much more dependant on international coordination than the US. The same is true for countries in Europe. Such dependencies make for delicate Western alliances; they create the potential for disagreement that China can capitalise on.

With US-Chinese competition in full force, new internet technologies, in particular AI and quantum technologies, emerge as the figurative ace up the sleeve that promises ultimate advantage to end the gridlock, and win. With this mind, what are the respondents views on a quantum internet that connects classical and quantum computers over QKD? The respondent in Singapore attests to great excitement in the field.

> ‘I have colleagues who actually were so convinced by [quantum technologies] they left the university and now build quantum software. I am really excited for them because honestly, what’s happening this time, there is genuine momentum now.’ (A)

However, there are considerable obstacles to overcome. Respondent A smiles at what he calls the ‘naivety’ of the discussion around QKD. He agrees that in principle, QKD is secured by the laws of physics.

> ‘It’s very difficult to say what the interplay between cyber and quantum for the quantum internet is going to be. I think no matter what happens, I think we’re never going to get away from the need for cyber protection over classical channels. And cyber warfare is always going to be there [...] You see, the thing is, on paper, everything is secure. But they’re always physical threats, such you have to be aware of what your physical side channels are and understand why they can be a problem.
>
> So just thinking of how would you stop a man in the middle, intercepting your quantum message and manipulating it is very naive. Yes, perhaps, we can assume that within the box, it’s all completely secure. But what matters is what goes in and out of the box. What happens if someone is looking over your shoulder? What is appearing on the screen? That’s why I say no matter what you do, we still need [classical] cyber nets to make sure no one is looking over your shoulder’ (A).

In this view, the quantum internet is unlikely to ever fully replace the internet we have today. QKD requires classical communication channels (also see Chapter 4), which makes digital encryption anything but obsolete. If anything, the quantum internet will make the internet more complex to manage.

For GCHQ, the quantum internet is still many years away. Here too complexity surfaces as a major issue.

> ‘Now, the great thing about the internet and the mobile phones that we have now is that they pretty much always work because if you’re calling your friends in Beijing, and a bit of the network goes down in Scandinavia, you will know because you’ll just be routed around some other parts of the world to be able to talk to your friends.
>
> If you rely on one of these networks with fixed structural nodes [i.e. quantum repeaters] in the middle, that can be broken and will degrade over time so it will need to be maintained at someone’s expense. So that’s the problem. The maximum length I think they can go at the moment without some sort of repeater is 126 kilometres. It’s about that. So a long-distance network that they’ll be having in China will have literally hundreds of these things in between that will need to be secured, literally a building with a locked room or something like that. In China they can certainly do that but it’s harder here [laughs].
>
> What they’re trying to do in space, it’s from the ground to a satellite that rotates around the earth. And when it goes to China it beams something down there. I don’t actually know the exact detail of what they are proposing. But who will really want to sit there and wait for

> three hours to get a text over to China with all the cosmic rays going around and all that?' (C)

Most technologies turn out quite differently than intended so it remains to be seen if GCHQ are not indeed in for a surprise. China considers its *Micius* satellite a proof of concept, certainly not yet a workable technology. A future Chinese satellite communication system that is impenetrable to Western intelligence services would surely be a cause of concern.

The repercussions of a quantum internet reach well beyond US-Chinese competition. For informant D at the internet standardisation body, the quantum internet may increase economic concentration in a market that is already dominated by a small number of players. Quantum internet technologies may accelerate massive data harvesting by large companies such as Amazon that offer cloud services. According to the informant, small to mid-sized companies that find it too difficult to get their own intranet up and running are too quick to upload all their data onto the cloud. The issue will become even bigger as the quantum internet will add new capabilities for cloud storage, AI/ML, and corporate services.

> 'Running a network has become so complex that it takes very, very specialised people to run a network and a lot of smaller companies struggle and even midsize companies struggle to hire people that can do that work, so it's easier for them to throw it at the cloud, although that doesn't solve the problem [...]
>
> Now, the downside is [...] the more information you have about someone, the more you know about that person. The more you know about them, the more you continue their experience to keep them captivated

> and online. And the more they're online, the more you know about them [...] How many years did it take for Amazon after Netflix had pushed out their data and all their streaming to Amazon servers to come out with Amazon's own video service? How did they learn to build that video service?' (D)

So a quantum internet, a new internet hybrid, would make for a much more complex network that will require an ever more specialised and highly-skilled engineering workforce to build, maintain and integrate. This is likely to benefit established corporate giants that have the resources to train and retain such talent. On this reading, the quantum internet is bad news for competition and smaller businesses. Above all, the quantum internet cements dependencies on critical internet infrastructures, D finds.

> 'What's happening is as 80 percent of the traffic has gone from being scattered to being Amazon, Facebook, Google, Microsoft, whatever, all the physical infrastructure is being built to those companies [...] Facebook is just putting in a new undersea fibre cable, and Google owns tons of them, and you think wow, so now the physical infrastructure is built towards them.
>
> If I'm a small or medium sized company and I want to get fibre between here and London, how do I do that? Microsoft will let you use their fibre, as long as you're using Microsoft Cloud servers. *So now they have you kind of locked into the backend and things start getting really dicey at that point as to how you get out of it.*' (D, emphasis added)

So for internet regulators and governance champions in the West the quantum internet presents a double whammy. It may increase the power of big tech at home. On top of that, it may give a strategic rival a considerable economic advantage, perhaps to the extent that suboptimal governance models become difficult to reject. As it stands, China seems to have a bigger interest in realising the quantum internet than the West. The reason for this could be to find a technology that breaks the dominance of US corporations.

With the 'internet in everything' (DeNardis 2020) today, our very understanding of the object of internet governance begins to shift, respondent E argues. Given that all parts of life have become entangled with internet activity, it makes no longer sense to separate internet, or digital, forms of governance from other areas of regulation. Internet governance is likely to evolve considerably and blend with other regulatory domains.

> 'In five or ten years' time, I think we're still going to talk about global governance. Exactly what type of technology governance will have to be in place remains to be seen. The way it's going is that technology is integrated in other forms of governance so we'll have a digital aspect to all types of governance, whether it's health, or the digital part of every other form of governance we have.
>
> It doesn't necessarily make sense to have it separated out the way we have it right now that we just discussed, like internet issues on one side and development concerns, for example, on the other. Everything is on the table, just with a technology twist. I think it would make much more sense that technology is the technology part and the digital bit is a subset of those bigger domains.

> *It makes much more sense, rather than say we need laws and norms and regulations specific to the internet, we can say well let's see what the role of the digital world is right now and how that plays out in everything else we're doing and regulate that as part of the sector itself rather than as a separate thing so I don't know if we're going to have internet governance proper in the near future or we might just have more global governance with a subset of issues.*' (E, emphasis added)

Should this trend materialise in shifts of this kind, the stakes of a quantum internet become even higher. It is no longer about infrastructural control over a key network technology but arguably the ultimate promise is leverage over any form of interaction that has a digital flipside to it–i.e., pretty much everything. Such a development would provide China with an even bigger and richer opportunity to shape Western policy. Respondent E gives an example in the domain of labour regulation.

> 'I can give you a very practical example here in Geneva, again for a long time I was following the work of the UN and they have struggled with this very issue, you know, when they put these concerns on the UN agenda, well these issues hadn't been around at the time of the creation of the institution, obviously. Everybody's trying to do something on digital because it's so relevant right now, but it's so difficult to find the right place for it and just having a dedicated venue is impossible.
>
> So in the end, the truth is, most of the organisations that have engaged on the entire issue have done that within their own mandate. If it's the International Labour Organization, they now work on digital conditions of work, they work on what they call the Future of Work

> Agenda. So it's all about what happens if your employees are connecting remotely. What happens if your employer can actually control the communication, if they get access to your data and can see what you're doing. Can they ask you to connect after work hours, all of these issues that obviously weren't there when the organisation was set up are now part of the conversation, and it makes sense that they're now part of that mandate, rather than saying well everything you do will be discussed in a different forum in a different place, and then countries should bring all the conversations to that place.
>
> Now it makes more sense that you would bring the concerns to the labour organisations if they were labour related and that you bring them to the trade organisations if they are trade related. Because at the end of the day, digital is just a small part of our bigger world. Obviously it's becoming a more important part, but it's not around digital that we should reorganise existing governance instruments, I say it should be the other way around.' (E)

This trend, potentially amplified and exacerbated by quantum internet technologies, would amount to the further diffusion of responsibilities for internet governance. Rather than overseen by a defined set of bodies, the internet of the future would be shaped by any organisation that recognises the internet as an influential factor in their mandate. In a way, such a move would mean a considerable extension of 'multi-stakeholderism'. It would surely make it much more difficult for a single state actor, either China or the US, to dominate the internet governance discourse. On the other hand, it provides economies of scale for state actors that do manage to shape the governance model for the quantum internet.

This trend however works against considerable drives towards increased fragmentation, informant E continues.

> ‘Generally, we can probably distinguish between a few forms of fragmentation. We’re seeing to a certain extent a technical issue. To start with, let’s look at the infrastructure we have seen now for a couple of years, attempts to develop national systems, and the case with China is probably the most prominent of them. But it’s also the case with Russia where they’re probably just a few steps away from disconnecting from the global Internet. And of course we see Iran taking more measures to control the system.
>
> So there is a technical fragmentation that is happening now. It’s not necessarily what we are reading in the media, because we’re reading about a complete disconnect and so on. In practice, all of these systems are interoperable to a certain extent, there’s a decision as to where you want to connect them, but the Chinese are not completely outside the global internet the same way the Russians aren’t either. So, some things could be controlled more on a national level and that is the case for sure, especially for the big powers.
>
> Then there is also political fragmentation. We have lots of diverting initiatives at the moment if you think about the regulatory space; we definitely see that countries have come up with regulations that are not necessarily compatible at either the legal or global level. So in that sense, *we’re just seeing reflections of the geopolitical tensions translated into law.*’ (E, emphasis added)

For internet governance in the 2020s, the above discussion suggests two central themes that coalesce around the quantum internet. Firstly, fragmentation is likely to accelerate. However, it is important to note that fragmentation is not a binary question of a 'free internet' vs 'global disconnect'; the question is not if global players flip an on/off switch. The much more complex and nuanced question is one of what may be called *selective connectivity*; a governance principle that reflects the political needs of the ruling powers of that state. A Chinese quantum internet would be an example of such a powerful subnet that connects to the internet but can be separated from it. If so, governance principles are likely to become more state-centred, specific and targeted.

However parallel to this trend towards selectivity the very scope of internet governance is likely to widen. Virtually any matter that requires international coordination and regulation has a digital dimension to it, which makes internet governance an increasingly powerful tool to shape the international system. China seems to have recognised this well before the West did. Over the coming years, the struggle for dominance in the internet governance domain will only intensify.

5.3 Taking stock

If the quantum internet is not going to replace the internet but make it a much more powerful version of itself, then it would make sense why China should want to shape the internet governance model and its institutions to the degree witnessed presently. In light of Chinese efforts, respondent F urges Western allies to rethink their approach to internet governance.

> 'So we have to come up with, in particular in international relations and

> international standards bodies, a better and more convincing story [...] for example we do like telecommunication standardisation processes that are industry-led, that has always worked really well. And now you have a strategic approach from the Chinese side who say, okay, so if this is voting by numbers, and this is industry-led, so if we just bring more people to the table we can vote more, right?
>
> *China is playing the system, it's understanding exactly how the system works and then twisting it into that direction that suits their preferences, and that's the thing, it doesn't always lead to completely silly outcomes.* So if you look at cybersecurity regulation in China, obviously this is a big problem, but some of the tools that they have are impressive, in particular [...] regarding some of the methods they have employed to make transactions over the internet more secure, particularly because the level of trust is so low in China and the level of trust in the system is so low, and the level of trust and companies is so low.' (F, emphasis added)

The issue of trust is a constant one in conversations about China. There is little to suggest that Western quantum internet technologies could provide China with any assurances in this regard. In the intensifying emerging technology race, Europe in particular seems in hot water. The European Commission has been busy advocating for 'technological sovereignty' on many occasions, as outlined in Chapter 2. This would suggest a concerted policy effort towards infrastructural independence from the US and China. In reality, however, this is not really happening, as informant E points out. The same point can be made about the UK.

> 'Now the reality is, most of our communication [in Europe] relies on this

> [US and Chinese] legacy infrastructure. It's a rough estimate but we can probably say there's some 60% American, 30% Chinese and then some European companies in there as well. So that's the status quo, we have these legacy systems that are only likely to become stronger foundations for what we are building right now, I don't think they will go away and I don't think they will be replaced anytime soon.
>
> Yes, we have some sort of changes but change is really limited with regards to basic infrastructure. We've seen this again with the 5G debate, the Chinese have not been traditional players in this space, but they are becoming traditional players, for the last decade for sure now that they've been part of many more systems, especially in developing countries. So at that level we won't have technological independence or autonomy or sovereignty, there's simply no way.' (E)

Therefore, in many ways, the future of the internet, in particular when it goes quantum, is one of US and Chinese competition. Europe, and arguably the UK, do not really play a significant role in this game. This fact is not helped by what the UK Cabinet Office informant considers a significant lack of deep understanding among officials.

> 'So one of the challenges we've seen, in particular with the quantum tech side of things, is that people across Government, seniors and ministers don't understand these technologies [...] this means making a decision about something they don't understand and quite often this results in knee-jerk reactions to things [...]
>
> I think that's one of the key issues which is quite problematic: how

> can someone decide how to regulate or oversee something when they don't quite understand it?' (B)

It's a strategic disadvantage for Western liberal democracies that they are unable to plan ahead to the extent the Chinese leadership can, the informant continues:

> 'The third issue I would highlight is the fact that people tend to think in election cycles. Of course it's understandable; if I were a minister I wouldn't necessarily be thinking 10-15 years in advance when there may or may not be a quantum computer that may or may not be able to do certain things [laughs]' (B)

The trouble is, of course, that the UK and her allies face an adversary that very much thinks in those terms. Not all respondents are pessimistic about quantum technologies, however. Respondent A for instance views quantum network futures open-ended and indeterminate.

> 'I'm a scientist. I like to be precise. I'm not a futurist [but] the quantum internet is more than just distributed entanglement globally.' (A)

While it would be too early to say what the quantum internet will be exactly, and too early to be pessimistic about it, the analysis in this chapter demonstrates there should be significant concern about Chinese leverage in shaping future quantum realities. The respondents of this study find little ground for optimism that the current political tensions that reflect in internet governance would eventually benefit the West and China equally. As far as quantum communication technologies go, an important subfield of the emerging technology race, interview data suggests that China is ahead in the game.

5.4 Main points of Chapter 5

In summary fashion, the major takeaways of this chapter are:

US–Chinese rivalry and strategic competition

5.a China's strategic outlook has changed under President Xi. Informants suggest that China has come to consider the US its chief strategic rival. Blocks such as the European Union matter only little in China's strategy portfolio. Europe, and the UK, are only relevant insofar as they are targets for China to nurture disagreement between the US and its allies, which helps keep US planners and stategists preoccupied and busy.

5.b China has grown considerably more assertive in international relations. This is also due to domestic pressure. Since Chinese big tech companies have emerged as internal rivals to Party dominance, the Chinese leadership has responded by reining in on big tech. It considers the Party the principal 'data sovereign': no entity above the Party must hold vast amounts of data on the Chinese population.

5.c Opportunities to engage with China constructively on standards for emerging technologies, including quantum technologies, are 'near zero', as one participant puts it.

5.d China is concerned about the extent to which US big tech corporations shape US policy positions. Sitting at the top of a 'trust pyramid', the Chinese leadership is more comfortable in dealing with other state actors. Too much private sector involvement in the US makes it difficult for China to identify who the actual powerful actors are in the emerging technology race with the US.

5.e Deep mistrust on both sides presently makes it impossible to find technical solutions to internet governance issues that would be available in principle.

Security implications of a Chinese technology leadership

5.f GCHQ and the British government consider the direct security implications of Chinese QKD, and a Chinese quantum internet, manageable. They place their bets firmly on post-quantum cryptography and the many engineering challenges that quantum communication presently faces.

5.g Countries at the periphery of Chinese influence, such as Singapore, seem less relaxed: the quality of intelligence signals will drop when China moves to communicate internally over quantum channels.

5.h Conversations suggest that the British government and its intelligence services may underestimate the value of Chinese quantum internet technologies for signalling purposes. Chinese quantum advantage means considerable reputational gains for China at home and abroad, and may help Chine forge new alliances with unaligned countries at international institutions, notably internet standardisation bodies: a Chinese quantum technology stack, coupled with standards, translates into substantial bargaining power.

The quantum internet

5.i Trust is an important trope for the Chinese government. A Chinese quantum internet, built with Chinese quantum communication systems, is hoped to deliver a technology that unlike previous internet and computing stacks is wholly Chinese and therefore trustworthy in principle.

5.j A quantum internet will add an extra layer of quantum capabilities to the internet rather than replace it. This raises questions about integration and is a cause for concern should the internet effectively split into a 'quantum fast lane' (and priced as such) and a digital legacy lane for those who cannot afford to go quantum.

The future of internet governance

5.k Respondents align in their views that the governance model for the internet of the future will be largely shaped by US–Chinese competition; one interviewee at the United Nations speaks of an open conflict in internet governance at present.

5.l Europe and the UK will have little, if any, opportunity to shape the trajectory that internet governance and standards-finding is going to take.

5.m Respondents have mixed views about the 'multi-stakeholder model' for internet governance. One respondent says, contrary to how it is being portrayed, ‘multistakerholderism’ in practice has always meant bowing to pressure from big corporations and powerful governments.

5.n Internet governance as a single and separate entity is likely to dissolve and be absorbed by other regulatory domains so that internet policies will be handled in domain-specific fashion. For instance, labour organisations are likely to have a stronger mandate to regulate digital aspects of work.

5.o The US and its allies struggle to formulate a response when China offers solutions to actual technology gaps and problems yet the West believes it must reject them. Non-aligned countries will expect better than a default no to any Chinese proposal, even if Chinese ambition is not universally appreciated and shared.

5.p ‘New IP’ is a prime example of Chinese ambition. A signal of intent rather than a workable proposal, one respondent fears its implementation would mean the end to the open internet.

5.q The discussion about the ‘fragmentation’ of the internet is incomplete unless it also considers ‘institutional fragmentation’, which brings with it increasingly antagonistic views among the stakeholders that are involved with internet governance.

Chapter 6

Quantum patent data: descriptive statistics and ERGMs

The previous chapter has discussed the governance challenges of the internet of the future. In conversations with domain experts, it has found that the internet has come under pressure on various fronts. In terms of its architecture and protocols, China is pushing for a complete overhaul of the physical infrastructure of the internet so that it can deliver better the promises of the IoT and embed quantum capabilities–although, experts agree, the Chinese proposal, come to be known as 'New IP', seems to advance hardwiring new mechanisms for surveillance, control and discriminatory pricing into the IP and transport layers. Undoubtedly, the current 'multi-stakeholder' governance model has served US interests well over the past four decades. In light of a more assertive China, however, internet governance today has become an arena for US–Chinese competition that leaves little room for inclusory and participatory governance principles, the experts have found.

In early May of 2022, Dr Ian Levy, Technical Director of the UK's National Cyber

Security Centre, discussed the strategic and international security implications of advanced technologies at a public talk at RUSI, the defence and security think tank. He argued that the Western alliance does not do nearly enough in countering Chinese influence in the internet domain. Importantly, Dr Levy noted that Western powers struggle to present an alternative vision to Chinese ambition (Levy 2022)–the participants in this research project very much confirm this view, as has been discussed in the previous chapter: China is not wrong to diagnose a problem, such as issues of IP to accommodate 'real-time' connectivity for, say, autonomous vehicles. The West may not appreciate the solution China proposes but finds it difficult to arrive at an alternative plan. The issue has become even more pressing since China has announced bundling new emerging technology patents with appropriate standards: its 'China Standards 2035' plan was discussed in Chapter 2.

The nascency of quantum computing is one of the chief reasons why the study of patenting activity matters. For many observers, quantum computing has reached a level of development where R&D and deployment begin to shift from academia to the private sector–a sector that will want to secure property rights. 'At this point, many of the later-stage technical developments are protected via trade secrets or by patenting' (Parker et al. 2022, p. 3). The RAND Corporation observes, 'in the past few years, this shift has begun to occur with QIS [quantum information science], with many companies (both start-ups and established firms) beginning to work on quantum technology and file patents for their inventions' (ibid.). Patenting activity for quantum internet technologies, a subset of quantum technologies more generally, is picking up pace.

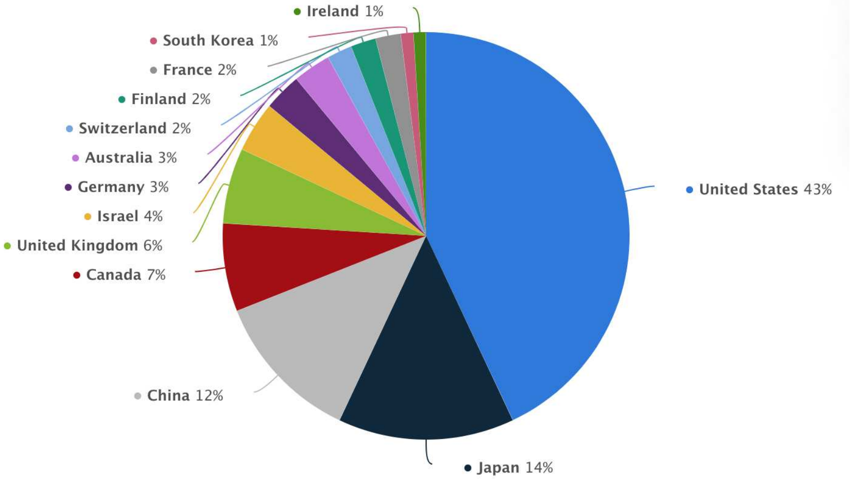


Figure 6.1: Country breakdown of leading 100 companies that filed quantum computing patent applications in 2020. Source: Statista.

The World Intellectual Property Organization (WIPO), an agency of the United Nations, which serves as the 'global forum for intellectual property (IP) services, policy, information and cooperation', defines patents as 'an exclusive right granted for an invention, which is a product or a process that provides, in general, a new way of doing something, or offers a new technical solution to a problem' (WIPO 2021). As argued in detail in the literature review and methodology chapters, patents are signals about the future trajectories novel technologies may take. As 'indicators of technological emergence [they] promise valuable intelligence' (Porter et al. 2019). As such, they have formed the empirical base for a great number of studies that forecast how innovation will diffuse and whom it will serve.

Over the past twenty years, patent registrations worldwide have increased sharply in number, which attests to the growing status of patents, both for governmental and corporate planning and management. As such, patent data provide insights into the diffusion and propagation of early technologies and prototypes that have not yet reached maturity. ‘Although there is more to invention than patenting, patents are primary indicators of invention, providing valuable technological and geographic detail’, the US National Science Foundation sums up the consensus in the literature (NSF 2020). Patent data in quantum computing and communication must be considered strong signals of possible technology futures. Chapter 3 has provided a detailed justification for considering patent data indicators of how the quantum internet is going to shape up.

With this positioning in mind, this chapter builds further empirical evidence of a technology leadership race between the US and China in the quantum internet domain. A technology leadership position would give either of the two superpowers considerable momentum in pushing for a reformed internet governance model that can advance the national interest. To this end, following the proposed mixed-method approach argued for in Chapter 3, the previous chapter has analysed qualitative interview data. This chapter, then, analyses sets of patent data to draw an empirically rounded and informed picture of the race to build the quantum internet.

The chapter is organised as follows. Section 6.1 presents details of the datasets that have been employed. Section 6.2 discusses descriptive statistics that attest to the structural differences, and similarities, between the Chinese and US quantum development programmes. The section finds strong evidence for the preferential treatment of domestic technologies, which suggests the parallel evolution of two quite separate and self-sustaining research programmes. Section 6.3 inquires in more detail into the dynamics that drive the Chinese and US quantum internet programmes, as it finds reflection in patenting activity. It develops and tests ERGMs for this purpose. Dividing quantum patenting activity into three separate time periods for both the Chinese and US cases for ease of comparison, the model finds that the country of patent filing, the type of registering organisation and the number of IPC codes that had been given for filing purposes are all strong predictors of strategic patenting activity in the quantum domain. Finally, section 6.4 concludes.

6.1 The quantum patent datasets

Chapter 3 has developed the research strategy for retrieving data from the EPO's proprietary Global Patent Index's databases. As a result of this strategy, the following datasets have been assembled. Searches were limited to patents registered since 2015 when the quantum race began to gather momentum (Giles 2019). Combined with keyword searches, the search retrieved the following sets of patent families.

Search	**Boolean search string**	**Number of** **patent records**
1	CPC = G06N10/00 and ABEN = “quantum*”	1,564
2	CPC = B82B and ABEN = “quantum*”	55
3	CPC = B82Y10/00 and ABEN = “quantum*”	483
4	CPC = G06E3/00 and ABEN = “quantum*”	3
5	CPC = H01L39/00 and ABEN = ”quantum*”	9
6	ABEN = ”qubit*” or ”qbit*”	541

Table 6.1: Numbers of records retrieved per CPC group and keywords for the domain of quantum computing.

where ABEN stands for ‘Abstract in English’. The union of these searches yielded 1,966 patent families in total.

The field of quantum communication is less neatly defined and incorporates several research traditions; the table below reflects this increase in scale. The search produced the following results.

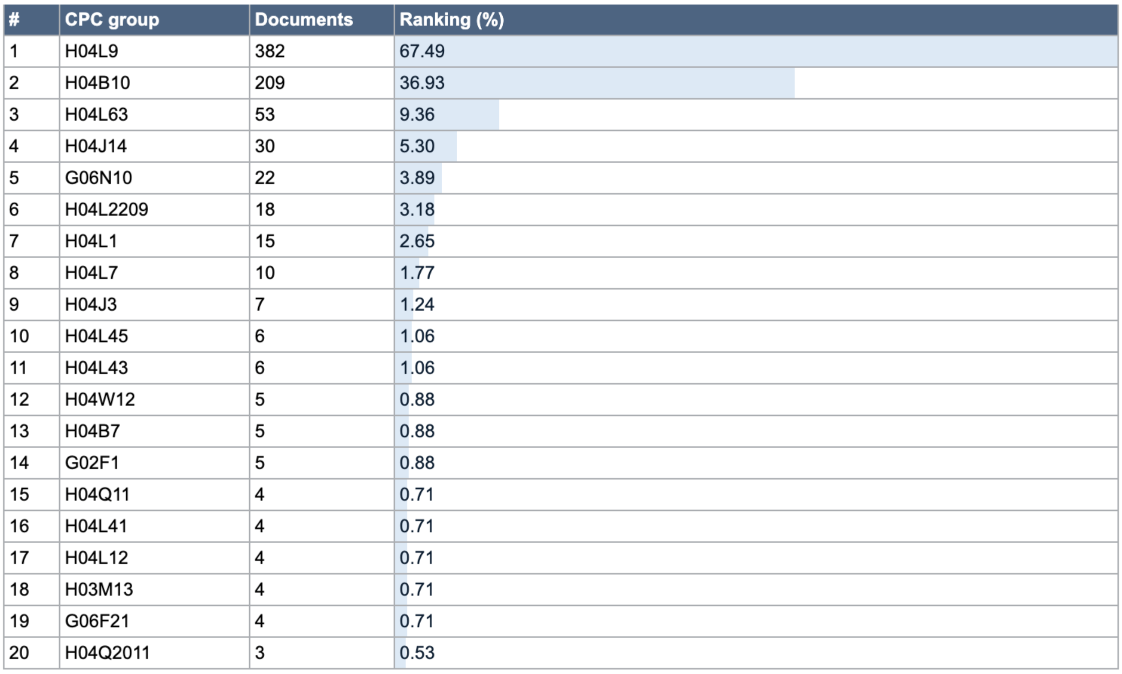
Search	Boolean search string	Number of patent records
1	CPC = B82Y20/00 and ABEN = ”quantum*”	2,126
2	CPC = H01L31/00 and ABEN = ”quantum*”	4
3	CPC = H04L 9/00 and ABEN = ”quantum*”	4
4	CPC = H01L 33/00 and ABEN = ”quantum*”	63
5	CPC = H04B 10/00 and ABEN = ”quantum*”	1
6	CPC = H04B10/70 and ABEN = ”quantum*”	831
7	CPC = H04W 12/00 and ABEN = ”quantum*”	1
8	CPC = G02F 1/00 and ABEN = ”quantum*”	4
9	CPC = H04J 7/00 and ABEN = ”quantum*”	1
10	ABEN = ”quantum comm*” OR ”quantum key*” OR ”QKD*” OR ”quantum channel*”	566

Table 6.2: Numbers of records retrieved per CPC group and keywords for the domain of quantum communication.

The union of the ten searches in the table above yielded 3,407 patent families. Now, the overall union of both searches, i) quantum computing and ii) quantum communication, produced 5,234 patent families in total.

The sets of patent records so retrieved were then checked manually for goodness of fit by reading through titles and abstracts. In preparation for this task, over a six-month period parallel to preparing earlier chapters, the author of this thesis had pursued two certified quantum computing and quantum communication degrees with the Massachusetts Institute of Technology. While removing false positives can be automated to an extent, a manual check proved more rigorous due to the left-field character of many outliers. This somewhat tedious process identified 1,043 false positives, i.e. patents that do not seem strictly relevant for building the quantum internet, such as, for example, patent applications for, curiously, a particular game-theoretical procedure. This means that the total number of patent family records retrieved in the search process, which are being used in the analysis below, was **4,191**.

To provide an illustrative example of the search and retrieval process, the figure below shows that about a third of all patent data that have been retrieved with the keyword search 'ABEN = "quantum comm*" OR ABEN = "quantum key*" OR ABEN = 'quantum channel*" AND APD>=2015' sit in the CPC group H04L9, 'Cryptographic mechanisms or cryptographic arrangements for secret or secure communication', pointing to the dominance of this classification subtree for registering entities. The graph below plots the 20 most popular subgroups for the classification of patents in the domain of quantum communication.



#	CPC group	Documents	Ranking (%)
1	H04L9	382	67.49
2	H04B10	209	36.93
3	H04L63	53	9.36
4	H04J14	30	5.30
5	G06N10	22	3.89
6	H04L2209	18	3.18
7	H04L1	15	2.65
8	H04L7	10	1.77
9	H04J3	7	1.24
10	H04L45	6	1.06
11	H04L43	6	1.06
12	H04W12	5	0.88
13	H04B7	5	0.88
14	G02F1	5	0.88
15	H04Q11	4	0.71
16	H04L41	4	0.71
17	H04L12	4	0.71
18	H03M13	4	0.71
19	G06F21	4	0.71
20	H04Q2011	3	0.53

Figure 6.2: Top 20 CPC subgroups following a keyword search for quantum communication.
Source: EPO GPI database.

The master results list that contains 4,191 records (and links to c10,000 other patent records outside the dataset, which the records in the set cite as prior art) was divided into 'US' and 'Chinese' datasets for the purposes of identifying structural characteristics and ERGM modelling. The question of what makes a particular patent a 'Chinese' or an 'American' one is by no means straightforward. Inventors who file patents can be residents of country X but file a patent in country Y and then seek to patent the innovation in countries A, B and C or globally (WO). A patent registered in China but registered by a foreign company is not necessarily a patent that fits the label 'Chinese' given that the foreign company has leverage over it, which is what matters for the purpose of this thesis. A Chinese company, on the other hand, may seek to register a patent with the US patent office, which gives the patent application a US country code, yet it would be more appropriate to say it is a ‘Chinese’ invention.

This chapter inquires into the ownership structure and, ultimately, the potential sway state actors enjoy over institutions that register quantum internet patents. ‘Leverage’, ‘sway’ and ‘influence’ are vague concepts, admittedly. Obviously, patent records and their citation links contain no classifier to their effect. In order to get a sense of the trajectories of government influence on how the quantum internet may shape up, an indicator of leverage had to be found.

To do this, it was decided that the decision criterion, what constitutes ownership of a patent and thus, ultimately, leverage over its technology, should be where the institution that has registered the patent is based. For multinational companies, this means headquartered. For instance, if the US arms manufacturer Northrop Grumman (headquartered in Falls Church, Virginia), registers a patent in the UK, this study does not consider it a UK patent but a US one. Hence in the following, a patent is Chinese/American if the registering institution is headquartered in China/the US.

It is assumed that a domestic organisation headquartered in country X has closer ties with the national government of X than with that of any other country, or would find it more difficult to escape its own government’s influence. While this may not be true for all cases it is a reasonable proxy to say the US government enjoys a more privileged relationship with Northrop Grumman than, say, the government of Finland does. This project makes no further assumptions regarding the exact quality of this relationship; it is merely to classify data so that patent data can be labelled either ‘US’ or ‘Chinese’ on reasonable grounds.

More than half of the records obtained from the EPO databases did not contain any country codes for filing purposes. This required the author to manually look up the geographic location of the headquarters of the filing entity and manually amend the dataset for nearly 2,700 records, which proved to be a very time-consuming process. For about 90 percent of the patent records that included no further information regarding the location of registering entities and thus required manual lookup, the filing institutions turned out to be headquartered in China. While speculating whether this is due to differences in filing practices or amounts to purposeful, strategic underreporting is beyond the scope of this chapter, it is nonetheless an interesting point to note. Non-Chinese inventors are less opaque about the origins of their sponsoring entities.

To gain some high-level insight into the structural characteristics of the Chinese and US quantum patenting landscape, the following section discusses some of the most important parameters of the Chinese and US quantum patent networks.

6.2 Quantum leadership

One of the auxiliary queries outlined in Chapter 1 asks about the entities involved in building a future quantum internet. Figure 6.3 below shows the top ten organisations that have registered relevant patents in the domains of quantum computing and quantum communication in 2015-2021. The top two registering applicants are IBM and Intel, multinational companies headquartered in the US, followed by TCL Corporation, a Chinese consumer electronics company headquartered in Huizhou with reported revenue of c$10 billion in 2019.

By count of newly registered quantum internet patent data, IBM is the single biggest player by a significant margin. However, places 7-10 go to Chinese organisations, notably ‘Origin Quantum Computing’, which has links to the University of Science and Technology in Hefei, the leading Chinese research institution in the quantum internet domain.

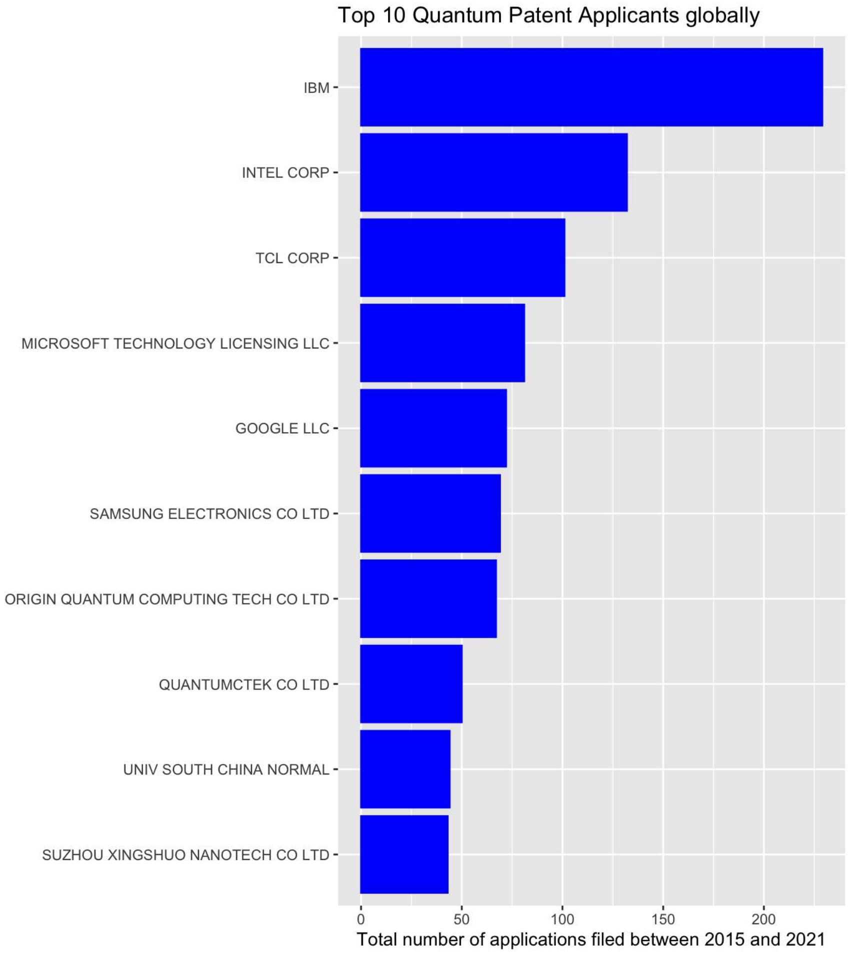


Figure 6.3: Cumulative quantum internet patent registrations by the top 10 registering entities, 2015-2021.

However, the dominance of US companies at the top of this chart does not necessarily imply an overall leadership position in patenting activity. Figure 6.4 shows the total number of relevant quantum tech patent data registered by country for each year under consideration. While roughly on a par with the US only eight years ago, at the start of 2022 China dominated the patenting landscape and outperformed the US by a magnitude of 4 in terms of annual patent registrations. While the big players are American, China has successfully developed a large number of small to mid-sized entities that register quantum patents at significant pace. Over a five-year period, the number of annual patents that organisations headquartered in China have registered, has risen fivefold.

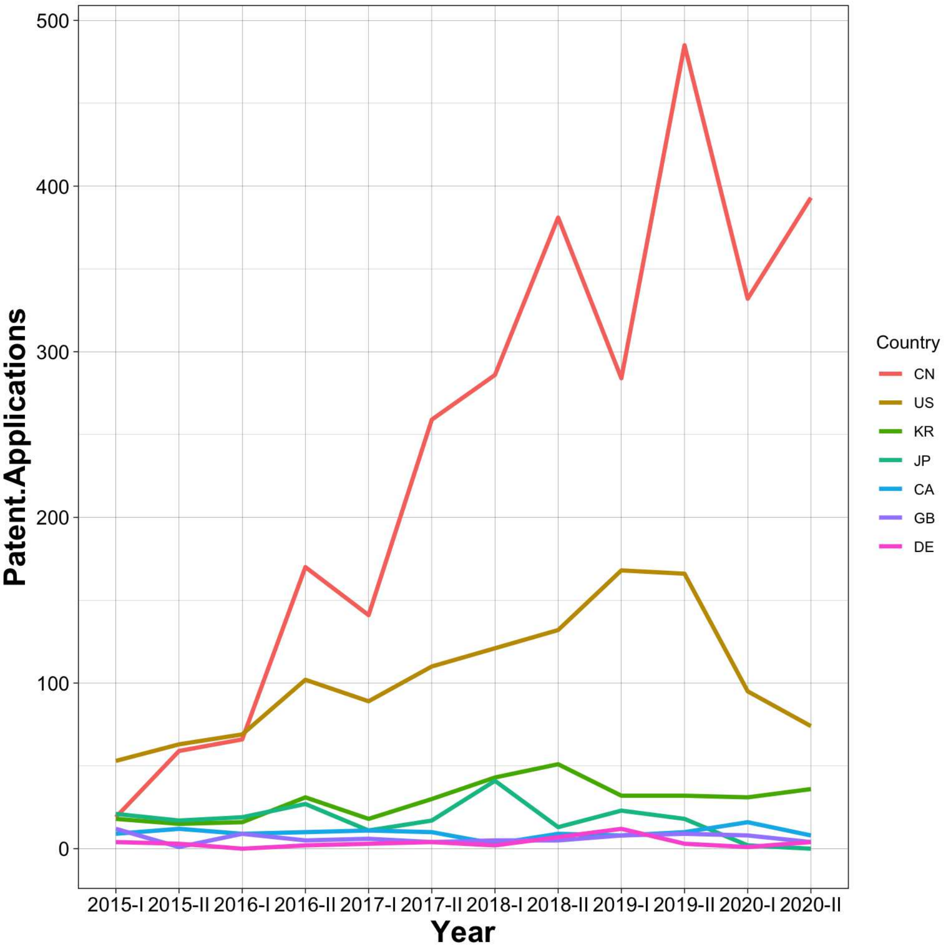


Figure 6.4: Quantum internet patent registrations in the top 5 countries.

Other countries trail by a significant margin. The patent output rate of Japan, Canada, the UK and Germany has been fairly steady however. It should also be noted that the quantity of output in this domain does not necessarily reflect on the quality or robustness of the inventions so registered. This issue will be discussed further in Chapter 7. However, a first, cursory glance at the data reveals that China seems to have changed gears around 2015 and is now pursuing its quantum development programme at full throttle.

6.2.1 Quantum patent citation data as networks

The data retrieved from the EPO contain all information available about a patent in a single row entry. Details of citations are contained in a dedicated column. If a patent cites no other patents as prior art, the associated cell returns a nil value. Blank cells indicate bad practice. Similar to research output in academia, such as articles and conference papers, sources that have informed the work should be included. Therefore, in a first step, ghost nodes (isolates) of this sort were removed.

Next, the datasets were analytically transformed into network objects. Every patent record can be considered a node in a network (cf. (Easley & Kleinberg 2010)). To do this, records retrieved from the EPO had to be cleaned further and separated by citation. When a record in the dataset contains x number of citations to other patents (themselves included in the dataset or not), it forms x edges to other nodes such that these other nodes are the output from the cells that contain information about patent citations. This process necessarily increases the number of records in the set. For instance, if a record in the raw dataset retrieved from the EPO cites four other patents, there will be five nodes in the network.

To provide an illustrative example, consider the Chinese patent (CN 104638076 A 20150520), later published as (CN104638076A), '*LED (light-emitting diode) epitaxial structure capable of increasing LED backward impedance and preparation* *method thereof*'. This is a 2015 patent for placing multi-quantum layers on substrates, a research area in optoelectronics. The patent was registered by Suzhou Nanojoin Photonics Co Ltd, a semiconductor company headquartered in Jiangsu. Thanks to separating citation information into nodes, the citation relationship of this patent with other patents (nodes) can be illustrated as follows.

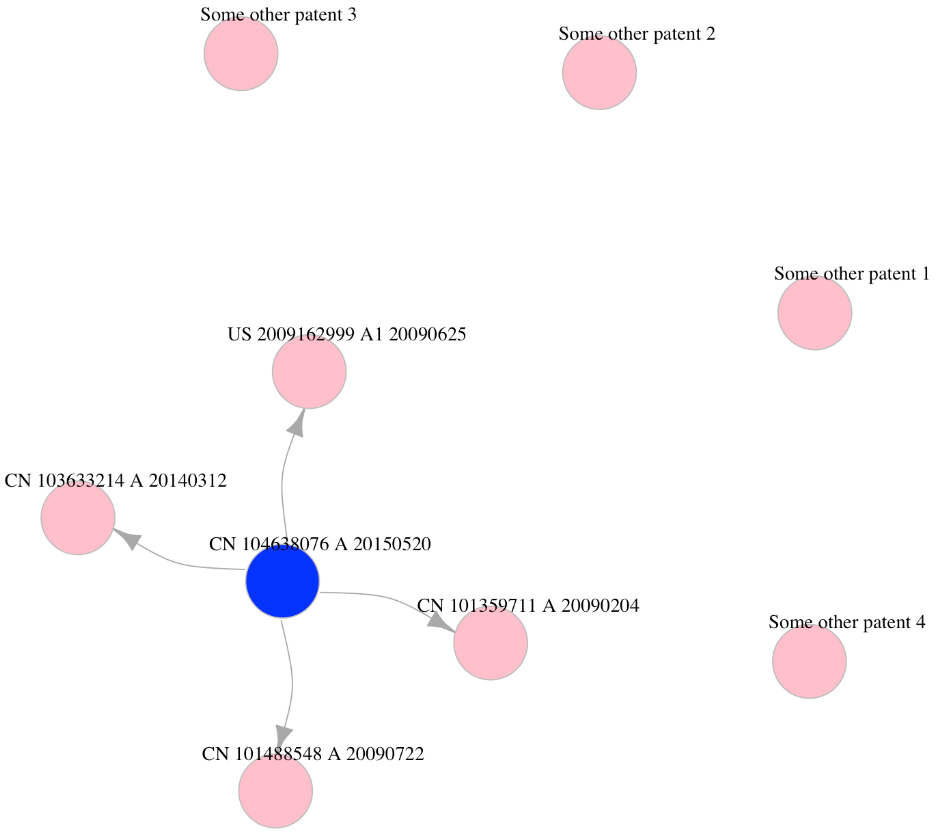


Figure 6.5: An example of representing a citation network as a graph object.

Four edges point from the patent in question (coloured in blue). This means that the invention cites four other patents as prior art. Details of the cited patents can be found in Table 6.3 below.

Patent ID	Title	Applicant
CN 101359711 A 20090204	Green light LED	SHANGHAI BLUE LIGHT TECHNOLOGY [CN]
CN 101488548 A 20090722	LED in high In ingredient multiple InGaN/GaN quantum wells structure	SHANGHAI BLUE LIGHT TECHNOLOGY [CN]
CN 103633214 A 20140312	InGaN/GaN superlattice buffer layer structure, preparation method of InGaN/GaN superlattice buffer layer structure, and LED chip comprising InGaN/GaN superlattice buffer layer structure	HUNAN HUALEI OPTOELECTRONIC CORP
US 2009162999 A1 20090625	Method of Growing Nitride Semiconductor material	UNIV NAT CENTRAL [TW]

Table 6.3: The patents cited by (CN 104638076 A 20150520).

For the purpose of further analysis, nodes were then divided into three categories. Each node has either of the following characteristics:

i) source: these are new patents relevant to building the quantum internet that were registered by Chinese/US institutions over the period 2015-2021. Nodes in ‘source’ cite other patents but are not themselves cited by any other patent record in the dataset. The patents that are cited as prior art by ‘source’ patents were further coded in binary fashion as either ‘domestic’ or ‘foreign’ in origin. The citation therefore establishes an outward edge between the patent and a prior patent that is being cited (patent citation networks are directed graphs). As they cite other patents but are not cited by any other patent in the dataset, source nodes have only outgoing edges.

ii) hubs: new inventions may cite prior patents that serve as hubs. These are cited by new patents in the dataset but may themselves also cite other patents in the same dataset. For example, a 2020 patent cites a 2018 patent which cites a 2016 patent, all of which are in the dataset that covers the period 2015-2021. Hubs therefore have in- as well as out-degrees, meaning that a chain of citations traverses through the hub.

iii) sinks: such chains come to a stop when they cite sinks. Sinks are patents that are cited by others in the dataset but themselves do not cite any other patents or prior art. Sink nodes therefore only have in-degrees.

'Hub' patents therefore have an outward edge pointing to 'sink' records and incoming edges from 'source' that point to 'hubs'. To sum up: 'source' patents only have out-degrees, 'sink' patents only in-degrees, and 'hub' data have both incoming and outward edges.

Grouping patent records in this way allows for visual inspection of structural features depending on the relative status of a record in the network. Large networks are difficult to visualise as they can quickly turn into messy, uninformative 'spaghetti' or 'hairball' plots. To avoid this, the data is here displayed as hives. A hive plot shows the network in its entirety as a graph with three axes: source, hub and sink. In hive plots, axes are distributed radially where distance between nodes captures some qualitative or quantitative characteristic of the structure of the network.

In the graphs below, nodes were grouped by their degree (i.e. the number of links they have with other nodes): the farther the distance to the core, the higher the degree of the node. While hive plots are visually much more informative than traditional network plots, the drawback is that they are computationally expensive. For the Chinese quantum patent network, for instance, the hive plot requires calculating an adjacency matrix with 50 million elements.

Put differently, nodes (i.e. patent records) were ordered by their magnitude, i.e. their degree: the number of edges that either point to the node, or point from the node to a different patent (in undirected graphs, this difference would not matter, but here it does). Let edges that point to domestic citations (i.e. a Chinese/US patent cites another Chinese/US patent as prior art) be coloured in green. Citations of foreign patents are to be coloured in red. The two hive plots below, rendered using the HiveR package in R ((Hanson 2020)), amended for the purpose of this analysis, show how the Chinese and American patent networks differ in terms of their structural characteristics. Each is discussed in turn.

China: The Chinese quantum internet patent citation network is made up of 6,134 nodes and 6,970 edges, with radii spanning from 1 to 27. This means that the smallest node in the network (closest to the core) only has one edge pointing either to it or away from it, while the biggest node (as furthest away from the centre of the graph) connects to 27 other nodes (citations).

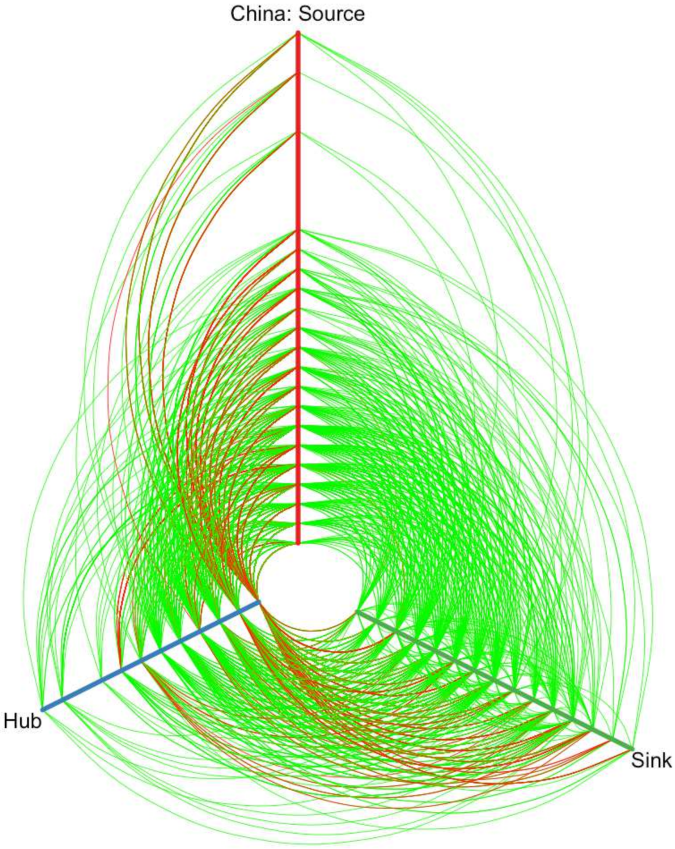


Figure 6.6: A structural hive plot of the Chinese quantum patent network that visualises how citations of domestic (green) and foreign (red) prior art feed through the network.

Two things stand out immediately: (i) New Chinese quantum internet technology patents overwhelmingly cite domestic, i.e. Chinese technology (green), which suggest a fairly independent and self-sustaining quantum ecosystem. (ii) Where new Chinese patents that are not being cited by any other entity (source), or cite patents that themselves do not cite any prior art (sink), these citation relationships are almost one hundred percent domestic. This is the right hand side of the graph between the ‘source’ and ‘sink’ axes that is almost entirely coloured in green. This is empirical evidence for a fairly exclusive and exclusionary Chinese patent network where Chinese inventions establish R&D chains with domestic technologies only.

USA: The first important point to note is that the US quantum patent dataset is significantly smaller (as already suggested by Figure 6.4. However it is much wider in range by measure of degree centrality, i.e. the number of edges that point two or from US citation nodes. The US quantum internet patent network is made up of 2,863 nodes and 3,201 edges, with radii spanning from 1 to 63. This means that the most visible US patent is more than twice as prominent as its Chinese counterpart that only counts 27 edges.

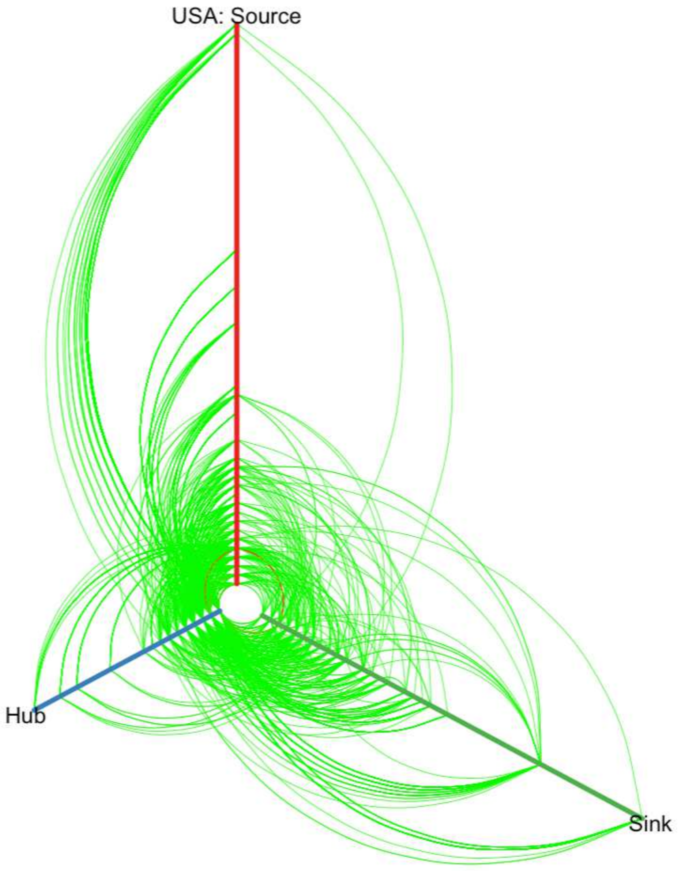


Figure 6.7: A structural hive plot of the US quantum patent network that visualises how citations of domestic (green) and foreign (red) prior art feed through the network.

As far as the US is concerned, the phenomenon of exclusively citing domestic technologies is even more pronounced than in the Chinese case. Out of more than 3,000 edges (i.e. citation links) in the network, only a hundred or so point to foreign technologies. These are mostly low-impact nodes around the core with only a couple of edges pointing to/from them and as such are hardly visible in the graph.

Thus a cursory inspection of the two hive plots reveals some remarkable insights.

Commentators would often point to lax Chinese practices in recognising foreign intellectual property (Huang & Smith 2019). There is of course a large number of cases where China has outright appropriated intellectual property from competitors abroad, which causes significant costs to Western economies. While there is evidence in the data that in the quantum domain, there is a strong preference of Chinese entities to cite domestic technologies, this effect however is much more pronounced in the case of the US. American companies, universities and research institutions cite almost exclusively US-owned technologies when registering novel quantum internet patent data. What happens in the rest of the world does not really matter.

This is empirical evidence for two quite separate and independent research programmes. The full implications of the structural qualities of the two patent networks will be discussed in more detail in Chapter 7.

6.2.2 Some further indicators

In a citation network, nodes differ in terms of their degree centrality (i.e. the number of edges that connect them to other nodes). The minimum value is 1 (to be included in the analysis the patent cites at least one other, or is being cited by at least one invention). The maximum value may be construed a measure of its relative importance in the network: either as a patent that is being cited by many others if its in-degree centrality is large, or a patent that cites other works extensively so that its out-degree centrality is high. In the above case of a US node with a centrality of 63, the patent in question, is an example of the latter. US patent (US 9971970 B1 20180515) indeed cites 63 other US patents as prior art, displaying the maximum possible degree of homophily. Figure 6.8 below illustrates the citation behaviour of this node coloured in blue.

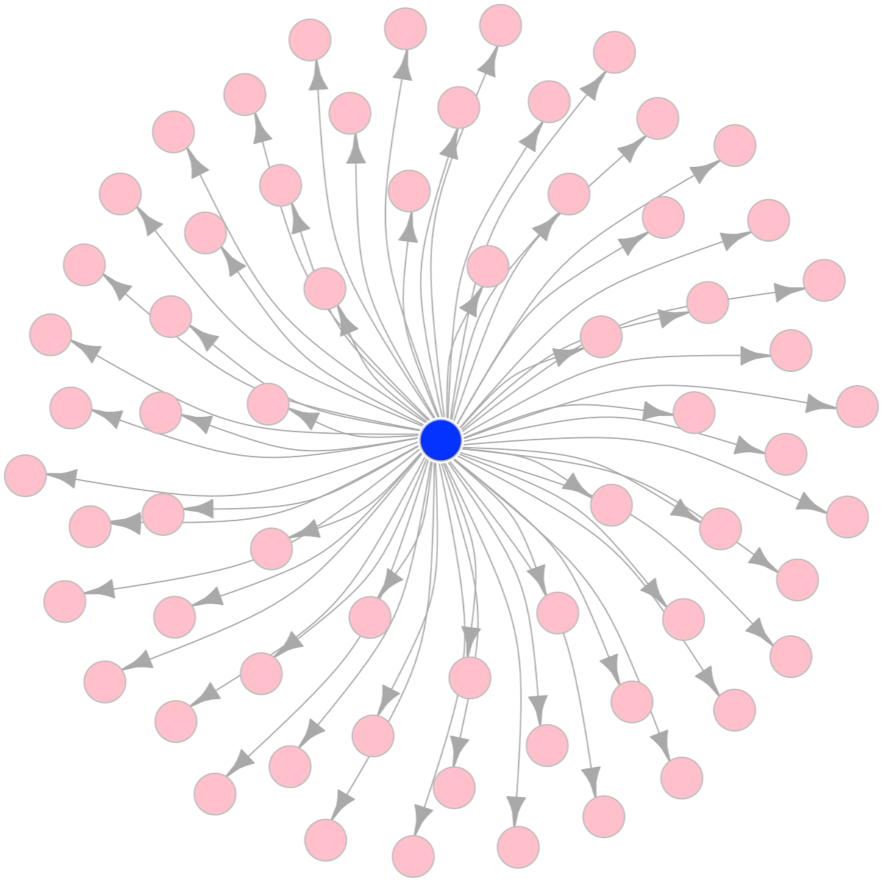


Figure 6.8: A subgraph of the citation practice of patent (US 9971970 B1 20180515), the node with the largest degree centrality. It cites 63 other US patents as prior art. Node IDs have been omitted for better visualisation.

There are, of course, other indicators that provide insight into the technological determinants that will shape the quantum internet. Table 6.4 below collects some for further discussion.

Measure	China	USA
# of nodes	6,134	2,863
# of edges	6,970	3,205
Mean degree	1.136	1.119
Density	0.0001852747	0.0003911443
Transitivity	0.01874341	0.005263456
Diameter	6	6
Mean distance	1.569286	1.447725
# components	340	212
Size of largest component	2,230	1,589

Table 6.4: Some key indicators of the structural properties of the Chinese and US quantum internet patent citation networks.

Mean degree: This is simply the total number of edges divided by the total number of nodes in the network and therefore expresses an average: $m = \sum E / \sum N$. With no further knowledge of network structure, one would expect any randomly picked node to have m citation links. Both networks are remarkably similar in terms of this measure, which suggests a similar approach to citation practices overall. This may simply be because of the very nature of this research area; one that affords citation signalling that can be summarily expressed as $1.119 \leq m \leq 1.136$. It is a remarkable finding however in that it attests to a convergence of approaches across quite disparate and siloed research ecosystems.

Density: The density of a citation network d captures how many citation links are actually present out of all possible links. In an empty graph, no node is connected to any other, so $d = 0$. In a maximally full graph, each patent record would cite every other patent in the dataset so that $d = 1$. The indicator is therefore calculated as $d = (\sum E/\sum N) * (\sum N - 1)$ (cf. (Jilbert & Lizardo 2020)).

The US citation network is twice as dense as its Chinese counterpart. This means that a random node in the US network is twice as likely to cite (or be cited by) a different node in the dataset, which suggests a more thorough citation practice and/or comprehensive knowledge of the (domestic) quantum patenting landscape.

Transitivity: As the term suggests, this indicator expresses how easily, or how quickly, a patent citation will pass through the network. In statistical terms, it is the probability $0 \leq p \leq 1$ that nodes form local clusters. In the literature, this term is therefore also referred to as the 'clustering coefficient'.

On this measure, the Chinese patent network is significantly more likely to form clusters. It surpasses the US network by a factor of 3, which means that a Chinese patent record is three times more likely to be part of a local group or community of records than an American one. This is evidence of significant homophily in the Chinese quantum internet patent network.

Diameter: This is the longest citation path present in the network (in terms of the number of edges). It expresses how 'wide' the network is and how far a citation travels from two maximally distant nodes. As such, it is a measure of relative importance of the initial patent in the chain so that a future patent will cite it, which in turn will be cited by yet another patent and so forth. On this measure, both networks are structurally identical.

Mean distance: This is the average number of edges between any two randomly picked nodes in the network. Phrased differently, it is the overall average path length, i.e. the mean of the shortest distance between pairs of nodes. It can be broadly construed a measure of efficiency of patents in citing each other in that on average, each patent record is x steps away from any other, where x is the mean distance. In this case too, both networks are structurally similar. On average, nodes are $1.447725 \leq x \leq 1.569286$ edges (steps) apart.

Number of components: Large graphs are usually made up of smaller subgraphs or communities in which nodes are more strongly connected to each other than to other nodes in the network. In the case of patent citations, these are groups of patents with a stronger preference to cite one another relative to the citation network as a whole. This is an informative indicator regarding the structural partitioning of the graph.

The most common way to partition a network is to separate it into connected components. In each of these components, the nodes are connected to each other but not to any other node outside the component. It is common for most networks to have one single-biggest component that makes up a big chunk of the network overall, plus several smaller components that are self-contained (Meghanathan 2016, Das et al. 2018).

The number of components in the Chinese quantum patent network is 340. This means there are 340 complete subgraphs in the network, each of which is comprised of weakly connected nodes such that all nodes in the subnetwork can be reached via directed citation chains, (i.e. node i can reach node j but j can't reach i). There are two large components of around 2,000 nodes each; the remaining 338 components are of size 2 to 20.

With two independent subgraphs of this magnitude present in the data, it must be assumed that China pursues not one but two distinct quantum research programmes that are fairly independent from each other. This can be accidental or strategic. If strategic, it suggests a purposeful strategy to run two programmes, although an explanation for this approach is not in the data. If accidental, it would imply that one programme does not really know (or cares) what the other is doing.

The US network looks different. It contains a single-biggest component of 1,589 nodes followed by a dozen or so smaller subgraphs that range between 10 and 38 vertices, and a vast trail of dyads. This suggests a more unified approach in that the US quantum research programme seems to be one big project that draws on the same sources of prior research.

At this stage it helps to visualise the distribution of a key structural indicator, that of the mean.

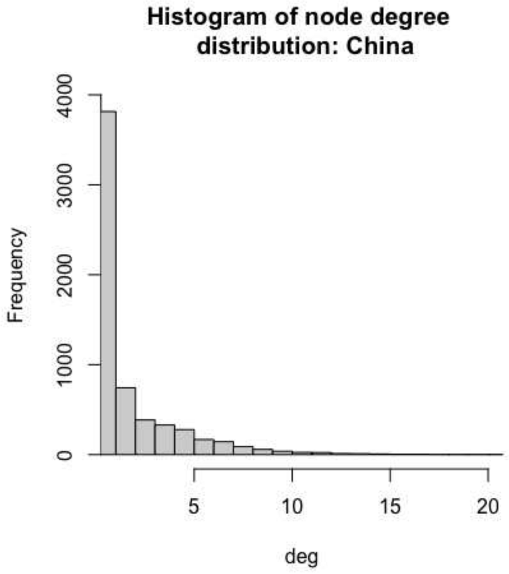


Figure 6.9: Node histogram of the Chinese patent citation network.

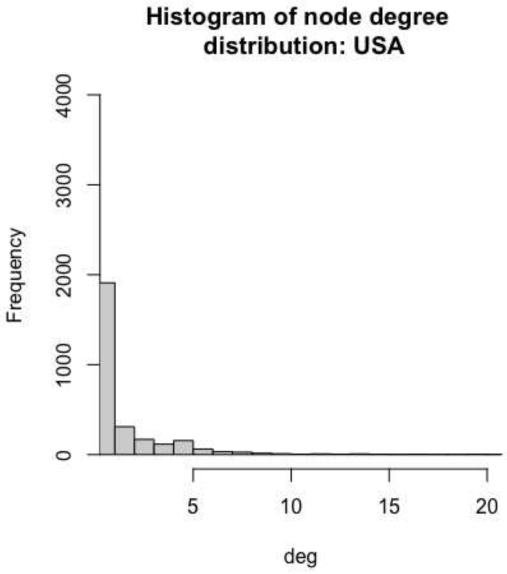


Figure 6.10: Node histogram of the US patent citation network.

While the degree distribution seems to be following roughly the same power law, the Chinese network has more than double the number of unitary nodes that cite only one other patent, or are being cited by only a single invention. Put differently, in the Chinese network, the number of patents that do not gain much traction, is nearly one hundred percent higher relative to the US network.

There are two possible reasons for this. Either Chinese inventors are ahead of the curve to such an extent that not even fellow domestic scientists pick up on their output, or, perhaps more realistically, there is significant deadweight in the Chinese patent citation network, meaning a lot of research with little or no impact finds registration with patent offices. This point will be discussed further in Chapter 7.

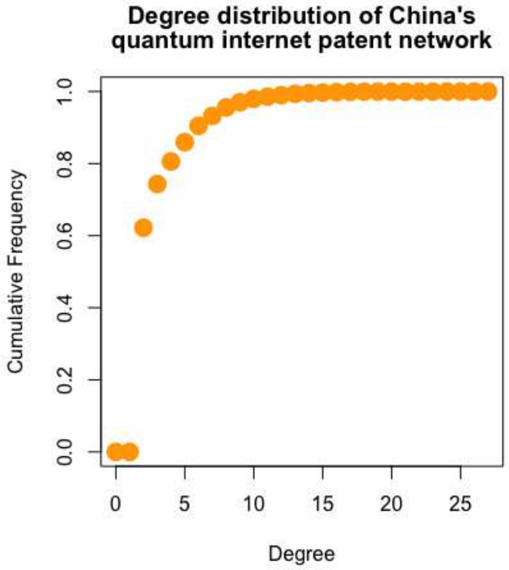


Figure 6.11: Node degree distribution of the Chinese patent citation network.

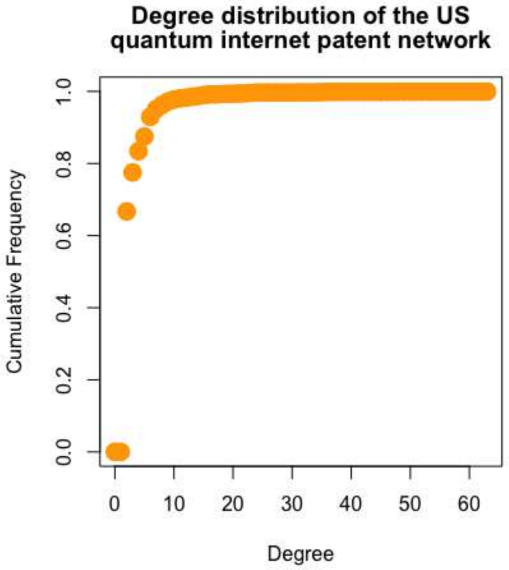


Figure 6.12: Node degree distribution of the US patent citation network.

Plotting the degree distribution for both networks (figures 6.11 and 6.12 above), confirms the earlier discussion of network structure, mean degree and diameter. Both networks show a large number of nodes with relatively few degrees. In both networks, nearly 95 percent of all nodes have ten or fewer citation links, attesting to significant structural similarities. In the US network, however, the tail end is much longer in that it reaches the aforementioned ‘super node’ of 63 connections.

The above analysis has identified important structural characteristics of the network as a whole. But what are the most important patents in the Chinese and US patent networks, and what makes them ‘most important’? A final descriptive measure that is immensely helpful in this context is that of the k-core (Hoffman 2021*a*). The concept assumes undirected graphs so consider, for a moment, that the direction of citations does not matter.

The idea is to successively ‘peel away’ outer nodes with only a few connections to reveal the core of the network that holds the entire graph together. The k-core is a token of resilience of a network: how many shocks to its periphery can the core of the network survive? The core is the subnetwork of the most tightly interlinked nodes. Applied to the context of patent citations, it means finding the most influential patents the removal of which would cause the entire citation network to fold and collapse in on itself (i.e. return an empty graph with zero edges).

Formally, the k-core of a network is the maximal subgraph of the graph such that the minimum degree of that subgraph is greater or equal to k. It is a dynamic concept. It is not possible to identify from the outset what the k-core of the graph will be. By design, both citation networks only contain records with at least one citation link so by definition, there are no isolates to remove. The starting point is therefore $k = 1$ so that only nodes can remain which have at least $k + 1 = 2$ edges.

In this iterative process, removing all nodes with only one connection ($k = 1$) will first 'peel off' all nodes with only a single link. In so doing however it will expose new nodes that now only have one connection left (i.e. those of degree 2 previously for which the removal of an edge has caused it to lose a link so that now has only one edge left). These newly emerging nodes of degree 1 will need to be removed also. In the next step, the procedure is repeated for $k = 2$ and so forth. The process stops at the point where $k + 1$ would return a null, or empty, graph; i.e. there is no subnetwork with more than k edges. The resulting k-core then is the most stable, and arguably fundamental and most important, subnetwork.

The below table 6.6 shows the results from computing the k-core for the Chinese quantum network.

k	1	2	3	4	5
# nodes	4,429	1,463	218	11	13

Table 6.5: k-core statistics for the Chinese quantum patent network for $k = 1...5$.

The Chinese quantum patent citation network has a unique core for $k = 5$, meaning that there is a unique subnetwork of 13 nodes that cannot be reduced any further. More than 4,400 nodes get lost after the first cut. Only 13 patents out of more than 6,000 records survive and constitute the stable core of this citation network. Removing only these 13 patents would collapse the entire Chinese quantum internet patent citation network. Figure 6.13 below visualises the Chinese 5-core subgraph.

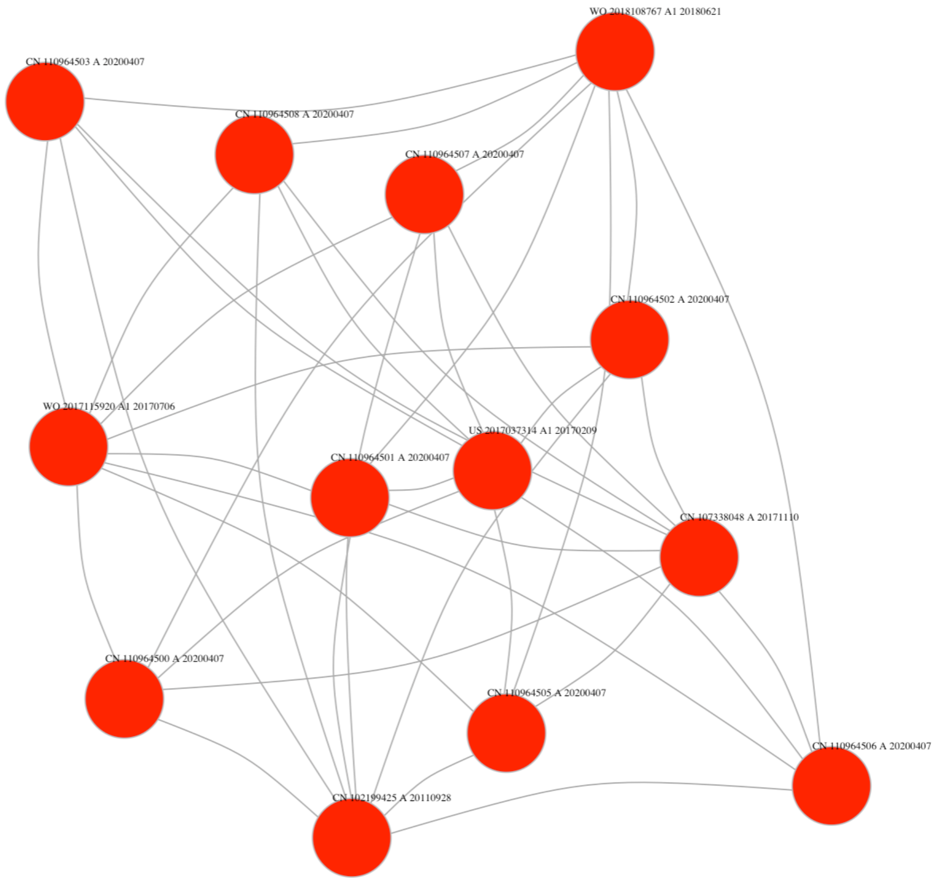


Figure 6.13: The stable 5-core of the Chinese quantum patent network.

As far as the United States are concerned, the results are discussed below. The maximum subgraph is reached for $k = 4$, suggesting that the US citation network is less closely linked and less stable than the Chinese one: there are no nodes with five or more connections that could emerge out of previous rounds of 'peeling off'. While the Chinese network loses around two thirds of its nodes after the first round, this effect is even more pronounced in the US network where roughly three quarters of patents do not survive the first chop.

k	1	2	3	4
# nodes	2,215	520	110	18

Table 6.6: k-core statistics for the US quantum patent network for $k = 1...4$.

The US 4-core is visualised below. It contains 18 nodes, i.e. five more than its Chinese counterpart.

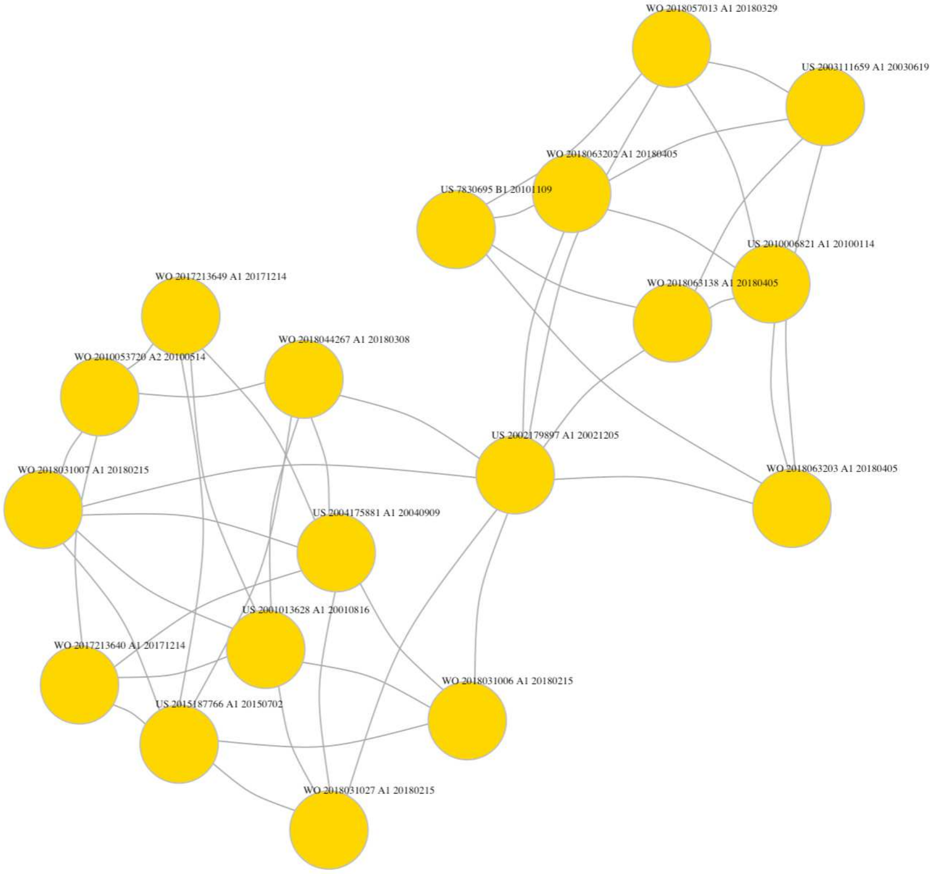

WO 2018057013 A1 20180329
US 2003111659 A1 20030619
WO 2018063202 A1 20180405
US 7830695 B1 20101109
US 2010006821 A1 20100114
WO 2018063138 A1 20180405
WO 2017213649 A1 20171214
WO 2018044267 A1 20180308
WO 2010053720 A2 20100514
US 2002179897 A1 20021205
WO 2018063203 A1 20180405
WO 2018031007 A1 20180215
US 2004175881 A1 20040909
US 2001013628 A1 20010816
WO 2017213640 A1 20171214
WO 2018031006 A1 20180215
US 2015187766 A1 20150702
WO 2018031027 A1 20180215

Figure 6.14: The stable 4-core of the US quantum patent network.

Both the Chinese and US quantum patent networks are structurally similar on important metrics. They also carry a large number of patents that do not seem very influential (they cite only one patent, or are being cited only once). Despite their similarities however they are independent from each other in that neither side would cite the other; it is almost as if they are sealed off against foreign influence. The next section dives deeper into the internal dynamics of these networks.

6.3 An ERGM quantum patent model

The bird's eye view of the previous section has established some important insights into the Chinese and US quantum patent networks. While there are differences in terms of density and k-core, the networks are structurally similar on counts of mean degrees, mean distance, diameter and, importantly, the character of their largest components, albeit there being two in the Chinese case. Yet the patent networks seem to be evolving quite independently. The analysis of descriptive indicators reveals only little cross-referencing, or recognition, of the adversary's achievements in the quantum domain. In any case, they are not openly acknowledged in a way that would reflect in patent citations. Rather, it seems there are two siloed programmes of development that seem to wish to make as little reference to one another as possible.

The analysis of patent citation graphs suggests a large degree of homophily in the data: Chinese patents overwhelmingly cite domestic inventions as prior art. American filers of patents even more so. This section takes a closer look at the factors that constitute these properties. It inquires into the internal mechanisms of the Chinese and US networks that drive citations, and ultimately, quantum innovation.

The raw data retrieved from the European Patent Office's Global Patent Index contains additional information regarding the place, or locale, where new patents have been registered, the legal names of the registering entities, and the dates of the publication of any prior art cited in new patent applications. This is intelligence that can be added to graph nodes. The immediate question arises, are these attributes good predictors of patenting activity? In other words, do the places of publication or the type of organisation that files new patents predict US and Chinese citation practices? Is patenting activity driven by popular subcategories? What are the variables in a regression model that tests for significance of these attributes? This section pursues these points.

When it comes to patent citation data, regrettably, standard regression analysis does not apply. This is mainly because regression analysis, as it is being pursued in many important fields, implies the independence of events. If, for example, the Bank of England wishes to study how the British public responds to price increases of foodstuff, their econometricians can assume that purchasing decisions made on a Wednesday at a Tesco outlet in Southampton are independent from those made at a Waitrose in Tunbridge Wells on a Friday. While shoppers of course respond to macroeconomic news such as a spiralling inflation rate in a similar fashion, there is, most likely, no *interdependence* between responses among residents who are not even aware of each others' existence.[1] Thus BoE researchers can draw on decades of statistical modelling that assumes the independence of events.

By design, however, patent citations are different. Patent citations are strategic. In any case, they are governed by legal requirements, (gender) norms and estab-

[1] Shoppers A and B may both decide to not purchase a pack of crisps because it got so expensive but A does not refrain from purchasing it because of B's decision and vice versa.

lished practice (Bikard & Fernandez-Mateo 2022, Ryu & Kim 2022). A research breakthrough in some quantum domain, which is associated with a rise in citations of the successful patent, will have knock-on effects on entire citation chains. The previous section has found strategic over-citing of domestic technologies, which in itself is evidence that patent citations are not independently distributed. This structural problem in the data requires a different class of models.

As argued in more detail in the Methodology chapter, ERGMs have proved very useful for this purpose. ERGMs constitute a fairly novel research field, with early work on the computational modelling of interdependent processes published only fifteen years ago (Hunter et al. 2008). ERGMs take the following characteristic form.

The probability $\mathcal{P}_\theta$ of observing the network as constituted by the data, i.e. the graph (G), $\mathcal{P}_\theta(G)$, is defined as:

$$\mathcal{P}_\theta(G) = \frac{\exp\big(\theta^T \cdot \Gamma(G)\big)}{\sum_{G^* \in \mathcal{G}(N)} \exp(\theta^T \cdot \Gamma(G^*))} \tag{6.1}$$

The probability $\mathcal{P}_\theta$ of finding the observed network in reality, i.e. finding an expression for the chance that the graph (G) is a good representation of what is truly going on 'out there', $\mathcal{P}_\theta(G)$, is defined in the terms of above where $\theta, \theta \in \mathbb{R}^q$, is a q-dimensional vector of parameters, $\Gamma : \mathcal{G}(N) \rightarrow \mathbb{R}^q$ projects $\mathcal{G}(N)$ into $\mathbb{R}^q$, $G \rightarrow (\Gamma_1(G), ..., \Gamma_q(G))^T$ is a collection (of functions) of network statistics, such as homophily and transitivity and is as such q-dimensional, and finally,

$$c(\theta) := \sum_{G^* \in \mathcal{G}(N)} \exp\big(\theta^T \cdot \Gamma(G^*)\big) \tag{6.2}$$

which is a vast normalisation constant that is expensive to compute, and therefore requires approximation with standard Markov Chain Monte Carlo (MCMC) simulations (Stivala et al. 2020, Vega Yon et al. 2021, Caimo & Friel 2014).

In less technical terms, ERGMs test if the observed graph, in our case, the quantum internet patent citations networks modelled from data retrieved from the European Patent Office, is random. If so, there would be nothing significant to say about it. However if the observed graph is substantially different from random simulations based on similar characteristics (such as the indicators developed in the previous sections), then it reveals curious structural characteristics that are worth exploring further.

The model achieves this by dividing the probability of finding the observed model in reality (the numerator of the term above) by the sum of the probabilities of all possible observations of graphs with the same characteristics. Doing so derives an estimate of the chance that the observed graph could indeed be non-random. This explains the vast constant c that is so difficult to calculate–for N observations (in our case, the number of quantum patent citations, which equal the number of nodes in the network), there are 2^{N-1} variations of the model. This number is practically impossible to calculate even for small N, and therefore requires approximation.

Essentially, ERGMs assume that model dynamics can be explained by simultaneously occurring, interdependent events that can be summarised by network statistics, and are therefore an expression of them (Yon 2022). This makes it possible to test for interdependent tie formations, e.g. asking if registering a patent in one country drives the emergence of new patents in another while allowing that these activities also inform, say, what kind of organisation is likely to register new innovations.

The great feature about ERGMs is that formally, every factor is given the opportunity to be related to everything else–if they are not, they will not be significant. This is a huge plus as it does not require the researcher to make difficult assumptions about dependencies prior to the act of testing the model. In statistical terms, ERGMs predict tie formations as functions of individual covariates. This allows for disentangling endogenous from exogenous effects (which would have to be explicitly modelled in standard regression analysis). Because of this feature, ERGMs estimate the entire network in one step. The drawback is, unsurprisingly, that estimates take a lot of time to run.

The point of estimating ERGMs is to re-express the probability of the entire graph (as found in 'nature') in terms of probabilities of a tie formation between two nodes. These individual chances of tie formations (i.e. a citation chain in the context of this thesis) are presented as log-odds however and must therefore be transformed into percentage changes, which can be done by finding the expit (i.e. the inverse logit) of the coefficient θ that captures the term's individual contribution to the tie:

$$\beta_i = \frac{exp(\theta)}{1 + exp(\theta)} \tag{6.3}$$

The R documentation for ergm libraries contains a detailed discussion of the statistical theory behind this class of models (Statnet 2021).

For the purpose of building an ERGM, the data retrieved from the Global Patent Index was manually amended to better capture the intelligence contained in patent records. In particular, it hypothesises that the place (country) of publication, the organisational type of registering entities, and the IPC codes under which patents have been registered, have predictive power over how the Chinese and American quantum internet research programmes are shaping up.

To model these effects, the below variables have been added to the nodes of the patent citation graph. This exercise required a fair amount of time to look up places and institutions as there was a significant number of empty fields to deal with. This additional data was stored on separate .csv files that were then transformed into attribute lists, and finally joined with node matrixes so that they form multiplex graph objects. This was done in MS Excel and R.

Variable	Category	Expression
Country	2	CN = China
	3	DE = Germany
	4	EP = Spain
	5	GB = UK
	6	JP = Japan
	7	KR = South Korea
	8	US = USA
	9	WO = World / Intl
Applicant	15	Industry
	16	Private individual
	17	University or research institute
	18	Military
	19	Other
# IPC codes	21	1
	22	2
	23	3
	24	4
	25	5
	26	6
	27	7
	28	8
	29	9
	30	10
	31	11
	32	12
	34	14
	37	17
	40	20
	0	Otherwise

Table 6.7: The categorical expressions for the additional coding of patent data retrieved from EPO's GPI.

The category ‘# IPC Codes’ clusters the data according to the number of IPC codes under which publication had been sought. ‘1‘ means that the applicant has given their invention a single IPC code only while the maximum number of ‘20‘ means that the invention relates to 20 different categories in the IPC classification tree, and is therefore maximally broad in terms of the range of applicability and potential use cases. The ERGMs include these categories as potentially significant drivers of citation behaviour.

The following subsections develop the model for the Chinese and US quantum internet patent datasets. For both subsections, it presents three time-sliced ERMGs for the purpose of comparison: i) Period 1: July 2015 – June 2017; ii) Period 2: July 2017 – June 2019; and iii) Period 3: July 2019 – June 2021. The data has thus been grouped into three time periods of two years each going back to 2015. This is in order to trace the evolution of the quantum internet patent models and compare their significant coefficients.

6.3.1 The Chinese case

This subsection estimates three ERGMs for the Chinese dataset for the overall period July 2015-June 2021.

Period 1: July 2015-June 2017

The Chinese quantum patent network for this period has the following characteristics. It is a network of 1,036 nodes that connect over 940 edges. The density of the network is $0.00087x100 = 0.087$ percent. It is plotted below.

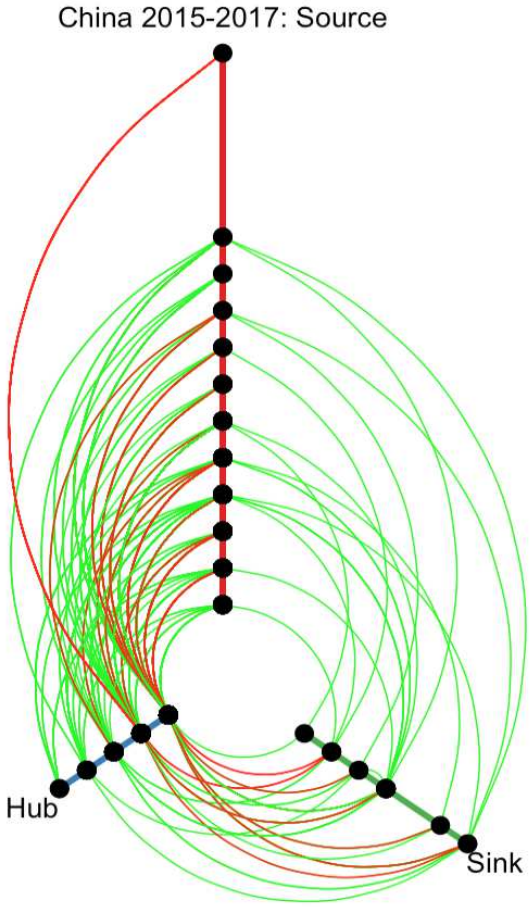


Figure 6.15: Network visualisation of the Chinese quantum internet patent citation network for July 2015 - June 2017.

As established in the previous section, descriptive indicators and a visual inspection of Chinese patent data suggest homophily in the data. ERGMs incorporate homophily terms so as a precursor to presenting estimates it makes sense to discuss what this covariate actually means.

The established term for homophily outside network analysis is assortativity (Meghanathan 2016, Bienenstock & Bonacich 2021, Mussmann et al. 2015). Assortativity a is the Pearson correlation coefficient and measures the degree to which a node property ψ correlates between pairs of nodes. It is normalised so that $-1 \leq a \leq 1$. A positive coefficient implies co-movement (and the network is said to be assortative): if $a > 0$, then nodes that share property ψ tend to be connected. The greater a, the more likely it becomes that nodes are connected if they share property ψ. Assortativity is therefore a measure of homophily in networks ('like attracts like'). In the context of this thesis, a measures the correlation between a vertex attribute ψ where $\psi = \{$Country of Patent Publication, Applicant Type, IPC clustering$\}$ and a patent citation, i.e. a is an expression for the chance that patent A cites B if they both share attribute ψ.

The below table collects the test statistics for assortativity for all three variables Country of Patent Publication, Applicant Type, IPC clustering for period 1, July 2015-June 2017.

Variable	Assortativity a
Country	-0.040
Applicant	0.0689
IPC	0.0379

Table 6.8: Assortativity covariates of the Chinese quantum internet patent network July 2015 - June 2017.

On this overall measure, if, for instance, two patents registered by Chinese entities share the property of being linked to x number of IPC codes, their chance of tie formation increases by $0.0379 \approxeq 4$ percent. The implications of these indicators are to be discussed more fully in the next chapter. While informative, they do not reveal much about dynamics internal to Chinese activity.

In its simplest form, an ERGM calculates the probability of observing the network,

$\mathcal{P}_\theta$, as a function of only one variable: edges. Computing this basic ERGM in R produces a Maximum Likelihood estimate of -7.047 for this period for China. This coefficient represents the *change* in the chance for a tie (citation formation) if the predictor (the number of edges) is increased by one unit. However, these coefficients are presented as log-odds and must be reverted to probabilities to make sense to the human eye–this is what the above equation β is for.

Doing so establishes an edge predictor of 0.0008766531, i.e. 0.9 percent. This means that there is chance of 0.9 percent to find an edge in the graph, or, alternatively, the probability of a citation being present is 0.9 percent. Returning to the discussion of descriptive statistics for a brief moment, logic demands this estimate to be equal to the density of the graph. A quick check indeed confirms this. Put differently, knowledge of the density of the network is sufficient for generating a stochastic process in which the only constraint is the chance for edges to be drawn (cf. (Hoffman 2021*b*)).

However the following sections assume that variables other than edges are relevant to understanding US and Chinese patenting activity–that is the very point of constructing an ERGM. In particular, as discussed previously, it assumes that the country of patent registration ('Country'), the type of registering entity ('Applicant') and the association with IPC codes ('IPC') all help to explain why the Chinese quantum patent citation network for that period should have formed the way it has.

In ERGM terms, this means estimating

$$\mathcal{P}_\theta = \hat{\beta}_0 + \hat{\beta}_1 \Delta(Country) + \hat{\beta}_2 \Delta(Applicant) + \hat{\beta}_1 \Delta(IPC) \tag{6.4}$$

where Δ captures a unit change in the value of the predictor and $\hat{\beta}_i$ is the log-odd change in response to it. The covariate $\hat{\beta}_0$ denotes the edges term as per above.

Computing the model in R produces the following Maximum Likelihood results:

Variable	Estimate	Std Error	MCMC %	z-value	$P > (\lvert z \rvert)$
edges	-6.06090	0.03315	0	-182.809	<1e-0 ***
nodematch.Country	-1.87252	0.31984	0	-5.855	<1e-04 ***
nodematch.Applicant	-0.08757	0.35670	0	–0.246	0.806
nodematch.IPC	-4.25425	0.65097	0	-6.535	<1e-04 ***

Table 6.9: ML test statistics for the ERGM of the Chinese quantum patent network June 2015-July 2017.

'Nodematch.X' is the ERGM term for homophily. The test reveals that the type of organisation has no predictive power over Chinese patenting activity. However, 'Edges', 'Country' and 'IPC' are most significant at the highest ***-level (reflecting a p-value of $[0 \leq p \leq 0.001]$.

Finally, calculating the probabilities from the log-odd changes (ignoring the organisational type) yield the following probabilities of citation formations.

Variable	Probability P
Edges	0.002326874
Country	0.1332504
IPC	0.01400482

Table 6.10: Probability estimators of the Chinese quantum patent network June 2015-July 2017.

The locale of patent citations has the biggest impact on tie formations. If an organisation that is headquartered in China successively registers two patents in, say, South Korea, the chance that they form a citation link is nearly 13.3 percent. This is empirical evidence for strong preferential treatment based on the location of the registering patent office–the density of the network is less than one percent as per above. Registering a new patent in the same country as previously multiplies the chance for a citation connection between them by a factor of 13. IPC clusters are also relevant but less so.

The presentation of estimates would be incomplete without a discussion of its goodness-of-it. The gof function in ergm prepares rounds of simulations of the patent citation network, to which the observed network statistics as presented above can be compared. The 'goodness' of the test statistic can be assessed relative to the outcome of the simulations. If the results above are close enough to what simulations predict the fit is 'good'; if they are far off it is likely that some processes are at work that have not been captured by the variables in the model.

The gof function achieves this in the following way. The above ERGM assumes that the process of citation formations are driven by the three variables that predict tie formations: Applicant, Country and IPC Code. If this is true, then these tie formations at the local level will, once aggregated, give the network its characteristic form. This network has properties, e.g. those discussed in section 6.2 above. The function then selects three of those: degree, edgewise shared partners and distance. These properties describe the network, and the function simulates several networks based on these parameters (Statnet 2021).

The question of goodness is then how well the model above, the one that was actually tested, can reproduce the networks that have been simulated using the parameters above. Put differently, how close is the estimated model to the network one would expect to see based on the characteristic parameters it has? The results from simulations vs actual test statistics can be plotted for visual inspection. Figure 6.16 below presents the most relevant summary plots for this purpose.

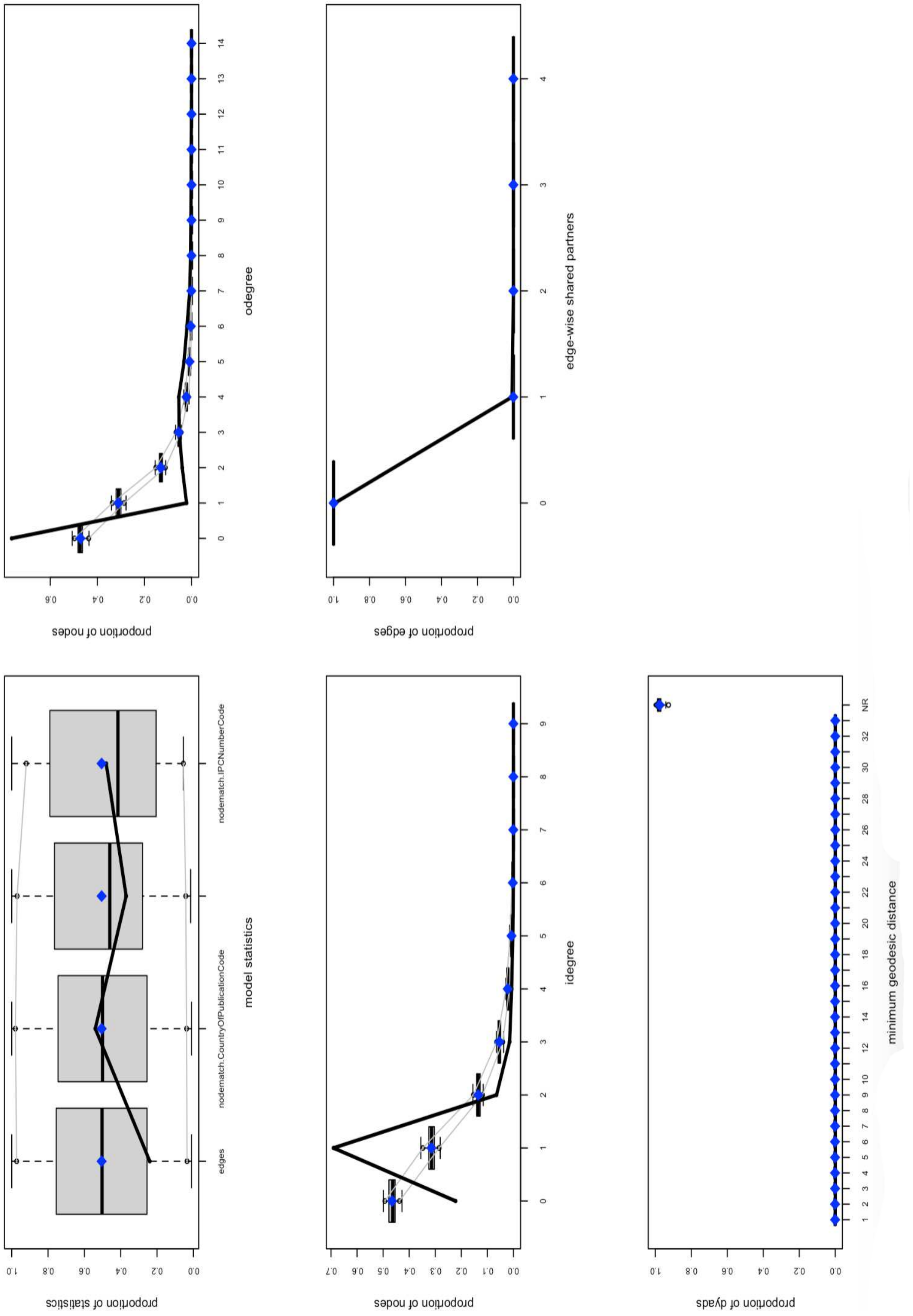


Figure 6.16: Goodness-of-fit parameters for the Chinese ERGM July 2015-June 2017.

Dots coloured in blue are the actual values from the dataset, the black line is the aggregation of the simulations. The better the black line fits the blue dots, the better the fit of the model. The ERGM performs well on all counts other than the number of in-degrees: simulations expect a greater proportion of in-degrees of value 1 than what is actually in the data. The implications are fully discussed in the next chapter. Overall, the model performs well.

Period 2: July 2017 - June 2019

The dataset for this period is significantly larger, reflecting just how much the quantum race has been gaining momentum. The network contains 3,208 nodes that span 3,243 edges. Its density is 0.0003152199, and the network is plotted below.

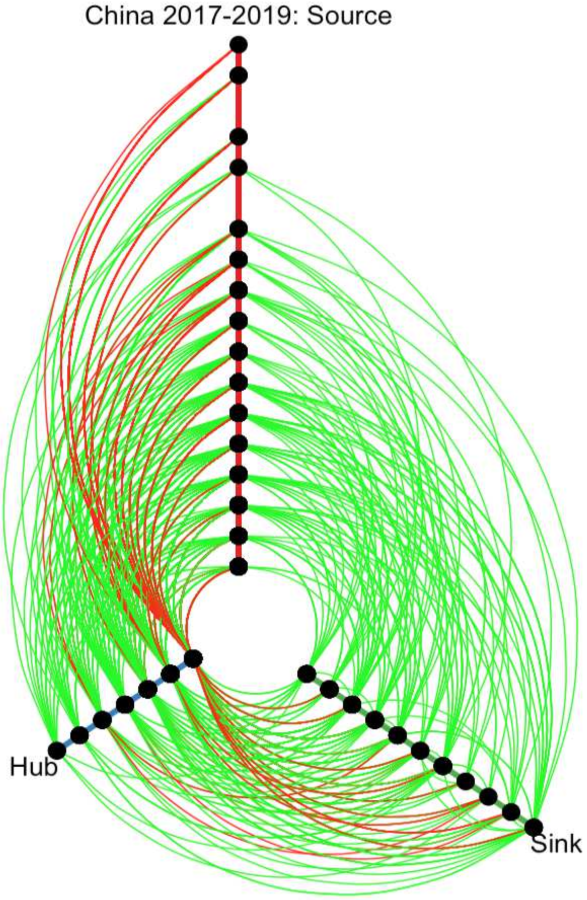


Figure 6.17: Network visualisation of the Chinese quantum internet patent citation network for July 2017 - June 2019.

As per above, the below table collects the test statistics for assortativity for all three variables Country of Patent Publication, Applicant Type, IPC clustering for period 2, July 2017-June 2019.

Variable	Assortativity a
Country	-0.06951287
Applicant	0.06633354
IPC	-0.008452967

Table 6.11: Assortativity covariates of the Chinese quantum internet patent network July 2017 - June 2019.

The assortativity measures for 'Country' and 'Applicant' have not moved much while 'IPC' in this period is now associated with moving in the opposite direction, if only mildly so.

And now the ERGM for period 2.

Variable	Estimate	Std Error	MCMC %	z-value	$P > (\lvert z \rvert)$
edges	-7.08774	0.01804	0	-392.930	<1e-04 ***
nodematch.Country	-1.06858	0.12646	0	-8.450	<1e-04 ***
nodematch.Applicant	-0.06872	0.15000	0	-0.458	0.647
nodematch.IPC	-3.48831	0.18346	0	-19.014	<1e-04 ***

Table 6.12: ML test statistics for the ERGM of the Chinese quantum patent network June 2017-July 2019.

The picture has not changed much. 'Country' and 'IPC' are most significant at the ***-level while the type of registering entity does not seem to be driving the Chinese quantum patent network in this period. Calculating the probabilities from the log-odd changes (ignoring the organisational type) yield the following probabilities of citation formations.

Variable	Probability P
Edges	0.0008345859
Country	0.2556732
IPC	0.02964668

Table 6.13: Probability estimators of the Chinese quantum patent network June 2017-July 2019.

The relative importance of country of filing as well as IPC cluster codes had risen sharply in period 2; in the case of ‘Country’ by more than ten percentage points while ‘IPC’ would witness an increase in relative importance by 200 percent. As to be discussed in the following chapter, this is evidence of an increasingly localised and siloed research programme.

The goodness-of-fit is as follows.

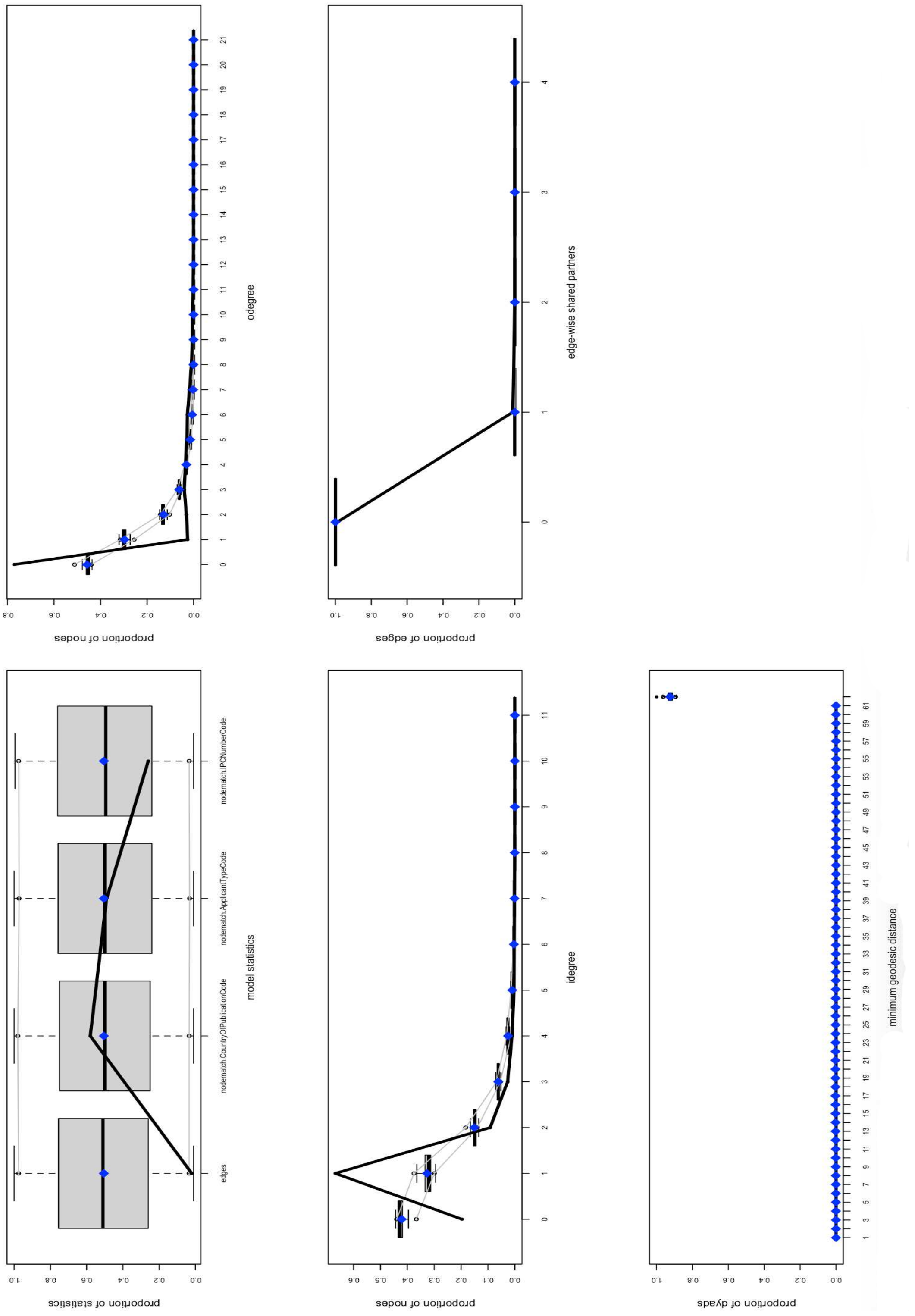


Figure 6.18: Goodness-of-fit parameters for the Chinese ERGM July 2017-June 2019.

In period 2, the ERGM fits the simulations less well: IPC codes are just about in range.

Period 3: July 2019 - June 2021

This subnetwork is of similar size. The network contains 2,810 nodes and exactly the same number of edges. Its density is 0.000354985, and the network is plotted below.

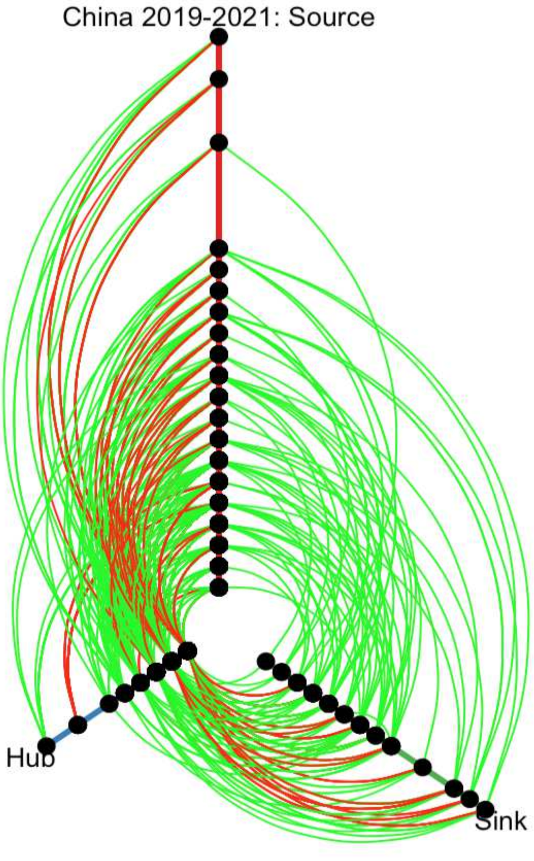


Figure 6.19: Network visualisation of the Chinese quantum internet patent citation network for July 2019 - June 2021.

As per above, the below table collects the test statistics for assortativity for all three variables Country of Patent Publication, Applicant Type, IPC clustering for period 3, July 2019-June 2021.

Variable	Assortativity a
Country	-0.03559451
Applicant	0.01589866
IPC	-0.08317109

Table 6.14: Assortativity covariates of the Chinese quantum internet patent network July 2019 - June 2021.

With this static measure, there is not much change of direction if compared to period 2.

And now the ERGM for period 3. In response to the decline in the goodness-of-fit of the model for period 2, the ERGM for period 3 introduces terms for reciprocity ('mutual') and triadic closure ('gwesp'). Reciprocity is excluded by the very fact that the network is a patent citation graph (patents cannot both simultaneously cite each other as prior art), and hence the coefficient is returned as -Inf (which means it can be discarded). Triadic closure suggests that triples are significant in the evolution of the network (if A and B, as well as B and C stand in a citation relationship, then A and C will form a link also).

Variable	Estimate	Std Error	MCMC %	z-value	$P > (\|z\|)$
edges	-6.79005	0.01921	0	-353.504	<1e-04 ***
nodematch.Country	-1.45733	0.17583	0	-8.288	1e-04 ***
nodematch.Applicant	-0.68515	0.19976	0	-3.430	0.000604 ***
nodematch.IPC	-3.37110	0.28414	0	-11.864	<1e-04 ***
mutual	-Inf	0	0	-Inf	<1e-04 ***
gwesp.fixed.0.4	2.65104	0.29477	0	8.994	<1e-04 ***

Table 6.15: ML test statistics for the ERGM of the Chinese quantum patent network June 2019-July 2021.

In the final period under consideration, the picture has changed considerably. All variables are now significant at the highest *** level, even the type of registering entity. The kind of organisation that registered a novel quantum internet patent has predictive power for the formation of citation chains. The coefficient for triadic closure (gwesp) is significant at the highest level, which suggests high level of local triadic clustering in the network.

And finally, calculating the probabilities from the log-odd changes produces the following probabilities of citation formations.

Variable	Probability P
Edges	0.001123649
Country	0.188876
Applicant	0.3351128
IPC	0.03321097

Table 6.16: Probability estimators of the Chinese quantum patent network June 2019-July 2021.

In the final period, with international competition over the quantum internet in full swing, the type of applicant is a substantial predictor of patenting activity. If, for instance, two patents were registered by the Chinese military or a military research facility, the chance of them forming a citation (sub)network rises by 33 percent (compared to the one percent chance of a tie formation for a random pairing of two nodes).

Finally, a check of the goodness of fit.

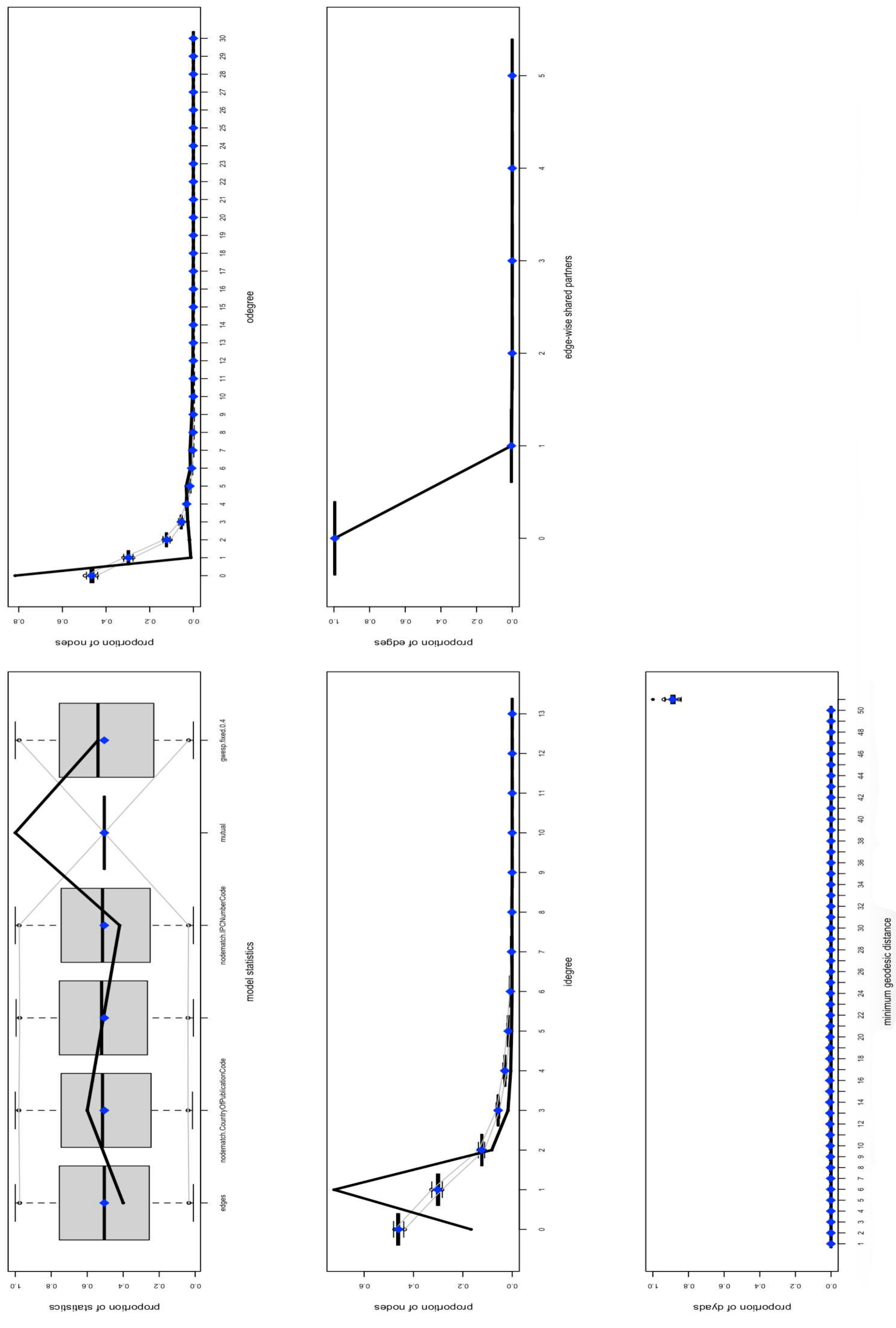


Figure 6.20: Goodness-of-fit parameters for the Chinese ERGM July 2019-June 2021.

The goodness has improved: all model statistics are in range and very close to the expected results from simulations (the coefficient for 'mutual' can be ignored as it is not defined). The goodness of fit for in-degrees is remains off however.

The following subsection develops three ERGMs for US data.

6.3.2 The US case

As discussed previously, the US quantum internet patent data ecosystem is smaller in scale but more robust in terms of static metrics. The below presents three snapshot time-sliced models following the same principles as in the Chinese case.

Period 1: July 2015 - June 2017

The US patent network for this period contains 725 nodes that span 672 edges. Its density is 0.001202134, and the network is plotted below.

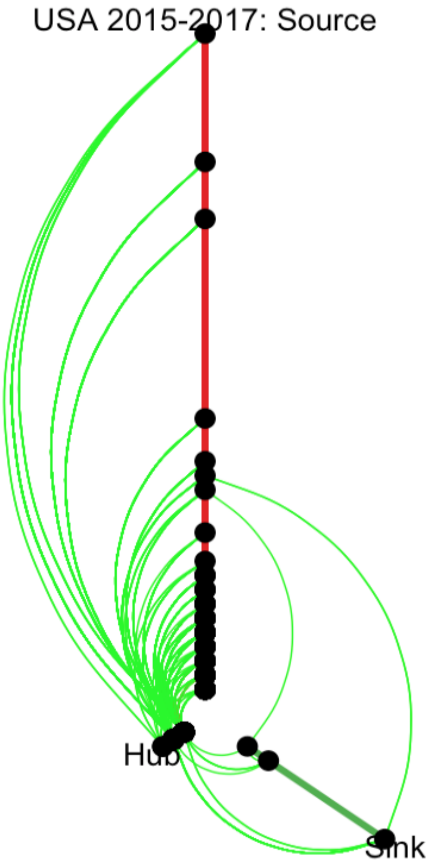


Figure 6.21: Network visualisation of the US quantum internet patent citation network for July 2015 - June 2017.

The below table collects the test statistics for assortativity for all three variables Country of Patent Publication, Applicant Type, IPC clustering for period 1, July 2015-June 2017.

Variable	Assortativity a
Country	-0.02490178
Applicant	0.0280033
IPC	-0.04363085

Table 6.17: Assortativity covariates of the US quantum internet patent network July 2015 - June 2017.

On these structural metrics, the US patent citation network is structurally similar to its Chinese counterpart.

The ERGM for period 1 is as follows.

Variable	Estimate	Std Error	MCMC %	z-value	$P > (\|z\|)$
edges	-5.52329	0.03902	0	-141.552	<1e-04 ***
nodematch.Country	-1.67033	0.57808	0	-2.889	0.00386 **
nodematch.Applicant	-1.59322	0.59272	0	-2.688	0.00719 **
nodematch.IPC	-Inf	0	0	-Inf	<1e-04 ***
mutual	-Inf	0	0	-Inf	<1e-04 ***
gwesp.fixed.0.4	-6.17045	36.74530	0	-0.168	0.86664

Table 6.18: ML test statistics for the ERGM of the US quantum patent network June 2015-July 2017.

Unlike the Chinese case for this period, the type of registering entity is significant at the ** level. IPC codes however cannot be calculated as the dataset is too sparsely populated for this period, which is why the program returns a calculation of '-Inf'.

And finally, calculating the probabilities from the log-odd changes for the significant values produces the following probabilities of citation formations.

Variable	Probability P
Edges	0.003976812
Country	0.1583802
Applicant	0.1689313

Table 6.19: Probability estimators of the US quantum patent network July 2015-June 2017.

Same-country and same-type-of-applicant registrations mean that the chance for a citation link to form is around 16 percent in each case.

The goodness-of-it computation returns the following.

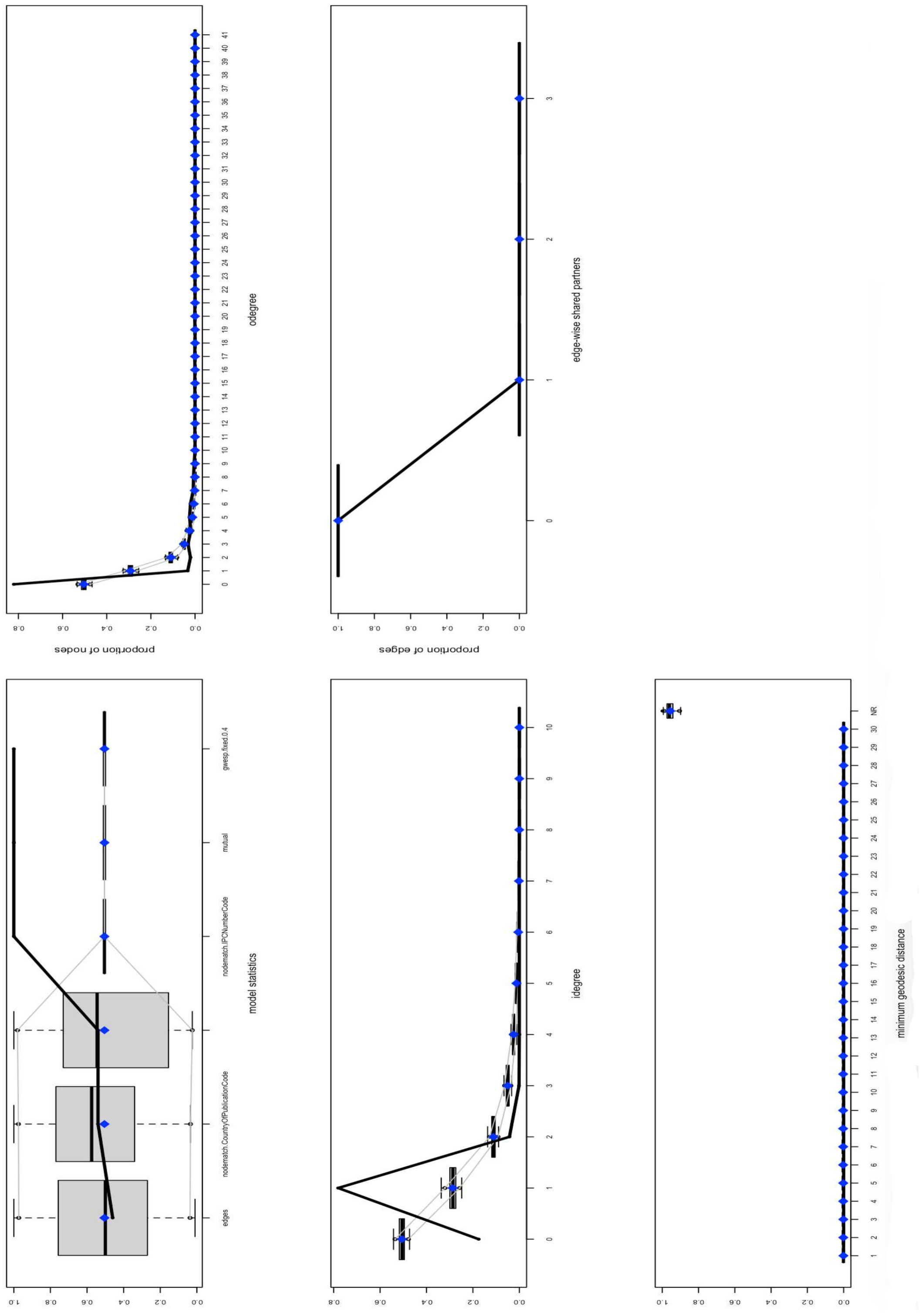


Figure 6.22: Goodness-of-fit parameters for the US ERGM July 2015-June 2017.

Since the program is unable to compute statistics for IPC codes and mutual tie formations (the former because of a lack of data, the latter because it is logical impossible), the model statistics only returns three estimates (upper left corner). The model statistics confirm that the ERGM fits the data well. As in the case with Chinese data, in-degree distribution proves a problem however.

Period 2: July 2017 - June 2019

The US subnetwork over this period has grown in size. It contains 1,404 nodes across 1,574 edges. Its density is 0.0007665705, and the network is plotted below.

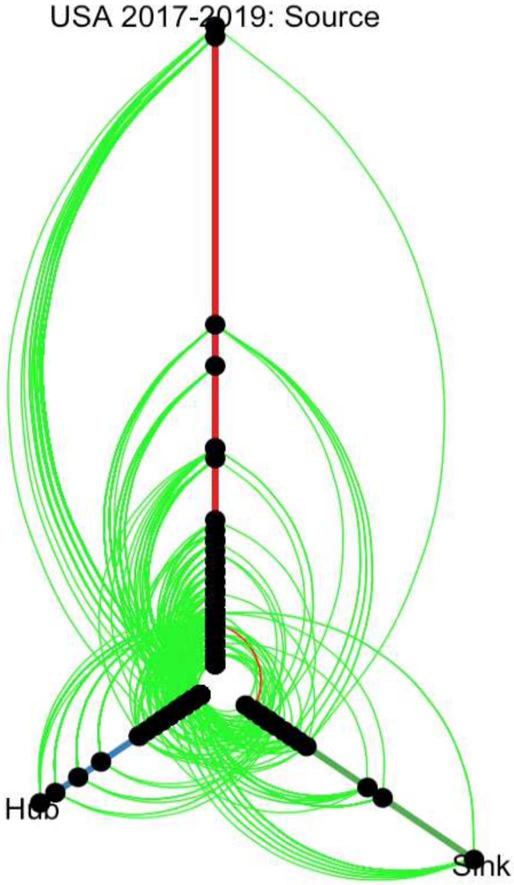


Figure 6.23: Network visualisation of the US quantum internet patent citation network for July 2017 - June 2019.

The below table collects the test statistics for assortativity for all three variables Country of Patent Publication, Applicant Type, IPC clustering for period 2, July 2017-June 2019.

Variable	Assortativity a
Country	-0.03431128
Applicant	-0.0436879
IPC	0.01426039

Table 6.20: Assortativity covariates of the US quantum internet patent network July 2017 - June 2019.

There are minor variations compared to the previous period.

The ERGM for period 2 is as follows.

Variable	Estimate	Std Error	MCMC %	z-value	$P > (\|z\|)$
edges	-6.1385	0.0264	0	-232.522	<1e-04 ***
nodematch.Country	-0.4761	0.2089	0	-2.279	0.0227 *
nodematch.Applicant	-1.4174	0.2249	0	-6.303	<1e-04 ***
nodematch.IPC	-3.9958	0.4284	0	-9.326	<1e-04 ***
mutual	-0.7264	0.9367	0	-0.775	0.4380
gwesp.fixed.0.4	2.4879	0.2322	0	10.714	<1e-04 ***

Table 6.21: ML test statistics for the ERGM of the US quantum patent network July 2017-June 2019.

All variables are found to be significant, albeit ‘Country’ comes back with a reduced confidence level of *.

And finally, calculating the probabilities from the log-odd changes for the significant values produces the following probabilities of citation formations.

Variable	Probability P
Edges	0.002153511
Country	0.3831735
Applicant	0.1950695
IPC	0.01806054

Table 6.22: Probability estimators of the US quantum patent network July 2017-June 2019.

In this period, country-to-country clustering has the biggest effect. When US-headquartered organisations file new quantum patents in the same country, their chance of forming a citation link is a whopping 40 percent. Applicant-to-applicant assortativity translates into a chance for a tie formation of nearly 20 percent.

The goodness-of-it statistics are as follows. The ERGM for the US for period 2 is the best fit so far.

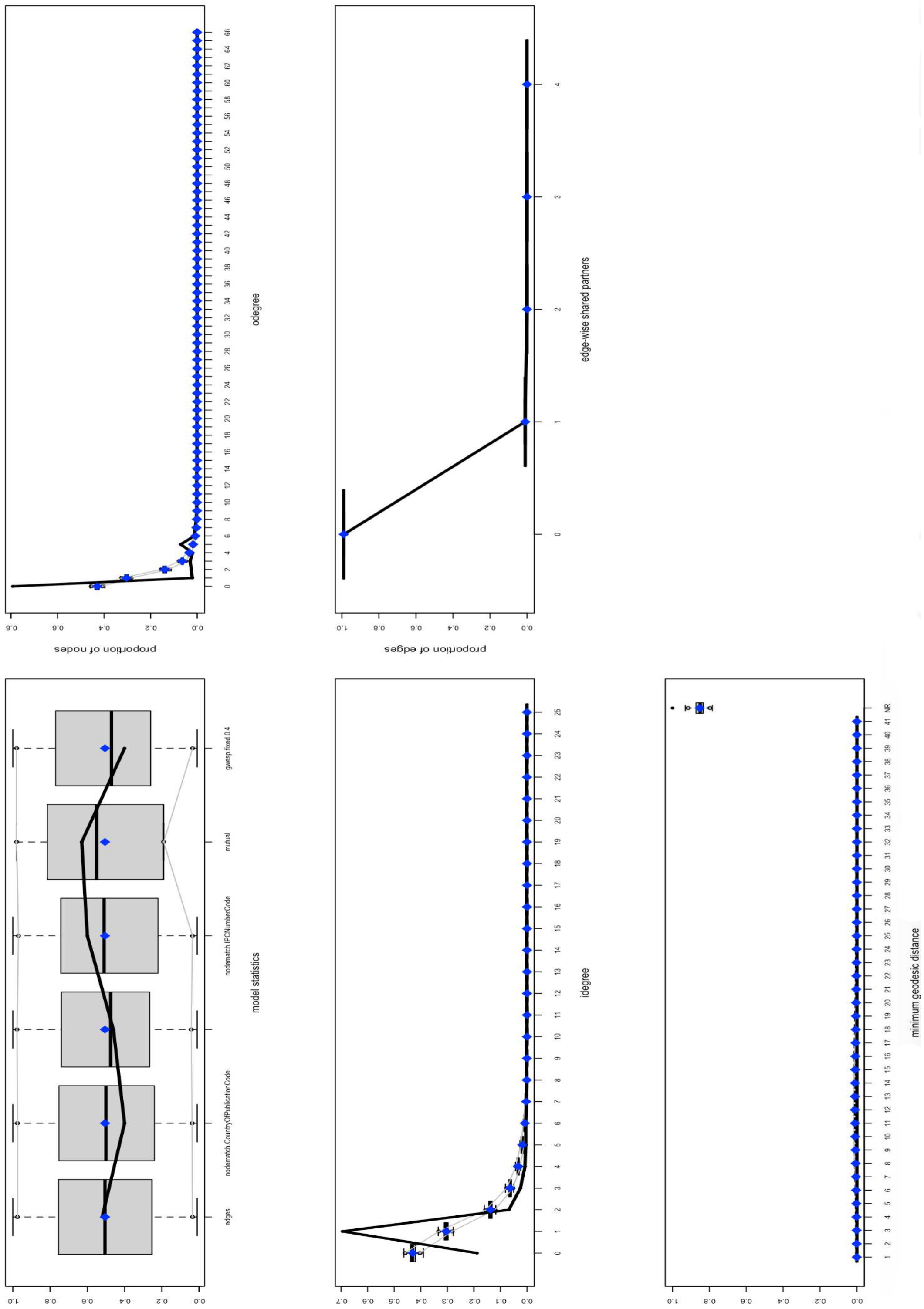


Figure 6.24: Goodness-of-fit parameters for the US ERGM July 2017-June 2019.

Period 3: July 2019 - June 2021

US activity in this period has gone down. The subnetwork contains 992 nodes that span 936 edges. Its density is 0.0009521174, and the network is plotted below.

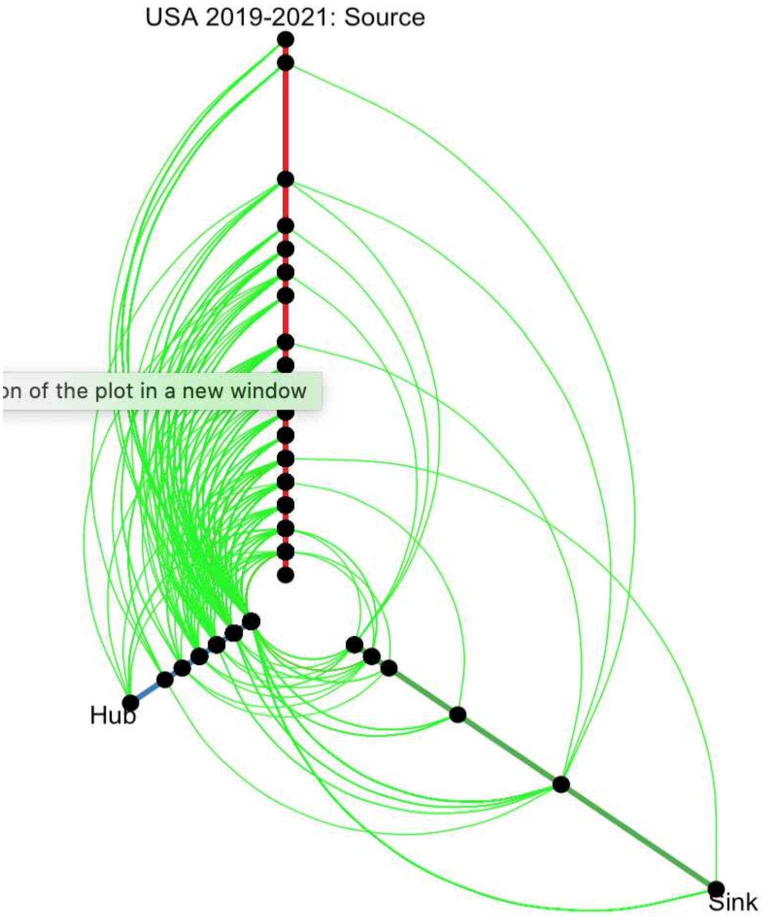


Figure 6.25: Network visualisation of the US quantum internet patent citation network for July 2019 - June 2021.

Once again, the below table collects the test statistics for assortativity for all three variables Country of Patent Publication, Applicant Type, IPC clustering for period 3, July 2019-June 2021.

Variable	Assortativity a
Country	-0.07555183
Applicant	-0.02450686
IPC	-0.02641583

Table 6.23: Assortativity covariates of the US quantum internet patent network July 2019 - June 2021.

There is minor negative co-movement in the data for this period.

The ERGM for period 3 is as follows.

Variable	Estimate	Std Error	MCMC %	z-value	$P > (\|z\|)$
edges	-5.94808	0.03401	0	-174.907	<1e-04 ***
nodematch.Country	-1.18942	0.38665	0	-3.076	0.0021 **
nodematch.Applicant	-1.84373	0.34218	0	-5.388	<1e-04 ***
nodematch.IPC	-3.75748	0.84924	0	-4.425	<1e-04 ***
mutual	-Inf	0	0	-Inf	<1e-04 ***
gwesp.fixed.0.4	2.26867	0.39543	0	5.737	<1e-04 ***

Table 6.24: ML test statistics for the ERGM of the US quantum patent network July 2019-June 2021.

All variables are found to be highly significant predictors of US patenting activity with significant evidence of clustering. Calculating the probabilities from the log-odd changes for the significant values produces the following probabilities of citation formations.

Variable	Probability P
Edges	0.00260405
Country	0.2333627
Applicant	0.1366107
IPC	0.02281005

Table 6.25: Probability estimators of the US quantum patent network July 2019-June 2021.

Country-to-country and applicant-type clustering prove once again the strongest predictors of patent citation formations for this final period under consideration.

Finally, the goodness-of-fit for period 3. Once again a very solid fit.

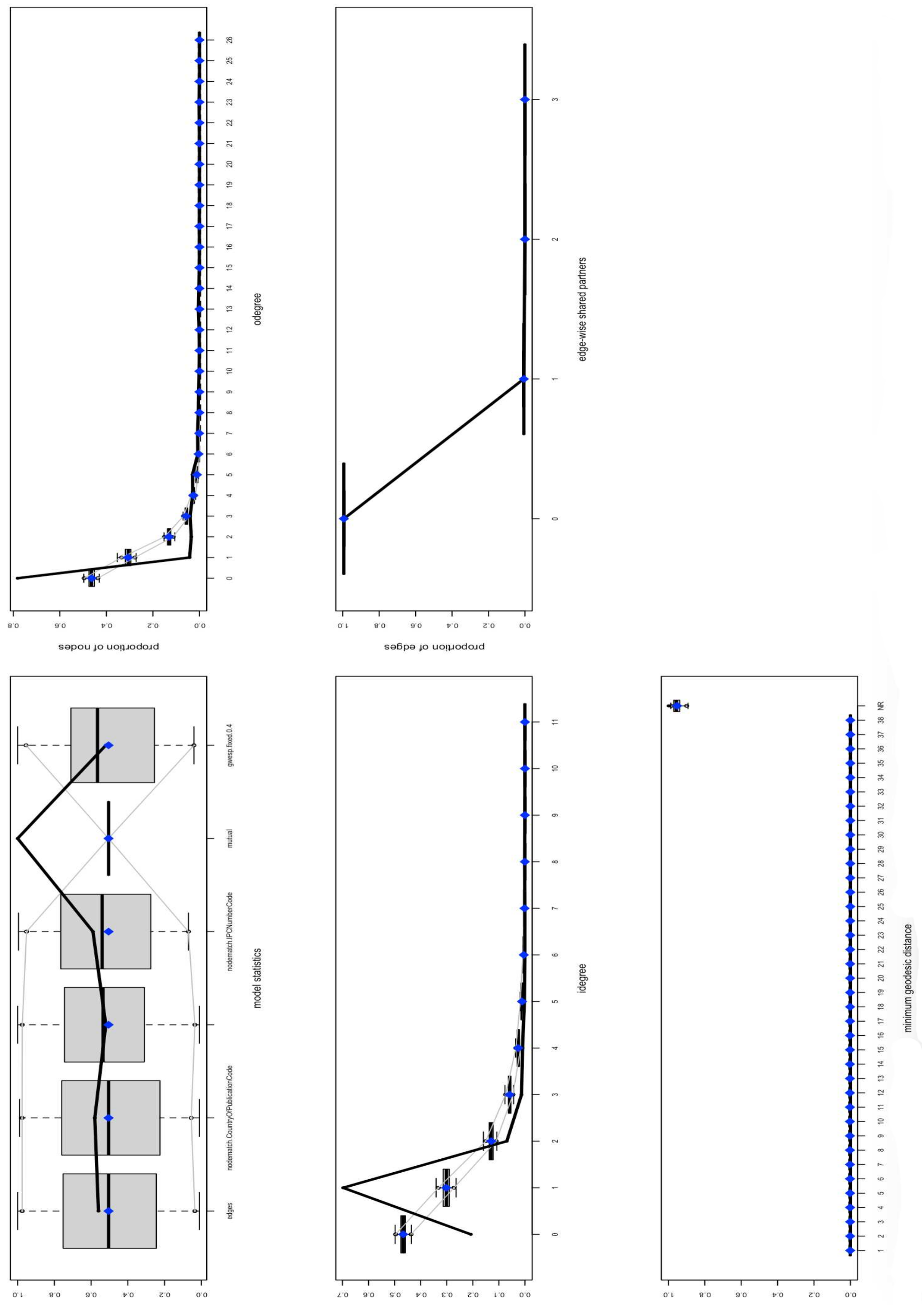


Figure 6.26: Goodness-of-fit parameters for the US ERGM July 2019-June 2021.

6.4 Main points of Chapter 6

This chapter has first collected descriptive statistics regarding the Chinese and US patent citation networks. These statistics show some striking similarities, most significantly in terms of siloed, or independent, research activities. In patenting the technologies for building the quantum internet, both superpowers wish to acknowledge only domestic technologies: Chinese inventors would only cite Chinese technologies as prior art; a phenomenon that is, perhaps surprisingly, even more pronounced in the US where the citation network is almost exclusively domestic in its trajectory. Put differently, in their quantum internet patenting activity, organisations headquartered in the US, either public or private, claim that foreign inventions (patents registered by non-US entities abroad) do not shape at all US efforts to build the quantum internet.

The comparison of descriptive statistics was complemented by estimating a regression model for plausible variables of significance. In dividing the data into three time periods for both the Chinese and US data for ease of comparison, the ERGMs so developed have found that the country of filing, the type of organisation that has registered a new patent, and the way the patent has been classified following the IPC classification tree, are all highly significant predictors of strategic quantum patenting activity. The implications of these findings are developed in more detail in the following chapter.

Network statistics:

6.a The chapter has analysed 4,200 patent family records in the domain of quantum internet technologies (and the 10,000+ other patents they cite as ‘prior art’). The data was retrieved from the EPO’s GPI. The data range is seven years, 2015-2021. The raw dataset contains all new patents that were registered by entities that are headquartered in the US or China. The data was split into US and Chinese subsets.

6.b By count of newly registered quantum internet patents between 2015-2021, the top two registering applicants were IBM and Intel, multinational companies headquartered in the US, followed by TCL Corporation, a Chinese consumer electronics company headquartered in Huizhou. Places 7-10 also go to Chinese organisations.

6.c At the start of 2022, China dominated the patenting landscape and outperformed the US by a magnitude of 4 in terms of annual patent registrations. While the big players are American, China has successfully developed a large number of small to mid-sized entities that register quantum patents at significant pace.

6.d The dataset was transformed into a network object in which registered patents are nodes, and edges describe a citation link between them. If node A has an outward edge to node B, A cites B. An incoming edge therefore means ‘being cited’. The quantum internet patent citation network is a directed graph.

6.e The Chinese quantum internet patent citation network 2015-2021 is made up of 6,134 nodes and 6,970 edges, with radii spanning from 1 to 27 (where radii capture the number of edges that point to/from the node).

6.f The US quantum internet patent network for this period connects

2,863 nodes over 3,201 edges, with radii spanning from 1 to 63.

6.g The analysis reveals a strong preferential treatment for domestic technologies in both the US and Chinese citation networks. New patents registered by entities headquartered in China between 2015 and 2021, if relevant to building the quantum internet, overwhelmingly cite patents that were registered at a Chinese patent office. New patents registered by entities headquartered in the US between 2015 and 2021, if relevant to building the quantum internet, overwhelmingly cite patents that were registered at a US patent office.

6.h The chapter collects several further indicators: mean degree, density, transitivity, diameter, mean distance, the number of components and the size of the largest components.

6.i The Chinese network has more than double the number of unitary nodes that cite only one other patent or are being cited by only a single invention. This means that in the Chinese network, the number of patents that do not gain much traction is nearly one hundred percent higher compared to the US network.

6.j The Chinese network contains two large components (complete subgraphs) of around 2,000 nodes each; the remaining 338 components are of size 2 to 20. This is evidence for two separately evolving research programmes in China. If this is due to strategic separation or accidental due to ignorance is not in the data.

6.k The US network looks different. It contains a single-biggest component of 1,589 nodes followed by a dozen or so smaller subgraphs that range between 10 and 38 vertices, and a vast trail of dyads. This suggests a more unified and coordinated approach in that the US quantum research programme seems to be one big project that draws on the same sources of prior research.

6.l The Chinese quantum patent citation network has a unique core for $k = 5$, meaning that there is a unique subnetwork of 13 nodes that constitutes the stable kernel of the network. Removing only these 13 patents would collapse the entire Chinese quantum internet patent citation network.

6.m The US has a unique core for $k = 4$, which contains 18 nodes. Removing only these 18 patents would collapse the entire US quantum internet patent citation network.

ERGMs:

6.n For the purpose of estimating and comparing internal factors that drive citation behaviour, ERGMs were built for three time periods: July 2015- June 2017, July 2017-June 2019, and July 2019-June2021.

6.o It was hypothesised that the country of filing (China, Germany, Spain, the UK, Japan, South Korea, the US and 'World'), the type of organisation that registers patents (industry, private individual, university or research institute, military, other) and the number of IPC codes that classify patents have predictive power for US and Chinese patenting activity.

6.p All six subnetworks have a density of < 1 percent. This means the chance that any two randomly picked nodes will stand in a citation relationship is less than one percent. This is the baseline for the comparison with ERGM test results.

6.q The picture changes dramatically when two nodes have the above attributes in common. The tables below collect the ERGM probability estimators for the Chinese and US patent citation networks.

China:

China	**2015-2017**	**2017-2019**	**2019-2021**
Edges	0.0023	0.0008	0.0011
Country	0.1333	0.2557	0.1889
Applicant	n/s	n/s	0.3351
IPC	0.014	0.03	0.0332

Table 6.26: Summary table of ERGM probability estimates for China for the three time periods under investigation.

USA:

USA	2015-2017	2017-2019	2019-2021
Edges	0.004	0.0022	0.0026
Country	0.1583	0.3832	0.2334
Applicant	0.1689	0.1951	0.1366
IPC	n/s	0.0181	0.0228

Table 6.27: Summary table of ERGM probability estimates for the US for the three time periods under investigation.

Chapter 7

Discussion

The purpose of this chapter is to discuss the findings of Chapters 4, 5 and 6 in response to the research questions developed in Chapter 1 and the literature developed in Chapter 2. Chapter 4 has outlined the basic characteristics of quantum computing and quantum communication, and covered the technical dimensions of a quantum internet. With a view to the intensifying strategic competition between the US and China, Chapter 5 has analysed a corpus of interview data to map the challenges that internet governance is facing in the 2020s. Chapter 6 has built an empirical analysis of a dataset of 4,200 patent families and their 10,000+ citation links in the quantum internet domain.

This chapter, then, in Section 7.1 first revisits the research questions before it moves on to discuss, in a conversation around QISG, important findings in more detail. Section 7.2 speaks to the topic of US–Chinese strategic competition and the future of the internet under the following themes: Chinese ambition, the protection of quantum IPR, quantum internet standards and securitisation, the role of big tech and the complexification of the strategy landscape, how 'New IP' should be construed a precursor to a fragmented quantum internet, and how the quantum internet introduces new dependency risks for the UK.

Section 7.3 focuses on the evidence from patenting activity for a discussion of the quantum internet. It considers the issues of quantum big tech vs smaller firms, how the US and China give significant preferential treatment to domestic industries, and discusses some summary statistics as well as the empirical drivers of quantum patenting in both countries.

Section 7.4 discusses quantum internet fragmentation and strategies to avoid it. It presents an outlook and the building blocks of a model for quantum internet standard finding. In light of the discussion, which finds evidence for two separate quantum internet research programmes in the US and China, the section introduces a transferable utility game to develop options for quantum internet governance. The model recommends the US make side payments to China for its leadership to shelve 'New IP' and agree to a shared global standard instead, a framework that ensures the interoperability of the quantum internet. Finally, Section 7.5 collects the major takeaways of this chapter.

7.1 Recap: the research questions

In Chapter 1, the following overall research question was developed:

> **R.1** How is the quantum internet being shaped by US–Chinese competition?

In order to operationalise this question, it was broken down into the following two subquestions:

R.1.1 What do domain experts observe regarding US–Chinese competition in internet governance?,

and

R.1.2 What do patent data suggest about US and Chinese activity in building the quantum internet?

The Methodology chapter has laid out further auxiliary queries that the engagement with R.1.1 and R.1.2 invites, these are

#	Auxiliary queries
AUX.1	What is a quantum internet?
AUX.2	What does internet governance presently involve?
AUX.3	Can the multi-stakeholder model of internet governance survive?
AUX.4	Who is involved in building a quantum internet?
AUX.5	Does China enjoy a leadership position in quantum internet engineering?
AUX.6	Is there evidence for competing quantum technology clusters developed in the US and China?

Table 7.1: The auxiliary queries that this thesis pursues in response to R.1.1 and R.1.2.

Embedded in a discussion of the literature, Chapter 2 has developed the concept of *quantum internet security governance*, or QISG: a heuristic device for mapping processes of multi-actor involvement in the emergence and control of security and governance practices around quantum networks. QISG invites a way of thinking the togetherness, or ‘coproduction’ (Jasanoff 2004, 2016, Jasanoff & Kim 2015) of technology and the practices that will govern the quantum internet. Studying the quantum internet through the lens of QISG is to aim for larger political tropes that surround the emergence of the next generation of the internet.

The findings of Chapters 4,5 and 6 attest to the involvement of 'multiple and separate authorities, interventions by both public and private actors, formal and informal arrangements' (Kirchner & Sperling 2007, p. 3), all of which are key characteristics of the concept of securitisation. In the coproduction of the quantum internet and the governance regimes for the internet of the future, the quantum internet is already being framed in security terms well before its arrival. The following sections develop responses to R.1.1 and R.1.2 against a QISG framing, i.e. with a view to international security and the competition between the US and China, and how these dynamics shape the quantum internet. The Conclusion (Chapter 8) addresses R.1 overall.

7.2 US–Chinese strategic competition and the future of the internet

The discussion below is grouped into the following themes: i) Chinese ambition, ii) arguments for better protecting Western IPR and how the Western intelligence community places little value in quantum communication, iii) how the quantum internet is being 'securitised' as defined in Chapter 2 even before it is built, iv) how big tech creates strategic concerns for China, v) why China's 'New IP' should be construed the precursor to the architecture of a quantum-enabled internet, and finally, vi) how the quantum internet is likely to create new dependency risks for the UK.

7.2.1 Chinese ambition

The interview data analysed in Chapter 5 suggest that the Chinese leadership recognises the US as its chief strategic rival. While China has traditionally considered Europe a political block in its own right, it now believes that Europe will side with the States in the event of a military conflict between the two superpowers. Informants suggested that China hopes to drive a wedge between the US and its Western allies to keep American planners preoccupied; continuous disagreement among European leaders supports Chinese ambition, a respondent said. For China, Europe's institutions have deteriorated to the point that they are now 'hopeless'.

The interviews further suggest that China has moved away from cooperation so that dialogue on emerging technologies has nearly become impossible. China has grown much more assertive, aggressive even, under President Xi Jinping. The rivalry has intensified to a degree that it will be very difficult for any state actor to circumvent US–Chinese conflicts over the standards and governance models for the internet of the future.

For China, shaping the quantum internet means making the internet a more efficient surveillance-and-control system: a network that serves first and foremost Party interests. An advanced internet with quantum capabilities may facilitate surveillance tasks that have traditionally been carried out by human operators, respondents found. A future internet run on Chinese standards would displace human personnel that is presently tasked to oversee and implement domestic control regimes. This way, the quantum internet is a piece of the puzzle that is the wholesale automation of surveillance. Given the deep levels of distrust towards the US, China's leadership seems convinced it can only trust a genuinely Chinese technology, independently developed, to achieve this task. This is one the reasons why China would seek to dominate emerging technologies, in particular quantum internet technologies.

Control over quantum technologies, both in terms of ownership of actual hardware as well as the capability to oversee their standards for implementation, would also support the Party in pushing back against domestic big tech corporations (and their owners) from gaining too much influence over Party politics. To an important extent, informants found, projecting dominance abroad also helps keeping the lid on potential threats to the Chinese leadership at home.

Ultimately, it was suggested that the Party is determined to maintain its position as the ultimate *data sovereign.* Sitting at the top of the 'trust pyramid', it requires absolute control over the internet: no group in China, neither businesses nor individuals, must be able to collect, store and analyse data in ways that restrict or outright exclude Chinese authorities. As there can be no data sovereign above the Party, internet technologies must be designed and governed in a way that accommodate Party oversight. One respondent expressed sympathies for this position–the problem of data privacy (or lack thereof) is considerable among Chinese businesses, and the Chinese leadership might be quite right to mistrust China's big tech companies to handle the issue well. The Party had pushed for big tech's success in the past, mainly to counter US global dominance, but now finds itself facing new and powerful internal rivals as a result of this.

This is why it must be assumed that quantum communication technologies are immensely important to the leadership, the interviews find. A genuinely Chinese technology such as QKD could be trusted by the Party and the security apparatus to get the paramount task of domestic surveillance right while also being a big reputational asset. Having developed such a game-changing emerging technology may also support building trust in Chinese quantum technologies abroad as well as among the general population at home.

The empirical findings in Chapter 6, further discussed below, support the views of the informant in Singapore that China does indeed enjoy an edge over its strategic rival. A Chinese quantum internet would be a ‘game changer’. For the informant in Singapore, the West has not ‘kept up with the game’. Countries like Singapore need to balance carefully their relationship with China for many reasons, the possible repercussions of a conflict in the South Asian Sea being of particular concern. While some commentators suggest China is more rule-compliant regarding its conduct in the South China Sea than Western narratives would like to accept (Raymond & Welch 2022), there is considerable unease in the region about the potential impact of Chinese quantum capabilities. However, the informant also notes that in the US, research that directly relates to encryption ‘falls under the purview of the NSA’. It is certainly a possibility that classified research is being carried out that will not find reflection in patenting data, or at least not in the near future.

7.2.2 Protection of quantum IPR

Western intelligence services, according to GCHQ, align on their assessment that the direct security threat of a Chinese quantum internet, secured by QKD, is manageable. Their assessment has shaped the UK’s official policy position. The respondent in the Government argued that because QKD is not a genuine threat, according to GCHQ, the most important issue that arises from quantum innovation is to protect British quantum IPR.

The Chinese leadership has certainly gained notoriety for its relaxed, if not outright supportive, approach to industrial espionage (Lindsay 2015). The UK Government seems to assume that China still operates a model of simply wanting to copy Western technologies. Arguably, China has moved on from this, in particular in the domain of quantum internet technologies. It has overtaken the US in registering patents across various subdomains, as found in Chapter 6 and discussed in more detail below. This is not to suggest the UK Government should ignore threats to British IPR, but it should note that industrial espionage is likely to become less relevant for Chinese businesses and the state should the Chinese quantum research programme continue to progress well. It could be too soon to outright dismiss QKD and quantum communication.

The public has come to expect new internet technologies to be commercially successful, the interviews suggest. No one would seriously think that AI, for instance, should be 'under strict military control', as one informant put it. The somewhat unquestioned assumption among politicians, researchers and the public alike is that the technology for the internet of the future will be developed by the private sector. Governments, then, hope to (re)vitalise entire domestic industries on the back of emerging technologies such as quantum.

The focus on IPR, at the expense of security concerns around quantum communication, creates obvious tensions. At the time of interviewing, the UK Cabinet Office expressed their discomfort about banning all Chinese foreign direct investment as it can help grow Britain's quantum sector. The interviewee pointed to the need to find 'the right balance'. Given that the 'US have a lot more people, and a lot more money than we do', the UK, just like the rest of Europe, is dependent on US leadership in quantum technologies. It is these delicate dependencies that

China seeks to upset, other respondents point out. Tensions between the US and its European allies serve Chinese interests.

This sentiment was echoed by GCHQ whose official agreed that ‘you might have a problem’ if China can build a quantum computer ahead of the West, one which generates sales and captures business investments into new IT systems. However, as far as actual use cases of quantum communication go, in particular those of QKD, the British government and the intelligence community see little value in them. In terms of actual capability, for GCHQ, as mentioned, ‘QKD just doesn’t address 90 percent of the actual problem space for government’. However this still leaves a sizeable 10 percent for a potential attack surface, which could prove a wide enough opening for adversaries to capitalise on. For the time being, there are better ways to protect against, say, phishing attacks, GCHQ pointed out. But QKD will become a problem from the moment strategic rivals begin to use it, whether or not Western alliances consider it a good and efficient technology.

7.2.3 Quantum internet standards and securitisation

For GCHQ, the problem of a Chinese quantum communication system is manageable because quantum-proof encryption models have been found that will translate into new internet standards: ‘wait for the scientists to do their job and say, we now recommend this new set of algorithms for quantum systems, then the standards will start to appear from global standards bodies that control the internet and telecoms networks’, the respondent said. The assumption that new internet standards that GCHQ finds agreeable will somehow naturally manifest is surely informed by tradition. The US has enjoyed a very privileged position in setting internet standards, as discussed in Chapter 2. At present, however, pushback is building up. China can influence standardisation bodies much more effectively than it used to. The road to standards that meet the expectations of GCHQ could prove rockier than the intelligence service assumes.

Particularly the ITU has attracted increased attention.

> '[China's] expanded presence and influence is manifest in the ITU. Houlin Zhao is completing his second term as Secretary-General. During his tenure, he has deepened and institutionalized ties between the ITU and Beijing, endorsed the Belt and Road Initiative, and increased Chinese employment in the organization. China also sends the largest delegations to ITU study groups and has flooded them with proposed specifications and contributions. China leads all nations with SEP applications. The goal is to make Chinese standards global standards and thereby give Chinese companies greater market share, increased revenues, and the inside track on next-generation technologies' (Schaefer & Pletka 2022, p. 2).

In light of China's progress, for the respondent with considerable experience in internet governance at the United Nations, the current discussion of internet fragmentation should also focus on what she called 'institutional fragmentation'. The respondent found no harmonisation across initiatives. Rather, state actors take aim at organisations and bodies where they can maximise influence and meet minimal resistance, which leads to intense focus on some forums and working groups while others are being entirely neglected. The West and China 'are really in the middle of a fight to occupy this space and have as many supporters on one side as possible', the informant concluded.

Other respondents emphasised just how much the question of standards and governance 'is a very military driven process', not just for China, but for the US also. When it comes to quantum internet standards and a governance model for the internet of the future, in terms of QISG, the quantum internet has been securitised well before its arrival. Chapter 2 has defined securitisation roughly in terms of identifying an object as a threat to (national) security and viewing it primarily through such a lens. Surely a reflection of its time, the quantum internet does not enjoy the kind of honeymoon period of utopian imaginaries of a better future that the internet was able to generate in its early days of commercialisation.

Future internet standards are such an integral element to China's quest to become wholly technologically independent from the US that it has little choice not to securitise the quantum internet in these terms. The interviews provided evidence that spaces for open collaboration and compromise in internet standards-finding are diminishing. Hierarchical 'military driven processes' seem back on the agenda.

Interview data analysed in Chapter 5 also point to a parallelism of state and corporate interests in international governance forums. Skilled individuals, who would oftentimes move between sectors (the chapter has discussed the 'revolving doors' problem in Western regulatory regimes), can build up considerable influence: operating on behalf of big tech companies and entrepreneurs alike, skilled lobbyists manage to capture officials. At international forums, a wealth of interests seek to shape official positions–the process by which GCHQ summarily declares new standards to 'appear' is a deeply contested and complex one.

7.2.4 The role of big tech and the complexification of the strategy landscape

Internet governance has come under increased pressure not only from military and security stakeholders. Big tech also attempts to reshape the internet and Web services to accommodate how they envision their businesses to evolve. Meta's 'Metaverse' is a particular popular buzzword at present. At the Eighth International Conference on Information Management in Cambridge in May 2022, proponents of this 'internet and computer-based, and socially connected networking space of three-dimensional virtual-reality worlds' speculate about 'quantum strategies' that would make a quantum-enabled 'Metaverse' more engaging (Shuliang 2022)–if one is to believe the hype. Imaginaries of fantastical future profits drive lobbying efforts to turn the internet into a virtual reality machine.

For one informant, multi-stakeholderism has always been a nebulous term and is best construed shorthand for accommodating the interests of large US corporations such as Meta–businesses that are heavily invested in building quantum internet technologies. The influence of big tech on US politics has been discussed at length. From an IR perspective, one major theme is the blending of corporate and public interests for the projection of power. Some commentators argue that big tech 'implicates core IR research in two ways: (1) it creates new private authorities as corporations control critical bottlenecks of knowledge, connection, and desire; and (2) it mediates the scope of state-corporate relations as states become dependent on Big Tech, Big Tech circumvents state overreach, and states curtail Big Tech' (Srivastava 2021). As a concept, QISG sits well with this body of critical analyses of the coproduction of corporate power and public policy.

Chapter 5 has discussed how big tech can become 'an alternative source of power' that threatens democratic principles. The scale of influence of big tech on US politics is being observed in China with acute interest. While one could imagine that corporate challengers to principled policymaking in the US would find implicit support from the Chinese leadership in the hope of destabilising the US government, in reality the picture is much more complicated. Rather, the Chinese leadership seems wary that big tech could be a threat to government. If US big tech can challenge the American system of government, Chinese big tech may very well also emerge as an alternative source of power and a challenger to Party dominance at home. Chinese big tech must therefore be contained while giving it enough leeway to help realise the quantum technologies the Chinese state demands, and for them to contribute to economic growth.

Moreover, the traditional view among top Chinese officials is that in international negotiations, state actors should deal with other state representatives. There is unease among Chinese leaders that dealing with big tech complicates diplomacy and makes strategic planning more difficult. Interview participants suggested that China would rather the US curtail big tech as this would reduce the complexity of the strategy space and limit the range of agents China needs to grapple with. Anything that reduces the complexity of the chief rival's decision-making processes is tentatively good news.

As Chapter 2 has discussed, in the current emerging technology race, actual technological affordances matter just as much as working out how an adversary may want to act on them in the future. Should the US decide to confront corporate power in a more robust fashion, it would mean fewer variables for the Chinese Communist Party to factor in. The smaller the number of actors it has to consider, and the more limited their range of interests, the more effectively China can influence internet governance models in the years to come.

While the list of the top ten registering entities of quantum internet technologies include TLC Corp at third place, as Chapter 6 has found, China's leadership position in registering new quantum patents at scale is due to the fact that since 2015, it has grown a sizeable ecosystem of quantum SMEs. From a Party perspective, it is not far-fetched to imagine that a large number of small companies is hoped to be easier to manage than yet another corporate giant. Empirical work on Chinese corporate power certainly confirms that 'monopolised platform economies' have a tendency to dominate smaller businesses and, importantly, they may increase 'income inequality, exacerbate overcapacity and generate financial instability' (Li & Qi 2022); complications the Party is keen to avoid in the current global economic climate.

7.2.5 'New IP': a precursor to the quantum internet

Since 2019, Chinese delegations with representatives from Huawei, China Mobile, China Unicom, and the China Ministry of Industry and Information Technology have made several high-level proposals at institutions such as the ITU to fundamentally reform internet architecture and protocols. These efforts have come to be summarily known as 'New IP'. The most relevant technical details of 'New IP', as far as they are available, have been presented in Chapter 5.

It is important to discuss 'New IP' in the context of QISG as the Chinese proposals provide a good indication of the direction of travel were China to be able to significantly shape the standards for the internet of the future. Many commentators argue that the TCP/IP suite of communication protocols is insufficient for the next generation of the internet that connects autonomous vehicles, wearables and multiple devices at home (see Chapter 2). However, it should be noted that one of the respondents interviewed for this thesis disputed this. Moreover, considerable work is being done at present to find IoT standards over IP as it exists today. 'Matter' is a standard that was launched in October 2022 that specifically covers connectivity issues in 'smart' homes (Hill 2022). However, the narrative that TCP/IP is hopelessly outdated seems to have captured a critical mass of commentators and stakeholders.

'New IP' addresses the demands of autonomous vehicles and the radical connectivity that the IoT demands but is dismissed by ICANN as the nail in the internet's coffin: essentially turning the open internet into several subnetworks that are linked (or decoupled) over various access points, 'New IP' introduces a great many new opportunities to monitor user behaviour, identify (and block) users at the basic infrastructural level, or switch off undesirable subnetworks without compromising the functionality of the rest of the network–the respondents to this thesis agree that 'New IP' would amount to no less than the kind of fragmentation of the internet at the infrastructural level that some commentators warn against (O'Hara & Hall 2018). The informant at the internet standardisation body considers 'New IP' a 'danger to the internet itself' as the protocol suite would amount to 'a bifurcation in the network [to the effect that] certain nodes won't be able to talk to other nodes any longer'. The internet would be iteratively replaced by a 'many nets' architecture (this is how the designers of 'New IP' had named their approach to systems design).

A many-nets approach to reforming internet architecture is one way to prepare the grounds for a quantum internet. Splitting up the internet into a set of subnetworks that connect via gateways can make the maintenance and upgrading of critical parts of the internet's infrastructure easier, or secure highly critical subnetworks better–for example, with quantum communication protocols. Rather than adding a quantum layer to the internet as it exists today, first-generation quantum networks, probably highly exclusive in character and for government and intelligence services only, could be mapped onto an internet subnetwork and thus be sandboxed.

As far as it is possible to tell from the high-level outlines of 'New IP' that are available, while coming at considerable cost in terms of accessibility and privacy, the proposal seems to have the potential for added security and stability at the level of fundamental transport layers. Gateways can be closed so that if a subnetwork is damaged or compromised it can be switched off easily without threatening the integrity of the entire network. 'New IP' must be considered a precursor to the ways in which China envisions the implementation of the quantum internet. Quantum capabilities could be made available to selected subnetworks only, effectively splitting the internet into a classical network and quantum-powered one. A *'New IP quantum internet* would connect to the rest of the network via strongly policed access points.

At closer inspection, most advantages of 'New IP' have a strong surveillance element to it. The idea that the internet should fragment into subnetworks that governments find easy to switch off, on top of a strong binding between user identity and the subnetwork through which they can access the internet in the first place, alarms observers. Informants to this thesis spoke of new roadways into discriminatory packet pricing and, above all, unprecedented opportunities for surveillance at a much more granular level than is possible today.

China's 'New IP' model has not yet been discussed to great extent in the literature. As far as the opinions are concerned that find reflection in publicly available material–an informant suggested that a classified white paper is being circulated among Western diplomats that warns about 'New IP'–the interviews add to the deep scepticism about the new protocol that, for instance, ICANN has formulated (Durand 2020). The discussion in Chapter 5 adds to this debate in that it relates 'New IP' to the quantum internet. It would be implausible for China to be pushing for 'New IP' to the extent it currently is, only to backtrack once the quantum internet fully arrives. This outlook would make the quantum internet not an open, general-purpose technology that makes the internet better for everyone but paints a vision of the quantum internet as tightly integrated with policies of surveillance and control.

The interviews further suggested that the struggle over the technology and the governance model for the internet of the future reaches well beyond governance as such. In terms of QISG, internet governance conflicts between the US and China are also a signalling game aimed at the rest of the world. Quantum internet advantage seeks to portray leadership and strength. Leadership in emerging technologies, on the other hand, signals trustworthiness and promises returns if other nations align and forge new alliances. In this context, Chapter 2 has discussed the notion of 'quantum patronage' that QKD could potentially offer to previously non-aligned state actors, e.g. in terms of exclusive licencing deals. Pushing ahead with quantum internet technologies is a bigger game that extends the narrow confines of standard specifications.

It is safe to assume that the Chinese leadership does not expect the rest of the world to embrace 'New IP' and rebuild the internet accordingly. What 'New IP' has already achieved, however, is to show the world that China is a serious contender: a player not only at the cusp of building a radically novel network technology but also being able to offer a blueprint for implementing a new vision of the internet with ample surveillance tools inbuilt–quite possibly a sweet offer for many authoritarian regimes around the world.

7.2.6 The quantum internet: new dependency risks for the UK

Respondents to this thesis expressed excitement at the prospect of a quantum internet; 'there is genuine momentum now', one informant confirmed. No participant considered the quantum internet an outright replacement for the 'classical' internet. Rather, a quantum network will add new capabilities. But what kind of services could the quantum internet provide, and who would offer them?

Interviewees expressed concern about the quantum internet potentially exacerbating the problem of increased market concentration among cloud service providers. In many instances, internet infrastructure is built to accommodate big tech, such as undersea fibre cables owned by Meta, Microsoft and Google. An article published in late 2021 in the magazine *Wired* presents the following summary assessment:

> 'The world's biggest owner of cables is a household name, at least to Americans–it's AT&T, which has a stake in around 230,000 kilometres of international internet cabling, or around one sixth of the total. But looking at others in the top ten reveals why both Big Tech and West-

> ern governments are starting to pay the apparently dull issue of cable ownership more attention: in second place is China Telecom, while Chunghwa Telecom (based in Taiwan) is third and China Unicom is sixth.
>
> In the tenth and eleventh spots, however, are some very familiar names: Facebook and Google. Big Tech is getting into big cables–and doing so in a big way. Over the past few years, 80 percent of investment in new cables has flowed from the two US tech giants. As of today, Facebook owns or co-owns 99,399 kilometres of cables, Google 95,876 kilometres' (Ball 2021).

Companies that already dominate Web services, in particular cloud storage and social media, are beginning to hold considerable leverage at the infrastructural level too. Moreover, interviewees pointed to the fact that many SMEs, and even bigger companies, find it increasingly difficult to build and maintain intranets. Internal systems are becoming ever more complex and are therefore expensive to build, and skilled engineers to maintain them are difficult to recruit and retain. For this reason, a lot of company data gets uploaded onto the cloud. The companies mentioned above own a growing share of the internet's infrastructure and invest heavily into the development of the quantum internet too.

Cloud services have quickly become critical infrastructure for UK businesses as well as the public sector. The term 'cloud' usually comprises three delivery segments: infrastructure as a service, platform as a service, and software as a service. While global overall spending on cloud services was over $400 billion in 2021 (see graph below), the cloud computing market in the UK was around $16 billion with 44% of the UK population using cloud storage (Vailshery 2022).

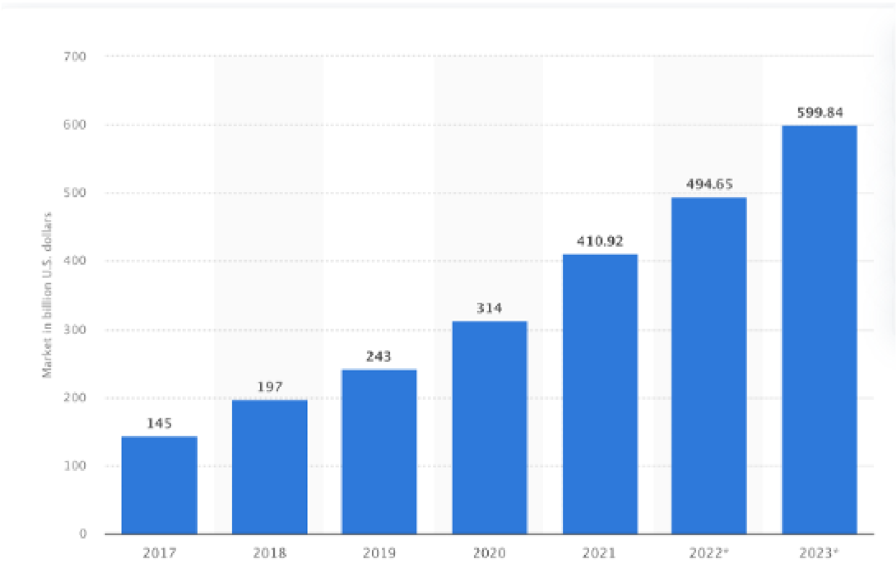


Figure 7.1: Public cloud services end-user spending worldwide from 2017 to 2023 (in bn US dollars). Source: (Vailshery 2022)

The US Department of Commerce estimates the UK market to be the largest in Europe (Administration 2021). They find that the UK is home to 3,000 software companies and is the world's second largest ICT market after the US in terms of spending per head. However, the market is dominated by three US companies (Amazon Web Services (AWS), Microsoft Azure and Google Cloud). This has introduced system-critical dependencies for the UK on foreign suppliers which establishes long-term, structural risks to the British economy. The issue is amplified by indications that cloud service providers follow an increasingly reactive pricing policy to lock in customers (Nazareth & Choi 2021).

The empirical findings of Chapters 4 and 6 indicate that many of the companies that dominate the cloud service market are investing heavily in the development of quantum networks. The initial offering of a quantum internet would be what may be called Quantum Computing as a Service (QCaaS). Given the scale of investment needed to build and service quantum computers and the auxiliary infrastructure required, such as large cooling devices, it is likely that many public and private sector organisations are going to want to rent quantum services over the cloud instead of building sophisticated facilities for providing quantum compute resources in-house. The big promise of QCaaS, secured with QKD, is cybersecurity. In the words of a renowned scientist involved in building the quantum internet, ‘people at the server are unable to know what kind of program you’re running and the data you have’ (Castelvecchi 2018).

QCaaS is likely to generate significant demand from the public and private sectors in the UK. Three areas of application seem particularly relevant.

Public bodies can store sensitive information securely

Personal and sensitive information such as NHS and HMRC tax records can be held securely with great levels of confidence against cyberattacks for many decades to come. With cyberattacks on public bodies significantly on the rise (Schwartz & Montfort 2022), QCaaS could help ensure long-term compliance with privacy regulation.

Secure online banking

Banks and financial services are likely to move to secure quantum communication networks for transaction and clearance purposes, and the storage of customer data, a consultancy business claims (Dietz et al. 2020). Large banks have begun to recruit quantum engineers and quantum physicists for the purpose of exploring opportunities of secure internal communication and the exploitation of future quantum computers for asset pricing. With a quantum-secured backend, the chances of third-party hacking into retail banking accounts are hoped to be low, with the potential to make the requirement for Multi-Factor-Authenticication (MFA) obsolete.

Domestic R&D is protected against foreign industrial espionage

Estimates suggest that British businesses lose up to the equivalent of three percent of GDP to industrial espionage and the theft of trade secrets each year (Searle 2021). China is of course suspected to be responsible for a large share of this loss. With any cyber-physical system only being as strong as its weakest component, running corporate R&D programmes on a secure quantum server could provide protection against the theft of intellectual property and 'shield' the UK economy against industrial espionage.

While these three points make for excellent use cases, there is a real risk that the quantum internet, proprietary technology from the outset and dominated by US big tech, will solidify structural dependencies of the UK on the US private sector. QCaaS is likely to amplify market-distorting forces in an already uneven playing field that is the cloud computing services market. US dominance in this domain must be expected to cement. Compliance with UK regulation, governance and auditing requirements may be complicated by these developments. An increasingly emboldened US big tech sector that also owns a large part of the internet's infrastructure could prove difficult to influence on grounds of regulatory specifics particular to the UK.

Moreover, large corporations such as Google already dominate both the apps and cloud services markets. This allows them to realise substantial network effects that manifest when more users sign up to a service. A strengthening of their leadership position in the quantum domain via QCaaS may further solidify their stronghold in apps, platforms and social media markets. This may have considerable repercussions for UK consumers, in particular where these markets consolidate further through mergers.

As the interview data in Chapter 5 suggest, the UK is unlikely to be able to build the infrastructure to provide QCaaS at scale to its internal market. While the UK government will surely prefer structural and deeply embedded dependencies on the US over dependencies on China, the degree to which the UK economy would depend on the behaviours of the private sector in the US should be of concern to UK policymakers.

7.3 The quantum internet: evidence from patenting activity

This section presents and discusses the findings of Chapter 6 with a view to the themes that have emerged in the discussion so far. It first considers descriptive statistics of the quantum patent dataset developed in the previous chapter, then discusses the ERGM estimates and what they reveal about the US and Chinese quantum internet technology landscape.

7.3.1 Quantum big tech vs smaller firms

In the first step of the analysis, new patents registered between 1 July 2015 and 30 June 2021 were traced back to the countries where the registering organisation is headquartered. For instance, a US company may decide to file a patent for a particular invention in quantum communication in South Korea. This would give the patent a 'KR' country code.

However, as fully explained in Chapter 6, this is misleading. As this thesis inquires into ownership structures and, ultimately, potential pathways for state actors to influence the development and growth trajectories of the quantum internet, the 4,200 patent family records in the dataset were annotated for the country where the filing organisation is headquartered. In the above example, the patent would then be labelled a US patent, not a South Korean one. The exact locale of filing (in this case, KR) was retained however as it provides valuable information as to the strategy of the filing organisation.

Figure 6.3 in Chapter 6 shows the top ten organisations that have registered relevant patents in the period 2015-2021. The top two registering applicants are IBM and Intel, multinational companies headquartered in the US, followed by TCL Corporation, a Chinese consumer electronics company. By count of newly registered quantum internet patents, IBM is the single biggest player by a significant margin. However, places 7-10 go to Chinese entities. Assessed on this metric alone, US companies seem to be enjoying an edge over their Chinese rivals.

However, this is not an accurate picture of actual activity. Figure 6.4 in Chapter 6 shows the total number of quantum technology patents registered across seven countries. While roughly on a par with the US at the starting period 2015, China at the start of 2022 dominated the patenting landscape and outperformed the US by a magnitude of 4 in terms of annual patent registrations. While the big players are big US companies, China has successfully developed a large number of small to mid-sized companies that register quantum patents at significant pace. Over a five-year period, the number of annual patents that organisations headquartered in China have registered has risen fivefold.

As developed in Chapter 5 and in the previous section, China's leadership is mindful that a too powerful domestic tech sector could easily challenge Party dominance. While there are strong contenders among the top ten of registering entities, the scale at which small companies have emerged in China seems to suggest that Chinese officials are more interested in growing a quantum internet ecosystem that is characterised by a large number of small firms rather than a small number of big companies. Perhaps the leadership finds smaller companies easier to control. Be as it may, the data suggest that China has changed gears around 2015 and is now pursuing its quantum development programme at full speed.

7.3.2 Significant preferential treatment of domestic industries in China and the US

Chapter 6 presents some informative hive plots that show the citation behaviour of Chinese and US quantum technology patents. Patents can be divided into categories of popularity that reflect their status in a patent citation network. Prominent, high-impact patents are cited by many other patents. Some patents cite a great deal of other inventions as prior art, some cite only a few. Colouring the citation relationships between the patents in the network according to the geographic location of the filing organisation of the cited patent (either foreign or domestic) reveals the extent of preferential treatment of domestic 'prior art' over foreign inventions.

The hive plots presented in Chapter 6 show considerable preferential treatment for both Chinese and US patenting activity. Quantum patenting is strategic and exclusionary. Chinese quantum patents overwhelmingly cite other Chinese patents as prior art, and the US patenting behaviour is no different. This is evidence for two separate quantum internet ecosystems that evolve independently of each other. Neither programme relies on its strategic rival to any meaningful degree.

This finding suggests considerable mistrust between both countries, plausibly to a point where references to the chief rival's research activities is implicitly discouraged. It is surprising, however, that collaboration in other closely related domains is much stronger. For instance, Stanford University's Institute for Human-Centered Artificial Intelligence finds that 'U.S. and Chinese AI researchers teamed up on far more published articles than collaborators between any other two nations' (Andrews 2022) despite the deterioration of the relationship between the two countries. While there seems to be closer collaboration in AI, presumably due to personal relationships that have formed while Chinese researchers had undergone training in the US, research in quantum computing and communication, particularly where it matters for the quantum internet, is siloed and sealed off.

In terms of structural parameters, however, quantum patenting activity seems to be following a similar trend to what researchers have already observed in AI. The top of the field is dominated by big US corporations while China leads by count of registered patents overall. This is due to an extremely large number of smallish research institutes that register AI/ML patents at pace (Freist 2019). A 2021 study of international patenting activity in AI arrives at a similar conclusion. While 'the analysis of top assignees showed that most AI patents are owned by large private companies', (Liu et al. 2021, p. 17) argue, 'public organizations and universities are less prominent in the ownership of AI patent applications, except in China where public research organizations and universities are frequent AI patent assignees'. This thesis can confirm a similar pattern in the quantum domain: the field is dominated by large US corporations but in terms of numbers, China enjoys an edge thanks to a large army of registering 'foot soldiers'.

The Chinese quantum internet patent citation network is made up of 6,134 nodes and 6,970 edges. Its US counterpart has 2,863 nodes and 3,201 edges. Thus the Chinese quantum internet patent citation network is twice the size of its rival. While this difference in scale is considerable, their structural characteristics are very similar. New Chinese (US) quantum internet technology patents overwhelmingly cite domestic, i.e. Chinese (US) technologies. Where new Chinese (US) patents that are not being cited by any other patent, or cite patents that themselves do not cite any prior art, these citation relationships are almost one hundred percent domestic in character.

This is an important finding. Some commentators, notably based at US political think tanks, are quick to dismiss Chinese patents as 'trash' (Kersten et al. 2022). It is fair to assume that a sizeable number of the patents in the dataset analysed in Chapter 6 will not go anywhere, and it should be noted that Chapter 6 has found that in the Chinese network, the number of patents that do not gain much traction is nearly one hundred percent higher compared to the US network. There is considerable deadweight in the Chinese quantum internet citation network. Thousands of patents only cite one other Chinese patent, which is never cited again. This suggests that a lot of registered patents in this domain have little, if any, impact.

However, if Chinese patents are 'trash' for being irrelevant internationally, indicated by the fact that they only cite other Chinese patents, then the same would have to be concluded about the American quantum ecosystem. The fact that both systems are likely to carry substantial deadweight notwithstanding, the findings of Chapter 6 rather point to two highly shielded and siloed quantum internet research programmes. American companies, universities, research institutions and the military cite almost exclusively US-owned technologies only when registering new quantum internet patents. The most extreme case in the dataset is US patent (US 9971970 B1 20180515) which cites no fewer than 63 other US patents as prior art, displaying the maximum possible degree of homophily in the network.

7.3.3 Some summary network statistics explained

The literature on graph theory provides a number of informative indicators of network characteristics. Statistical details are discussed in full in Chapter 6. To generate talking points for discussion, this subsection presents them in non-technical terms.

The US citation network is twice as dense as its Chinese counterpart. This means that a random node in the US network is twice as likely to cite (or be cited by) a different node in the dataset, which suggests a more thorough citation practice and/or comprehensive knowledge of the (domestic) quantum patenting landscape. There is lots of evidence for significant homophily in both the Chinese and US quantum internet patent networks. Both networks are structurally similar in terms of mean degree, diameter and mean distance.

It is insightful to look at two further descriptive measures: the number of components and the so-called k-core. Large graphs are usually made up of smaller subgraphs or communities in which nodes are more strongly connected to each other than to other nodes in the network. In the case of patent citations, these are groups of patents with a stronger preference to cite one another relative to the citation network as a whole.

In the Chinese quantum patent citation network, there are two large components (complete subgraphs) of around 2,000 nodes each. These nodes can be thought of as two independent networks that sit inside the global structure. This is a surprising and unusual result. Typically, for networks of this kind, one would expect one large component, i.e. one big subgraph that sits within the bigger network. This is indeed confirmed for the US case. It contains only one single-biggest component of 1,589 nodes. Two explanations come to mind as to why two complete subgraphs would sit next to each other in the Chinese quantum ecosystem: i) China pursues not one but two distinct quantum internet research programmes that are independent of each other; or ii) the Chinese programme lacks strategic oversight and steer to keep things together so that research activity begins to drift apart. It should be noted that this thesis has found no further evidence for i).

The idea of the *k*-core is to successively 'peel away' outer nodes with only a few connections to reveal the core of the network that holds the entire graph together. The *k*-core is a token of resilience of the Chinese and US quantum patent networks: how many shocks to its periphery can the core of the network survive? What are the most important patents in these networks without which the entire network would collapse in on itself? The core is the subnetwork of the most tightly interlinked nodes that cannot be reduced further.

It was found that after five rounds of 'peeling away' the outer layers, the core of the Chinese network is made up of only 13 patents. The US network is even less stable: roughly three quarters of patents do not survive the first chop, and the process comes to a stop after four rounds, revealing a core of 18 patent records. Put differently, for both networks, made up of thousands of nodes, only a handful of patents hold the entire network together. The removal of 13 core records in the Chinese case, or 18 in the US case, would reduce the network to an empty graph.

In both cases, there are only a small number of utmost important patents that drive the entire quantum patenting ecosystem.

To sum up: both the Chinese and the US quantum patent networks are structurally similar on important metrics. They also carry a large number of patents that do not seem very influential (they cite only one patent, or are being cited only once). Despite their similarities, however, they are independent from each other in that neither side would take any notice of the other; it is almost as if they are sealed off against foreign influence.

7.3.4 What matters for quantum patenting?

While the above results are informative and give a strong indication as to the character of the Chinese and the US quantum internet development programmes, they do not reveal how the programmes have evolved over time, and how things have changed over time since the starting period of 2015. Summary indicators of the sort discussed so far also do not provide insight into how variables that are not captured in the network statistics above could possibly be relevant to giving the two quantum development programmes their characteristic shape.

To gain a deeper understanding of both systems, Chapter 6 time-sliced the data into three separate periods and tested ERGMs for all of the six resulting datasets (cf. (Ji et al. 2022)). It considers the following variables: Country of Publication (where the patent has been published), Applicant Type (Industry, University or research institute, Private individual, Military, Other) and the number of IPC codes under which the invention was filed. The below discusses the results for China and the US separately.

China:

For the period 2015-2017, the country of filing and the IPC codes given at registration are highly significant estimators of Chinese patenting activity, each at about 14 percent. This means, for instance, if two patents were filed by two different organisations but are both headquartered in China, and both filed patents in the same country other than China, then the chance that they form a citation link is **14 percent** (compared to a one percent chance for a random pairing of nodes). The same is true for IPC code clusters. If two patents during this period were filed under the same number of IPC codes in the classification tree, then their chance of being connected in the network was of similar degree (again, compared to a one percent baseline chance for a match). This is significant evidence for preferential treatment, or 'like attracts like' when it comes to the country of filing and the number of IPC codes given.

In 2017-2019, the picture had changed to the effect that the country of publication emerged as the most sizeable predictor of Chinese patenting activity. Two patents published in, say, South Korea, increased the chance of a citation link to **nearly 25 percent** compared to the probability of a random match of less than one percent. IPC clusters were also significant, but at an effect size of about 3 percent they were less relevant in this period.

In the final period under consideration, 2019-2021, when patenting activity accelerated considerably, the type of applicant had become highly significant also. If, for instance, two patents were registered by the Chinese military or a military research facility, the chance of them forming a citation (sub)network was **more than 33 percent** (compared to the one percent chance of a tie formation for a random selection of two nodes).

USA:

In the first period, 2015-2017, IPC codes were not a significant predictor of US quantum patenting activity. However, Country and Type were highly significant. Same-country and same-type-of-applicant citations mean that the chance for a citation link to form was **around 16 percent** in each case (compared to a baseline chance of less than one percent). For instance, if two patents were filed by large US corporations, the chance of one citing the other was 16 percent.

In the second period, 2017-2019, all three variables were significant (the effect size of IPC clusters was minimal, however). Country-to-country homophily jumped to **nearly 40 percent**, meaning that if two patents filed by organisations headquartered in the US were published in the same country, the chance that one cites the other was 40 percent. For the type of applicant, e.g. military-to-military or private sector-to-private sector, the chance of a connection in the network was **nearly 20 percent**.

Finally, for the period 2019-2021, which showed reduced US activity, the empirical picture is more mixed. All three variables proved highly significant. Country and IPC clusters each were **about 23 percent** while the type of Applicant had **dropped to 14 percent**. All variables attest to strong effect sizes compared to the baseline scenario of less than one percent chance for a tie formation.

The estimators vary over the six different datasets, and they are considerable in their range, being between 14 to 40 percent compared to what would have to be expected for random, non-strategic patenting activity. The findings suggest that while patenting activity in both countries is strategic, it is very much internal and inward-looking in the sense that researchers engage with works that seem familiar to them (where familiarity is expressed in terms of being of the same country, organisational type, or IPC cluster).

Put colloquially, each side is ‘doing its own thing’. And within each sub-cluster of the already siloed Chinese and US quantum internet research programmes, preferential treatment stretches even further, which suggests that ‘doing one’s own thing’ and group think are the ultimate drivers of patenting activity in the quantum domain. University researchers prefer citing other university researchers, while military research rather cites other military research and so forth. Patents that are filed under x amount of IPC codes attract patent citations where the citing patent is filed under the same number of codes. Research in quantum computing and communication where it matters for the quantum internet is very much the antithesis to an open, global, and collaborative research effort.

7.4 Outlook: quantum internet fragmentation and how to avoid it

This thesis presents evidence for two independent, siloed quantum internet research programmes in the US and China. If these programmes succeed, there could emerge two alternative models for the quantum internet. As Chapter 4 has discussed, the quantum internet is most likely to manifest as an enabling technology that provides quantum compute resources over distributed systems. Quantum networks will link to the ‘classical’ internet over gateways.

Chapter 5 has found evidence for an intensifying rivalry over internet governance and standards between the US and China. Either side can be expected to try and push their own proposals for internet governance reform with a view to future quantum networks. It is plausible to imagine two competing quantum networks to connect to the internet, access to which is restricted to either US and Chinese domestic industries, governments and/or research institutions. Should this happen, the quantum internet would be fragmented from the start.

'Quantum fragmentation' however would be bad news. Global problems require global solutions. Climate change and health emergencies such as Covid19 are prime examples. Chapter 4 has discussed some of the promises of a quantum internet. Entanglement at scale, the fundamental quantum compute resource, is hoped to provide the technology to find solutions to tackle climate change better, for instance. A quantum internet may give other important research projects with a global reach a big boost also, such as drug discovery or blockchain.

Whether the quantum internet can deliver on all these promises remains to be seen. However, for it to be able to realise at least some of its potential, the internet should remain as open and interoperable as possible. A 'many-nets' approach or otherwise implementation of an off-switch for embedding selective interoperability at the level of infrastructure, as Chapter 2 has discussed, would likely prove a considerable obstacle to research collaboration. Yet international collaboration on global issues will require seamless access to shared quantum resources. Quantum internet fragmentation would make international cooperation much more difficult, e.g. when members of a US-Chinese research team in climate science would be unable to utilise internet capabilities such as quantum cloud resources by others in the team. On top of such pragmatic concerns, quantum internet fragmentation would also feed into narratives of nationalism and decoupling, which have been discussed in Chapter 2.

It is a well-known problem that international institutions, which are constituted by delegates from national governments, oftentimes act myopic in their aim to maximise (or at least not compromise) the outcome for their home governments. While this behaviour is perhaps rational from the perspective of individual actors, it can cause irrational gridlock from a systems perspective (e.g. where the system is Planet Earth and the problem is human-made climate change). As respondents to this research project pointed out, internet governance fora are certainly no exception to this phenomenon. The national interest usually trumps the global perspective.

In response, appeals to global solutions are often framed in terms of moral imperatives, human values, and a shared responsibility for future generations. State actors who care first and foremost about maximising the outcome of international negotiations for their country find it easy to brush off these calls as they do not contribute to their objectives. The task then is to demonstrate that a global solution is commensurable with the pursuit of rational self-interest. Only if state actors are convinced that their countries will be better off should a global solution be found will they be motivated to agree multilaterally on a new and different way of doing things.

This section develops the building blocks of a model to demonstrate that a global quantum internet standard is in the national self-interest of myopic players who are motivated by domestic concerns only. The approach step below is a first step towards a mechanism design for an interoperable quantum internet. As such, it is best considered an outlook for future research activity, rather than a final contribution to the matter.

The point of the model below is to show that if a 'the whole is greater than the sum of its parts' logic is applied to internet governance competition, suddenly many new opportunities for engagement and cross-country collaboration emerge. It is in the rational self-interest of the US to pay off China to let go of its many-nets approach, the model suggests. The important point is that countries will not need to give up their position of self-interest; they may still consider what is good for them and attempt to maximise the payoff for their state, not necessarily what is best for the world overall. Where appeals for morality fall on deaf ears, the global good must be procured.

The modelling of scenarios where self-interested actors compete in international negotiations is the realm of traditional ('non-cooperative') game theory (popular introductions and overviews are, among many others, (Fudenberg 1991, Maschler et al. 2013, Osborne & Rubinstein 1994)). This well-established branch of game theory makes strong assumptions about individual rationality. For instance, in the original formulation of the classical one-shot prisoners' dilemma, each player expects the other player to be egoistic so that reliable side agreements which, ironically, would make the situation better for everyone involved, are explicitly not allowed.

This section takes an alternative approach to this established tradition of game theory, usually referred to as 'cooperative' game theory, in which actors may or may not work together. It models a so-called 'transferable utility' (TU) game in which some of the strict assumptions that game theory typically makes are relaxed. TU games are a fairly recent contribution. They have emerged out of the dissatisfaction with the above-mentioned shortcomings of traditional non-cooperative game theory. Good introductions can be found in (Osborne & Rubinstein 1994, Peleg & Sudhölter 2007, Rothe 2015, Roughgarden 2016).

The term 'transferable utility' seeks to capture that actors can give away some of their payoffs if doing so satisfies a different kind of rationality assumption. In non-cooperative game theory, players do not want to give up what is rightfully theirs. In TU games, however, other actors can be 'bought' if they see no reason to agree and abide by a global standard voluntarily. For instance, China could ask for compensation for shelving its many-nets approach, and it would not be irrational by design for other state actors to consider such a demand. In this sense, utility, as that which players get out of the game, is transferable.

A globally optimal solution then emerges as a kind of byproduct, a welcome side effect; it is not necessarily the primary intention of self-interested rational state actors that aim to maximise their own payoff. A better result globally, such as a quantum internet that does not split or fragment, is then the outcome of rational side payments (utility transfers).

The model is best considered a first approach to modelling how a full-blown quantum internet governance conflict between the US and China could be avoided, and how a focus on self-interest, rather than ineffective appeals to shared values and moral responsibility, may help prevent the quantum internet to split. In line with QISG, it is a way of thinking about quantum internet governance: an approach to capturing the constitutive processes that will shape the quantum internet, and pathways to carving out possible spaces for intervention.

7.4.1 Model characteristics

There are four players in this model: the US, China, the EU and an unaligned 'rest of the world' (RW). These four actors play a transferable utility (TU) game over a quantum internet standard. While state actors aim for the best possible outcome for their countries, they can make side payments to other countries in order to get them to form profitable (sub)coalitions. Opposing coalitions incentive and hope to attract non-aligned states, for instance by offering 'quantum patronage' or actual side payments in monetary terms. This introduces opportunities for bargaining, exclusion and collusion. While a grand coalition (the 'world coalition' that sees all four players to agree on a single uniform standard) would be globally optimal, some states may find it profitable to join forces with other countries, break off and deviate. State actors maximise the payoff for their country, not a vague 'moral responsibility' function.

To get them to join coalitions, compensation will have to be paid (in real or monetary terms). Such side payments can take many forms, for instance the US could get China to join a global coalition for a common quantum internet standard by lowering tariffs on some goods in the current US–China trade war. Or it makes a direct payment. In this sense, utilities are transferable within each coalition. The model assumes that political and economic gains and costs can be sufficiently expressed in monetary terms, or in expected values of future gains and costs. It also assumes that state actors can reasonably approximate these figures at the time when quantum governance regimes are being negotiated.

The following characterises the model in its general form. Let $N = \{1, 2, ..., n\}$ be a set of n players. Let 2^n denote the power set of N, i.e. the set of all subsets of N: the number of all possible coalitions in the game. This implies that, technically speaking, state actors can form 'coalitions' with only themselves, i.e. the power set also contains n coalitions with only one member each.

The cooperative game G is then characterised by a tuple $\langle N, v \rangle$ where $N = \{1, 2, ..., n\}$ is the set of players and $v : 2^N \rightarrow \mathbb{R}^+$ is the so-called *characteristic* *function.* For each subset S (coalition) of N, $S \subseteq N$, the characteristic function v allocates a payoff for the coalition in question. It is important to note that v_i expresses the total payoff for coalition i; it is then up the members of each coalition how they distribute the payoff for the coalition amongst themselves. This will be an important point later on.

The model makes two common-sense assumptions: 1) $v(\emptyset) = 0$: the value of an empty coalition is zero. If no one shows up to negotiate quantum internet standards there will be no positive outcome for anyone. 2) $v(A) \leqslant v(B)$ for all coalitions $A \subseteq B$, which is to say that if A is a sub-coalition of B, the group payoff for B must be at least equal to that of A for the members of A to want to invite new members to their club–otherwise they would be worse off if they formed a larger coalition. Members of each coalition are also assumed to be efficient in the sense that $\sum_{i \in S} x_i = v(S)$ where x_i denotes country i's share of the group payoff for the entire coalition and S is a sub-coalition. In other words the group surplus of the coalition will be distributed in its entirety (if not necessarily fairly).

Finally, and most importantly, the game is assumed to be *superadditive* in the sense that state actors have reasons fo form coalitions in the first place:

$$v(A \cup B) \geq v(A) + v(B). \tag{7.1}$$

A larger sub-coalition that is made up of A and B must generate a payoff that is at least equal to, but preferably greater than, the sum of what each coalition could possibly achieve on its own, or else there is no point in forming a larger coalition. If this condition were not met, grand coalitions could never form and the quantum internet would be fragmented by definition. No actor would have an incentive to ever cooperate with anyone, which is an implausible assumption. Superadditivity assumes that all state actors will want to see a global quantum internet standard realised–as long as it suits their preferences and generates a better outcome for them 'individually' as states. They may never get to a global standard if, on their way, they find reasons to deviate. But superadditivity means that a global standard is not ruled out formally before the game begins.

Now, what are the conditions for each state actor to join the grand coalition? Importantly, they would need to be certain that their share of the payoff is at least as big as what they can achieve on their own. Put differently, the group payoff $v(N)$ of the grand coalition N that involves all n actors must be distributed according to a payoff vector $\boldsymbol{x} = (x_1, x_2, ..., x_n) \in \mathbb{R}^n$ such that

$$x_i \geq v(\{i\}) \quad \forall\, i \in N. \tag{7.2}$$

There are many possible ways to share the returns of an interoperable quantum internet. In the next step, all these plausible payoff vectors are collected in a set that is called the set of *imputations* of G:

$$\mathcal{I}(G) = \left((x_1, x_2, ..., x_n) \in \mathbb{R}^n \middle| \sum_{i=1}^{n} x_i = v(N),\ x_i \geq v(\{i\}) \ \forall\, i \in N \right). \tag{7.3}$$

Essentially, imputations are partitions of the overall game space in $\mathbb{R}^n$. They separate possible payoff functions from impossible ones. It follows that the set $\mathcal{I}(G)$ of all possible imputations is non-empty if and only if the overall surplus of the grand coalition is at least as great as the sum of all individual payoffs when players do not form coalitions with any other state, i.e. $v(N) \geq \sum_{i \in N} v(\{i\})$.

The following subsection discusses a numerical example to illustrate the implications of this model for finding a global standard for the quantum internet.

7.4.2 Case 1: the quantum internet will be fragmented

Consider the following illustration of the coalitional game above. As mentioned, there are $n = 4, N = \{1, 2, 3, 4\}$ state actors (players) in this game: the US, China, the EU and 'RW' (for 'rest of the world'). This order is motivated by the response of an informant, developed in Chapter 5, who considers quantum internet governance as largely shaped by US-Chinese rivalry 'with a dash of Europe'.

Ignoring the empty set, there are $2^n - 1$ subcoalitions in the game, i.e. 15. The payoff for single coalitions where countries form a quantum internet coalition only with themselves is normalised to zero. While there can be quite substantial benefits for state actors to build a completely autonomous quantum communication network that is not accessible to anyone, such as an internal quantum-secured government communication network, this benefit is assumed to be roughly the same for every player and therefore normalised to zero to make computations simpler.

When coalitions form, the countries that join respective coalitions will add to its overall payoff. Again, for ease of computation, the model assumes an order of contributions of $4 > 3 > 2 > 1$ for the US, China, the EU and RW. This means the group payoff will rise by 4 when the US decides to join an existing coalition, and it will rise by 1 if the rest of the world aligns with an existing coalition. This ordering is in line with the bargaining power these actors are found to have in the analysis of the literature and the interviews in Chapter 5.

The table below presents all possible coalitions in this game and the group payoffs associated with them.

Coalition $S(i,j)$	**Country tuples**	**Group payoff** v_i
S=({1})	S=({USA})	0
S=({2})	S=({China})	0
S=({3})	S=({EU})	0
S=({4})	S=({RW})	0
S=({1,2})	S=({USA, China})	7
S=({1,3})	S=({USA, EU})	6
S=({1,4})	S=({USA, RW})	5
S=({2,3})	S=({China, EU})	5
S=({2,4})	S=({China, RW})	4
S=({3,4})	S=({EU, RW})	3
S=({1,2,3})	S=({USA, China, EU})	9
S=({1,2,4})	S=({USA, China, RW})	8
S=({1,3,4})	S=({USA, EU, RW})	7
S=({2,3,4})	S=({China, EU, RW})	6
S=({1,2,3,4})	S=({USA, China, EU, RW})	10

Table 7.2: Group payoffs for all possible imputations $\mathcal{I}(G)$ in Case 1.

The figure below plots the set of imputations $\mathcal{I}(G)$ that characterise this game (the download link for the MATLAB code to generate this and the following graphs can be found in the Appendix). Each of the four vertexes of the game space (the corners where the edges meet) denotes the position of a player. In a

4-player game, this allows for the graphical representation of imputations in three-dimensional Euclidian space. The hull, in light pink for better visibility, encloses the entire set of available strategies, i.e. $\mathcal{I}(G)$. Whichever payoff can be found inside the pink-coloured tetrahedron is available to the players.

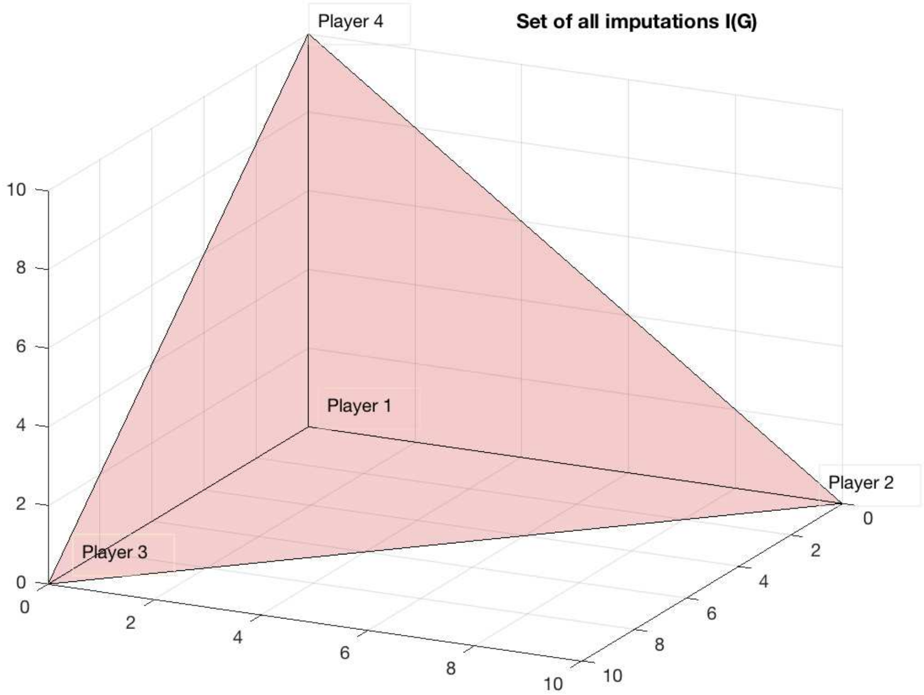


Figure 7.2: The set of imputations $\mathcal{I}(G)$, i.e. the collection of all available strategies in this game.

The surplus strictly increases in n. Globally, it is optimal for all countries to settle on a shared quantum internet governance framework to generate a surplus of 10 for the entire world. A 'world government' with legislative sway over individual countries would indeed implement $S = (\{1, 2, 3, 4\})$. No sub-coalition could generate a better payoff than the grand coalition. But in the absence of any such social planner that maximises global welfare, the question arises, is this grand coalition stable? Or can countries deviate and form smaller subcoalitions that promise a higher payoff so that they can credibly threaten to never join the grand coalition of quantum internet governance?

The grand coalition will not be stable (as in it will never be realised) if and when groups of countries smaller than the grand coalition can realise bigger payoffs by 'doing their own thing'. Thus for the grand coalition to survive beyond its planning phase, there must be divisions of the surplus of the grand coalition that are better than whatever could be achieved in subcoalitions. In the literature, this stability concept is called the *core* of a coalitional game (Osborne & Rubinstein 1994, Peleg & Sudhölter 2007). Essentially, the core of a cooperative game is the set of all strategies that no individual player finds profitable to deviate from. Formally,

$$\mathcal{C}(G) = \left((x_1, x_2, ..., x_n) \in \mathcal{I}(G) \middle| \sum_{i \in S} x_i \geq v(S) \;\; \forall \; S \subseteq N \right), \tag{7.4}$$

where $S \subseteq N$ is a sub-coalition of N.

If there are imputations for which the above inequality holds, the core is non-empty and the grand coalition can be considered *stable* in the sense that no state actor has an incentive to deviate. If, however, the core is empty, there will be strategy profiles available to country i in sub-coalitions that yield a share of surplus that is greater than what i could possibly gain by a share of the surplus of the grand coalition.

To check if an imputation is in the core, the following system of linear inequalities must be solved:

$$x_i \geq 0; \tag{7.5}$$

$$\sum_{i \in N} x_i = v(N) \ \ \forall \, i \in N; \tag{7.6}$$

$$\sum_{i \in S} x_i \geq v(S) \ \ \forall \, S \subseteq N. \tag{7.7}$$

where $S \subseteq N$ is a subcoalition of N.

With regard to the illustrative example discussed in this subsection, these conditions mean that for the grand coalition to be stable, i) every player gets at least nothing (i.e. they will not be worse off than if they sit by idly and do not participate in finding a standard), ii) the entire payoff vector of the grand coalition is being distributed, and iii) everyone walks away with a share of the payoff at least as great as what they could achieve in all possible sub-coalitions.

Therefore, for any division of the total surplus $\sum_{i=1}^{4} x_i = 10$ to be in the core, it must be decided in such a way that the inequalities $x_1 + x_2 \geq 7$, $x_1 + x_3 \geq 6$ etc all hold (please refer back to the first table in this section for the entire system of inequalities that need to be considered in this case). If, for instance, once the grand coalition payoff is divided, x_1 and x_3 would get a share such that $x_1+x_2 < 6$, they would have a good enough reason to deviate and build their own restricted US-EU quantum internet instead. This is because their assured payoff in that scenario would be 6, as per the payoff matrix in the table. Linear programs of this sort can be solved in applications such as Matlab if n is sufficiently small.

In the case under consideration here, there is no solution that satisfies this system of inequalities. This means that the core of the set of imputations is indeed *empty*–the grand coalition is not stable: this means that the quantum internet would be fragmented. There is no way for the group payoff to be divided so that some players would not be better off by forming sub-coalitions. If the above payoff table should be an accurate reflection of the stakes involved in finding a common standard for a future quantum internet, the outlook is pessimistic. It is implausible for countries to come together and unite around a shared governance framework. In this scenario, risks of a breakup of the internet abound.

7.4.3 Case 2: conditions for an interoperable quantum internet

The outcome of case 1 is sensitive to the group payoff that the grand coalition can achieve. In the above case, the characteristic function of the group payoff was simply the sum total of each player's contribution to the game. The grand coalition payoff $4 + 3 + 2 + 1 = 10$ is the sum of the value that each country adds. But this entails that the achievements of a grand quantum internet coalition are too close to what countries could do on their own. The above case contains no 'the whole is greater than the sum of its parts' logic. The fragmentation of the quantum internet was the result of a lack of a strong pull factor towards global cooperation.

In a variation of the case above assume that the global payoff of the grand coalition is increased by a modest unit factor: $v(N) = 11$. Such a step can be motivated by logics of economies of scale of a global quantum internet standard, such as the aforementioned seamless cooperation between researchers across national boundaries, or not having to implement several layers of infrastructure that will not be able to communicate with each other, as informants have suggested will be the case (see Chapter 5). How, then, will the game change? Computing the linear program reveals that the core of the adjusted game is now non-empty. The figure below illustrates this.

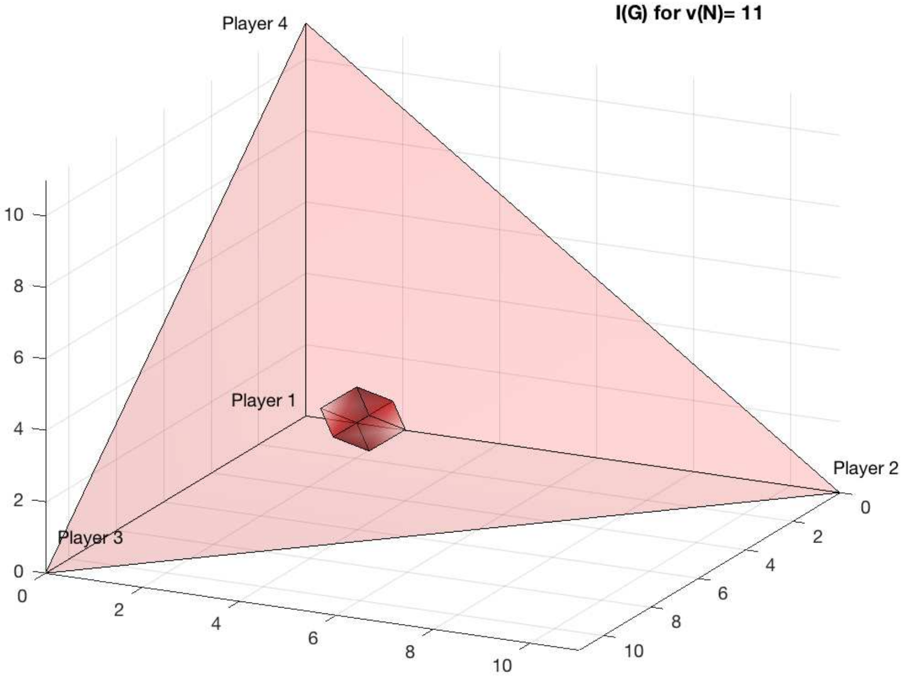


Figure 7.3: The core of the game $\mathcal{C}(G)$ for $v(N) = 11$, superimposed on the set of imputations $\mathcal{I}(G)$, i.e. the collection of all available strategies in this game, for the adjusted case when $v(N) = 11$.

This means that the grand coalition is now stable. There are imputations in the core, i.e. divisions of the grand payoff, that no state actor could possibly improve upon if she deviated. There is an incentive to stick to standards and protocols that will be found multilaterally in global cooperation.

What are the possible divisions of the grand payoff? The table below presents the computation of the vertices of the core when $v(N) = 11$. Between these edges of possible payoffs, any division is equally optimal in the sense that once agreed upon, no state actor finds ground to leave the grand coalition. The global surplus will not change either way but each division benefits countries to different degrees.

#	**USA**	**China**	**EU**	**RW**
(a)	3	4	3	1
(b)	3	4	2	2
(c)	3	3	3	2
(d)	5	2	3	1
(e)	5	2	2	2
(f)	5	4	1	1
(g)	5	4	2	0
(h)	5	3	1	2
(i)	5	3	3	0
(j)	4	2	3	2
(k)	4	4	1	2
(l)	4	4	3	0

Table 7.3: Vertices of the core of $\mathcal{C}(G)$, i.e. possible divisions of the grand coalition payoff $v(N) = 11$ among the four members, all of which are optimal.

There are three curious possible divisions, (g), (i), and (l), in which the rest of the world gets nothing. The smallest players in the game in terms of economic weight and bargaining power, the non-aligned mass of countries faces a 33 percent risk that the winning division of the surplus will exclude them from any benefit (or leave them very little). Such a scenario reflects the responses analysed in Chapter 5 that point to the concerns of smaller countries to get drawn into an internet governance conflict between the US and China, without any real power to shift the discourse, and with nothing to gain. Yet walking away from a global deal, even if they achieve next to nothing, would leave small countries even worse off.

To further illustrate the sensitivity of the core to the difference between the payoff associated with the grand coalition and the next best characteristic functions that sub-coalitions can possibly form, i.e. $v(4) - v(3)$, consider a variation in which the grand group payoff is not 11 but 20, as plotted in the graph below. The grand coalition is now even more stable as there are plenty of imputations in the core to choose from, none of which can be improved upon in smaller sub-coalitions.

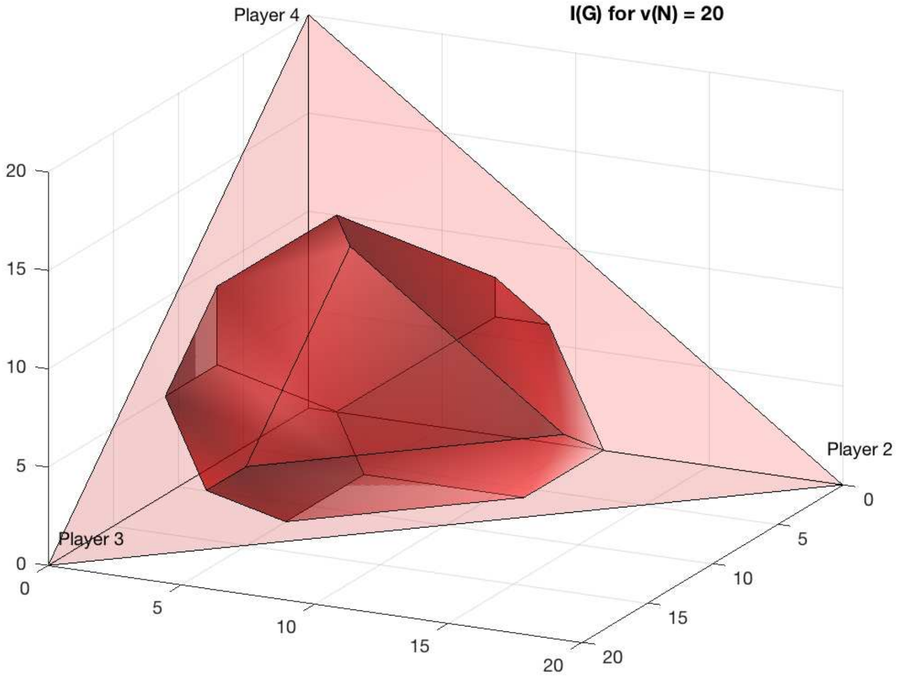


Figure 7.4: The core of the game $\mathcal{C}(G)$ for $v(N) = 20$, superimposed on the set of imputations $\mathcal{I}(G)$, i.e. the collection of all available strategies in this game, for the adjusted case when $v(N) = 20$.

The table below presents the vertices of the core for $v(N) = 20$, i.e. the outer edges of the set of all optimal divisions of the grand payoff. While these characterise the extreme points of all possible divisions only (any division between the vertices is equally optimal), again they point to significant risks to smaller countries. There is now a 50 percent risk to end up in a place where no or only relatively modest benefit can be obtained. Again, should RW face regions near (d), (f), (h), (i), (k) or (l), no actor has any reason to deviate. The higher the benefits of a truly interoperable global quantum internet standard, the bigger the risk for smaller countries to be unable to capitalise on these returns. The bigger the cake, the larger the pieces that dominant countries get.

#	**USA**	**China**	**EU**	**RW**
(a)	0	0	12	8
(b)	0	0	9	11
(c)	0	13	0	7
(d)	0	13	7	0
(e)	0	9	0	11
(f)	0	8	12	0
(g)	14	0	0	6
(h)	14	0	6	0
(i)	14	6	0	0
(j)	9	0	0	11
(k)	8	0	12	0
(l)	7	13	0	0

Table 7.4: Vertices of the core of $\mathcal{C}(G)$, i.e. possible divisions of the grand coalition payoff $v(N) = 20$ among the four members, all of which are optimal.

Under this variation of the model, countries will form a stable international coalition and an interoperable quantum internet will emerge. The greater the economies of scale that an open quantum internet can realise, the bigger the incentive for all countries to cooperate. The question then emerges, how should the grand surplus be divided? So far the model has been agnostic about payoff divisions. The following subsection discusses how China can capitalise on the returns of a global quantum internet by demanding side payments in response to its credible threat to walk away.

7.4.4 Sharing the benefits of an interoperable quantum internet

The above variation of the model produces a stable outcome, which is the condition for an interoperable quantum internet. If 'the whole is greater than the sum of its parts' logic holds, and there are many good reasons for an open quantum internet, a global quantum internet standard is possible. How should each country be rewarded for agreeing to a global standard? What would be the parameters of a fair division?

The *marginal* contributions of each player are plausible candidates, i.e. the increase in a sub-coalition's payoff when country i joins the coalition. These will be different for different subdivisions. For instance, if the US were to build an exclusive US-EU quantum internet, the group payoff would be $v(\{1,3\} = 6$. Since the US on its own can only generate a surplus of (normalised) zero, the marginal contribution of Europe is 6 in this case. However, if Europe wishes to join an existing coalition between the US and China, its marginal contribution would only amount to $v(\{1,2,3\} - v(\{1,2\} = 9 - 7 = 2$. Marginal contributions vary across the game space. On their own, they will not reduce the size of the core. In fact, the vertices of the set of marginal contributions enclose the core–the core is a subset of all marginal contributions as the figure below illustrates.

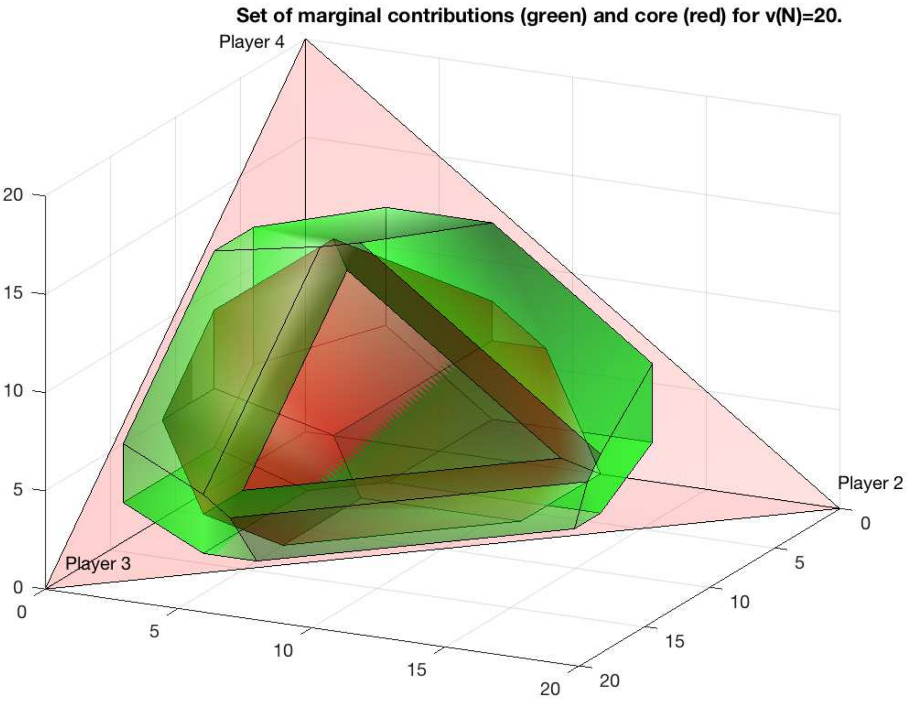


Figure 7.5: The vertices of the set of all marginal contributions (green) superimposed on the core (red) $\mathcal{C}(G)$ for $v(N) = 20$. The core is a subset of marginal contributions.

A fair way for all parties to proceed would be to introduce weights for marginal contributions. The so-called Shapley value is a popular allocation rule for assigning players a value that corresponds to their marginal contributions under the assumption that each sub-coalition is equally likely to form (Peleg & Sudhölter 2007). Formally, the share of the division d_i for player i can be expressed as

$$d_i(N, v) = \frac{1}{N!} \sum_{S \subseteq N \setminus \{i\}} |S|!(|N| - |S| - 1)![v(S \cup \{i\}) - v(S)]. \tag{7.8}$$

The Shapley value collects the marginal contributions that i makes to all coalitions that do not already contain i, which are then weighted by the number of ways in which i's marginal contributions can occur, which are then divided by the total number of possible permutations $N!$. Put differently, for each new coalition that can form, the new member demands the marginal contribution she makes as a fair compensation for her efforts. For each state actor, the average of these marginal contributions is then calculated as an expected value over the total number of ways in which a state actor can enter a coalition. If marginal contributions guide players' ideas of fairness, the Shapley value is the fairest division of the overall surplus (see (Rothe 2015, chapter 3.2) for an elegant proof).

The table below lists the Shapley values for both games $v(N) = 11$ and $v(N) = 20$.

$N(v)$	**USA**	**China**	**EU**	**RW**
$N(v) = 11$	3.75	3.08	2.42	1.75
$N(v) = 20$	6	5.33	4.67	4.00

Table 7.5: The Shapley values d_i for both games $N(v) = 11$ and $N(v) = 20$, which divides the grand surplus between all countries in a fair manner.

For $N(v) = 20$, the following can be observed. China 'only' contributes 3 as a new joiner to sub-coalitions as per the table earlier that displays each country's contributions. However, given the relative advantages of a global standard, it can monetise its strong bargaining position: the threat to walk away is not empty talk, it would leave the US, the EU and the rest of the world worse off. It can demand a transfer of utility of up to 5.33, which, under the assumptions of the Shapley value, is a fair ask. This would give China a wholesome yet justified return of $(5.33 - 3)/3 = 78\%$ over its actual contribution.

Now, it is in the rational self-interest of the US, the EU and the rest of the world to meet this demand. Even a joint payment of 5.33 towards China allows them to realise individual gains that are out of reach without China at the negotiating table. The policy implication of this illustrative model is that the US should push back against 'New IP' but present China with financial incentives for shelving its many-nets standard. Rather than calling out the strategic rival for wanting to implement an internet standard that has surveillance and control built into it, the US government should be prepared to incur financial costs and pay up to secure an interoperable quantum internet. It is in its own best interest to do so. China can demand this payment, and it must be considered fair.

The model predicts that the quantum internet will not be interoperable unless it is commonly accepted that 'openness' comes at a price. Arguably, this is change of perspective and perhaps a learning curve for the US and its allies for whom it is tradition that standards 'appear' that represent their vision of what the internet should look like. While it is not wrong to point to the considerable issues of surveillance and control in 'New IP', the danger of mobilising too much of a rhetoric that pits good against evil, the 'free' West against an authoritarian eastern regime, is to only antagonise China further. It would be more effective to accept that the good of a free and open quantum internet should be procured.

7.5 Main points of Chapter 7

This chapter has discussed the findings of Chapters 4, 5 and 6 in response to the research questions developed in Chapter 1 and the literature discussed in Chapter 2. The below collects the major takeaways of the chapter.

7.a For China, opportunities to shape the quantum internet offer a chance to make the internet a more efficient surveillance-and-control system. An advanced internet with quantum capabilities may facilitate surveillance tasks that have traditionally been carried out by human operators.

7.b The Chinese leadership is determined to maintain its position as the ultimate *data sovereign*. Sitting at the top of the 'trust pyramid', it demands absolute control over the internet. As there can be no data sovereign above the Party, internet technologies must be designed and governed in a way that accommodates Party oversight. To this end, a genuinely Chinese quantum technology stack could be trusted by the Party and the security apparatus to get the paramount task of domestic surveillance right while at the same time also being a big reputational asset.

7.c The UK government and GCHQ do not consider QKD a genuine threat. The most important issue that arises from quantum innovation is to protect British quantum IPR, they say. However this thesis finds that it could be too soon to outright dismiss Chinese QKD and other quantum communication technologies.

7.d Internet standardisation bodies suffer from what a respondent called 'institutional fragmentation'. Internet standards have been thoroughly securitised in that narratives of military control and security concerns are now shaping the discourse to a large degree, and both the US and China push for reform at organisations they dominate while ignoring others where they have less influence.

7.e US and Chinese big tech have emerged as alternative sources of power that try to shape domestic internet policy positions. China is concerned about US big tech and its influence on US policymaking for two reasons: i) it could fuel ambition among Chinese internet entrepreneurs at home whose attempts at shaping Chinese policies must be contained; and ii) China is principally more comfortable dealing with state actors. Too much influence of big tech complicates and obscures the strategy landscape.

7.f Empirically, China has established a leadership position as it has been registering potential quantum internet technologies at scale. This is due to the fact that since 2015, China has grown a sizeable ecosystem of quantum SMEs. From a Party perspective, it is possible to imagine that a large number of small companies is hoped to be easier to steer than a corporate giant.

7.g As far as it is possible to tell from the high-level outlines of 'New IP' that are currently available, China's many-nets proposal, while coming at considerable cost in terms of accessibility and privacy, seems to have the potential for added security and stability at the level of infrastructure and transport layers. Gateways can be closed so a damaged or compromised subnetwork can be switched off easily without threatening the integrity of the entire network. 'New IP' must be considered a precursor to the ways in which China envisions the implementation of the quantum internet. Quantum capabilities could be made available to selected subnetworks only, effectively splitting the internet into a classical network and a quantum-powered one. A *'New IP' quantum* *internet* would connect to the rest of the network via strongly policed access points.

7.h It must be assumed that the Chinese leadership does not expect the rest of the world to embrace 'New IP' and rebuild the internet accordingly. What 'New IP' has already achieved, however, is to show the world that China is a serious contender to Western dominance: a player not only at the cusp of building a radically novel network technology but also able to offer a blueprint for implementing a new vision of the internet with ample surveillance tools inbuilt. 'New IP' is a signal of intent, confidence and ambition.

7.i The quantum internet may create new dependency risks for the UK as it potentially exacerbates the problem of increased market concentration among cloud service providers, a market dominated by US companies. Cloud services have quickly become critical infrastructure for UK businesses and the public sector. The initial offering of a quantum internet would be what may be called Quantum Computing as a Service (QCaaS). Should big US corporations dominate the market for QCaaS also, and there are reasons to believe they will, structural dependencies for the UK on the US private sector will solidify.

7.j In the period January 2015–December 2021, the top organisations that had registered relevant quantum internet patents were IBM and Intel, multinational companies headquartered in the US, followed by TCL Corporation, a Chinese consumer electronics company. By count of newly registered quantum internet patents, IBM was the single biggest player by a significant margin. Places 7-10 went to Chinese entities.

7.k While roughly on a par with the US at the starting period 2015, China at the beginning of 2022 dominated the patenting landscape and outperformed the US by a magnitude of 4 in terms of overall annual patent registrations. While the big players are big US companies, China has successfully developed a large number of small to mid-sized companies that register quantum patents at significant pace. Over a five-year period, the number of annual patents that organisations headquartered in China have registered has risen fivefold.

7.l There is robust evidence for significant preferential treatment of domestic quantum industries in the US and China. Chinese quantum computing and quantum communication patents overwhelmingly cite other Chinese patents as prior art, and the US patent citation behaviour is no different. This is evidence of two separate quantum internet research ecosystems that evolve independently of each other. Neither programme relies on its strategic rival to any meaningful degree.

7.m This thesis can confirm for the quantum patenting domain a pattern that researchers have observed in AI: the field is dominated by large US corporations but in terms of numbers, China enjoys an edge thanks to a large army of registering ‘foot soldiers’.

7.n The Chinese quantum internet patent citation network is made up of 6,134 nodes and 6,970 edges. Its US counterpart has 2,863 nodes and 3,201 edges. Thus the Chinese quantum internet patent citation network is twice the size of its rival. While this difference in scale is considerable, their structural characteristics are very similar. New Chinese (US) quantum internet technology patents overwhelmingly cite domestic, i.e. Chinese (US) technologies.

7.o In the Chinese quantum patent citation network, there are two large components (complete subgraphs) of around 2,000 nodes each. They can be thought of as two independent networks that sit inside the global Chinese system. This is a surprising and unusual result. Typically, for networks of this kind, a single large component is to be expected, i.e. one big subgraph that sits within the bigger network. This is indeed confirmed for the US case. It contains only one single-biggest component of 1,589 nodes.

7.p The k-core of the Chinese network is made up of only 13 patents for $k = 5$. The US network is even less stable: roughly three quarters of patents do not survive the first chop, and the process comes to a stop after four rounds, revealing a core of 18 patent records. Put differently, for both networks, made up of thousands of records, only a handful of 'superpatents' hold the entire network together.

7.q In China, for the period 2015-2017, the country of filing and IPC codes are highly significant estimators of Chinese patenting activity, each at about 14 percent. In 2017-2019, the picture had changed to the effect that the country of publication emerged as the most sizeable predictor of Chinese patenting activity. In the final period under consideration, 2019-2021, when patenting activity accelerated considerably, the type of applicant had become highly significant also.

7.r In the US, in the first period, 2015-2017, Country and Type were highly significant variables. Same-country and same-type-of-applicant citations mean that the chance for a citation link to form was around 16 percent in each case. In the second period, 2017-2019, country-to-country homophily jumped to nearly 40 percent, meaning that if two patents filed by organisations headquartered in the US were published in the same country, the chance that one cites the other was 40 percent (compared to the probability of a random pairing of less than one percent). For the period 2019-2021, which showed reduced US activity, all three variables proved highly significant.

7.s The empirical analysis of six ERGMs has found that each side is 'doing its own thing'. Within each sub-cluster of the already siloed Chinese and US quantum internet research programmes, preferential treatment stretches even further, which suggests that 'doing one's own thing' and group think are the ultimate drivers of patenting activity in the quantum domain. University researchers prefer citing other university researchers, while military research rather cites other military research and so forth.

7.t A coalitional game theory model in which utility is transferable suggests that the quantum internet will not be interoperable but fragmented unless the US makes the conscious decision to offer China payment to shelve its 'New IP' many-nets approach. The model suggests an allocation rule that specifies how much compensation China can reasonably demand to let go of its ambitions to push for Chinese quantum internet standards. The important insight of the model is that it will be strictly beneficial for the US and its allies to make a financial sacrifice to obtain a global standard for an open quantum internet, even if this requires a change of perspective: the West is no longer able to implement internet standards at will; standards no longer 'appear', they must be procured.

Chapter 8

Conclusion

Against the backdrop of the intensifying strategic competition between the United States and China, this thesis has presented the first in-depth study of the technological and political factors that shape the emergence of the quantum internet. A quantum-enabled internet is hoped to provide the infrastructure for secure communication and to offer quantum compute resources at scale over distributed systems. This thesis investigated how the quantum internet is being framed in security terms in the aggravating rivalry between the two superpowers over emerging technologies of strategic importance, and what this means for the future of the internet. Over the past five years, commentators have increasingly expressed concern about a breakup or a fragmentation of the network of networks. The thesis asked how the strategic competition between the US and China may impact standard-finding for an open quantum internet and mapped out significant obstacles on the way to maintaining interoperability.

In an original contribution to research methods, this thesis was the first application of ERGMs to the analysis of patent data and their citation trees in the domain of quantum internet technologies. Following a mixed-method approach, this thesis evaluated a corpus of interview data and conducted a statistical analysis of 4,200 patent family records in quantum internet technologies and the 10,000+ patents they cite. It has found robust evidence for two separate and siloed quantum internet research programmes in the US and China. These programmes are further characterised internally by significant homophily and the preferential treatment of domestic industries. Findings further suggest a tentative edge for China in the domain of quantum communication, an important class of quantum technologies for realising a quantum internet. China's significant progress in developing components for a quantum internet is likely to give its increasingly assertive stance in negotiations at internet governance and standards fora some additional momentum.

In interviews, UK government officials and GCHQ expressed confidence that quantum internet standards that serve Western interests will appear. This thesis contends that given China's increasingly antagonistic position, this will be an uphill struggle. It argues that China should be expected to try and implement Chinese internet standards for the purpose of offering what this thesis called *quantum patronage*: a complete package of quantum technology stacks and appropriate standards in line with its 'China Standards 2035' plan. Quantum patronage may offer hitherto non-aligned countries the technologies for secure communication and quantum compute resources at scale in exchange for a commitment to allegiance and strategic alignment.

With a view to the UK, the findings of this thesis suggest the quantum internet is likely to generate new structural dependency risks for Britain. Quantum compute resources are likely going to be made available over the cloud. This is because of the prohibitive costs of building and maintaining quantum computing facilities. US big tech companies already dominate the cloud services market in the UK, a key pillar of public sector and business activity, and it is these very companies that also invest significantly in developing commercial offerings in the quantum domain. Dependencies on the US private sector for the whole of the UK economy are therefore likely to solidify when QCaaS, or Quantum Computing as a Service, arrives.

The empirical findings of this thesis have informed the first tentative steps towards a game theory model of quantum internet standards finding. Developing it further and evaluating it comprehensively will make for exciting future research in this area. In line with QISG, the model is a heuristic tool for spelling out the conditions for an open, interoperable quantum internet that is built on shared standards. It recommends the US make side payments to China as compensation for easing its strategic ambitions, in particular around its 'New IP' many-nets proposal. While telecommunications and internet standards have traditionally been developed to Western proposals, there is little ground to assume that this trajectory will necessarily continue. The model recommends Western policymakers to acknowledge this fact and actively pursue standard-finding for the quantum internet. The thesis argued that China can reasonably ask for compensation to agree to such a standard and suggested a first step towards designing a mechanism for doing so. Regarding future research, this line of enquiry should be pursued further.

The major contribution of this thesis is empirical. In Chapter 1, the thesis developed the following overall research question:

> **R.1** How is the quantum internet being shaped by US-Chinese competition?

For the purpose of empirical analysis, this question was operationalised and split into two subquestions that asked about expert views in internet governance and what patent data reveal about US and Chinese activity. In pursuing R.1, Chapters 4, 5 and 6 analysed publicly available sources, as well as interview and patent data following a mixed-method approach that had been developed in Chapter 3. Chapter 7 presented a discussion of the findings in conversation with the literature reviewed in Chapter 2.

While the full analysis and discussion can be found in the preceding chapters, the following section presents a summary of the main findings of this thesis. These findings are being synthesised into answering R.1 overall. The final section of this concluding chapter offers reflections on the research project and the findings so obtained and presents a perspective for Web Science as a discipline for when the internet goes quantum.

8.1 The main findings of this thesis

1. Chinese ambition

Quantum capabilities, particularly a quantum-enabled internet, would allow China to make headway towards four goals: i) to project global dominance and leadership in the emerging technology race with the US, ii) to secure internal communication against foreign espionage, iii) to further automate its domestic surveillance and control apparatus and, importantly, iv) to support the Communist Party in reining in on domestic big tech and establishing itself as the ultimate ‘data sovereign’.

A quantum internet will help the Chinese leadership assume what it considers its only plausible position at the top of a ‘trust pyramid’ from where it can exercise downward pressure, particularly on increasingly powerful domestic businesses that now hold vast amounts of data on the Chinese population, and therefore may challenge the state in its role as data sovereign. A genuinely Chinese quantum internet technology, proudly developed at home by Chinese scientists, will offer not just considerable reputational gains but deliver a technology stack that the Chinese leadership can trust.

2. Chinese big tech and quantum small tech

China has grown powerful firms that it hoped would challenge Western big tech. While they have in some cases, domestic big tech in China now poses a risk to Party dominance as successful entrepreneurs and industrialists have emerged as powerful internal rivals. This presents the Party with a double whammy as the Chinese leadership has now grown suspicious of big tech at home and abroad.

It considers the influence of large US technology corporations on US policymaking a complication and obfuscation of its strategy landscape. This is because their involvement increases the number of actors and the range of interests that China needs to consider and accommodate in its planning and campaigning. Traditionally, it prefers dealing with state representatives. This issue is then further complicated by the rise of influential big tech at home.

When it comes to novel quantum internet technologies, the leadership position that China has established is mostly due to the output of a large ecosystem of small firms, this thesis has found. It can be concluded that the Party leadership finds small and widely dispersed business networks easier to manage and integrate than a big quantum corporation that could emerge as yet another internal rival.

3. ‘New IP’ and good old surveillance

Since 2019 China has been proposing to reform radically the architecture of the internet. At the heart of its ‘many-nets’ approach is the proposal to divide the internet into several smaller subnetworks that are connected (or can be decoupled) via gateways that are strongly policed. The new protocol also makes for a strong binding of user identity and the screening of online behaviour at the level of transport layers and connections points such as routers, which offers new opportunities for surveillance and control.

Largely dismissed by experts, ‘New IP’ offers an indication of travel should China gain the upper hand in mandating standards for the quantum internet: split into several layers, each tightly integrated with domestic control regimes, the internet would indeed fragment. It must be assumed that China does not believe ‘New IP’ to be a winning proposal. Rather it must be considered a strong signal that China is soon fully able to decouple from the West, both figuratively and literally, and run its own sub-internet. This development could generate normative pull and interest from other authoritarian state actors who have similar preferences with regard to restricting internet activity. Not a polished proposal, ‘New IP’ is a strong signal of confidence, intent and ambition.

4. The UK’s response

For the British government, the main concern that arises from Chinese quantum capabilities is the threat to British IPR. While these concerns should not be dismissed, they seem to reflect a view of China as primarily playing catchup and seeking to copy Western technologies. Should China continue to progress in developing quantum internet technologies, however, the threat level to British IPR might be less considerable than the government presently believes it to be. In its preoccupation with IPR, there is a risk to lose sight of the challenges that Chinese dominance in quantum internet technologies may present.

GCHQ recommends the government and businesses to wait for quantum-proof internet standards ‘to appear’, in the words of its participant. While the US and its allies have traditionally enjoyed considerable influence at internet and telecommunications standardisation bodies, they are now facing an increasingly confident and assertive China that pushes for its own vision of an internet of the future. Informants note a return to ‘military driven processes’ in internet governance at the demise of the multi-stakeholder model. The ratification of standards to Western approval is going to be much more difficult than it used to be. Interview data suggest that the UK government is at risk of underestimating the issue of power play in internet governance at present.

5. The quantum internet will create new dependency risks for the UK

Large US corporations already dominate Web services in the UK, in particular social media and cloud storage markets. Since 2018, they have also begun to buy up critical internet infrastructure, in particular undersea fibre cables. Many of these firms also invest in developing quantum networks. They are in a strong position to offer commercial quantum internet services when the quantum internet arrives.

Should dominant players in the cloud services market be able to offer Quantum Computing as a Service (QCaas), or quantum cloud as a service, ahead of other companies, their dominant position is likely to cement further. These companies are headquartered in the US and as such beyond the reach of UK regulators.[1] For the UK economy, the advent of the quantum internet would create new critical

[1] The UK can, of course, regulate their behaviour on UK markets.

infrastructural dependencies on the US private sector.

6. China dominates the quantum patenting landscape

The analysis of 4,200 patent families in quantum internet technologies and the 10,000+ patents they cite as ‘prior art’ suggests that while roughly on a par with the US in 2015, the starting period of this research, at the beginning of 2022, China dominated the quantum computing and communication patenting landscape and significantly outperformed the US in terms of annual patent registrations. While the biggest registering organisations by number of filings are large US companies, China has successfully developed a large number of small to mid-sized companies that register quantum patents at significant pace.

Over a five-year period, the annual number of patents that organisations headquartered in China have registered, has risen fivefold. China changed gears around 2015 and is now pursuing its quantum development programme at full throttle. Overall, the Chinese quantum internet patent network is twice the size of its American counterpart.

7. Strong evidence of significant preferential treatment in China and the US

There is strong evidence of preferential treatment of domestic quantum technologies in US and Chinese patenting activity and citation practices. Chinese quantum patents overwhelmingly cite other Chinese patents as prior art, and the US patenting behaviour is no different. This phenomenon suggests the evolution of two separate quantum internet research ecosystems that evolve independently of each other. Neither programme relies on its strategic rival to any meaningful degree. The extent of preferential treatment is such that it cannot be ruled out that the two superpowers deliberately avoid engaging with the work of their strategic rival.

8. US quantum internet patenting activity seems more coordinated

The data suggests that the US patenting network enjoys a better steer compared to its Chinese counterpart. The US network contains one large component of around 1,600 nodes and several floating patents outside it that are not well connected. Surprisingly, the Chinese network has not one but two large components: complete subgraphs of around 2,000 nodes each that do not talk to each other. This suggests a lack of coordination and strategic oversight to the effect that two separate citation networks could form within the same network. Put colloquially, the structure is reminiscent of two university departments at the same institution that research the same issue but are ignorant of each other's existence.

9. Countries of publication, the type of registering organisation and IPC codes drive patenting activity

The data were sliced into three periods (2015-2017, 2017-2019, 2019-2021) to test for the significance of variables that drive Chinese and US patenting activity and to compare them over time. The thesis has found that the country where a patent was filed, the type of organisation that registered it, and the number of IPC codes it was given are highly significant predictors of citation practices.

For example, in the period 2017-2019, in the US country-to-country homophily jumped to nearly 40 percent, meaning that if two patents filed by organisations headquartered in the US were published in the same country, the chance that one cites the other was 40 percent. For the type of applicant, e.g. military-to-military or private sector-to-private sector, the chance of a connection in the network was nearly 20 percent compared to the probability of a random baseline pairing of less than one percent for both examples.

This is significant evidence of preferential treatment not just in terms of excluding foreign inventions, but for 'like-attracts-like' behaviour in patenting activity in both countries. For example, researchers in the military turn primarily to patents published by the military for prior art, or industry turns to industry etc. The significance levels of these variables suggest high degrees of group think and preferences for non-collaboration within two already highly siloed and sealed quantum internet research programmes. Work on the technical components of a future quantum internet is anything but collaborative.

10. Good quantum internet standards should be procured, not hoped for

Drawing on the above findings, the thesis assembled the building blocks of a coalitional game theory model in which utility is transferable. The model suggests that the quantum internet will not be interoperable but fragmented unless the US makes the conscious decision to offer China side payments to shelve its 'New IP' many-nets approach. This was found to be a much more effective way to contain Chinese ambition than the current approach to try and 'shame' China by pointing to the surveillance-and-control parameters of 'New IP'.

The model suggests an allocation rule that specifies how much compensation China can reasonably demand to let go of its ambition to push for Chinese quantum internet standards. The important insight of the model is that it will be strictly beneficial for the US and its allies to make financial sacrifices to obtain a global standard for an open and interoperable quantum internet, even if this requires a change of perspective and perhaps demands some humility: the West is no longer able to implement internet standards at will, standards no longer 'appear', instead they must be procured if the US and its allies hope to avoid a full-blown internet governance conflict with China. Future work in this area should build and evaluate this baseline model further.

The findings of this thesis attest to the extent to which the emergence of the quantum internet is being shaped by US–Chinese strategic competition and the rivalry over emerging technologies that are deemed crucial for winning the twenty-first century. Where do the findings above leave Web Science as a discipline?

8.2 Quantum Web Science

If Web Science is the study of the Web as a complex sociotechnical system and as a discipline questions the narrative that complex problems could be solved by technical solutions alone, it is difficult to imagine a better object to study than the quantum internet. The empirical chapters of this thesis identified numerous axes along which quantum internet technologies are being shaped by political forces. It was found that the current levels of competition, hostility even, between the US and China make for a strong framing of the quantum internet in security terms even before it has fully arrived.

As informants suggested, the issue is exacerbated by an increasingly unpredictable Chinese leadership that would adhere to rules only when they are convenient and ignore them when they are not. In the words of a respondent, this 'makes technical solutions to technical problems really problematic'–an implicit endorsement of Web Science. The current impasse about 'New IP' and its repercussions for a future quantum internet very much encapsulate the spirit of the discipline: good solutions to the problems that relate to the Web, and, by extension, to the internet, require both a technical and a political dimension.

Such a dual perspective is most relevant to the study of internet governance and standards-finding for the internet of the future. The multi-stakeholder model of internet governance has come under significant pressure from a great many sources. As argued throughout the thesis, today military and national security interests enjoy much more privilege, as captured by the heuristic tool of QISG developed in Chapter 2 and applied in Chapter 7. At present, it must be doubted whether internet governance can ever return to a truly democratic, inclusive and representative regime, if indeed it ever was.

Regarding standards, there is a real danger that criticism of 'New IP' quickly degrades to China bashing. This thesis did not intend for that. To say that China is 'playing the system' or to note that the Chinese leadership is flexible in its attitude to norm-following is not to suggest the West, and particular the US, were examples of immaculate behaviour. Above all, it is certainly possible to imagine that some actors in Western governments, who view the internet first and foremost through a securitised lens and narratives of ever-growing threat scenarios, would indeed welcome an internet so tightly controlled–leaving the 'dirty work' of pushing for a harsh governance regime to China as it would be difficult to call unabashedly for such radical reforms at home.

The interviews suggested further that China is pushing ahead in places where it meets little resistance while playing a waiting game in other areas where opposition is stronger. As the informant at the Cabinet Office said, Western officials think in election cycles while the Chinese leadership can plan much longer ahead, waiting for new opportunities to emerge. The policy strategy 'China Standards 2035' is an example of a long-term, credible commitment. This makes internet governance a long game. It is, at the same time, an example of the ways in which the strategic competition between two very different political systems plays out in practice. Given the edge China enjoys in quantum communication, and the patenting of quantum computing and communication overall, when it comes to regulating the quantum internet, the Chinese leadership can afford to sit it out. The US perhaps not so much.

A ‘New IP’/many-nets approach to internet architecture, which would pave the way for a quantum internet, would also allow China to offer hitherto non-aligned countries ‘quantum patronage’: a new infrastructure for secure communication that also provides quantum compute resources at scale. A many-nets systems architecture would translate into more bargaining power for China in internet governance forums. Internet governance should therefore be considered an increasingly powerful tool to reshape the international system. Quantum internet governance is indeed foreign policy by other means, to echo (Abbate 2000). It should be part and parcel of what (Calderaro & Marzouki 2022, p. 3) consider a revised notion of ‘internet diplomacy’, one which ‘extends to foreign affairs and international relations [...], including cybersecurity, internet governance, and the political economy of the internet’.

The push for ‘New IP’, likely to provide a blueprint for the quantum internet, as discussed previously, comes at the time when internet governance itself is at the cusp of significant change. This is because the very object of internet governance is shifting. Today, there are hardly any markets that do not have some digital element to it, even if it is only about sales over an online channel of goods traditionally traded offline. The UK has recognised this long-term structural change to the economy by announcing a new Digital Markets Unit in Parliament in November 2022.

The new regime is supposed to regulate big tech and their platform monopolies better in order to alleviate some of the concerns that have been discussed in this thesis, for example regarding the dominance of US corporations on system-critical markets. When so much of the economy and social life is underpinned by online activity, it makes little sense to keep the governance of the internet strictly separated from other regulatory concerns. Given the promises of a quantum internet for UK businesses and research institutions, the internet will only come to matter more, not less.

This prospect raises the stakes of internet governance even higher. With the 'internet in everything' (DeNardis 2020), the ability to shape how the (quantum) internet will be governed could yield significant influence over other regulatory domains also. Shaping the quantum internet promises returns that reach well beyond the internet and the Web. The regulatory landscape of the future is likely to be characterised by the entanglement of internet governance with the regulation and management of trade, labour, public health and public administration. For Web Science as a discipline, such developments provide an opportunity to push further into the research mainstream.

The degree to which the quantum internet can be separated from other regulatory concerns will depend on the speed of its integration with the 'classical' internet. Should QCasS become a reality rather quickly, the quantum internet will draw up significant governance challenges. Given the current impasse in international forums, extensively discussed in this thesis, against the rising influence of an emboldened China, a rethink is required of how good governance principles can be found. China can no longer be outmanoeuvred easily; a reality that it slowly sinking in among Western policymakers. The foundations of a game theory model suggested in Chapter 7 capture this new inconvenient truth. The model recommends Western policymakers to procure, in pragmatic fashion, good internet standards rather than assume they will appear somehow automatically, as they used to in the past.

Given the deterioration of US–Chinese relations–at the time of submission, the affair of the alleged Chinese spy balloon over sensitive military sites in the US was the latest escalation–these are demanding times for the internet and the Web. For Web Science as the interdisciplinary study of the Web, the question of how the internet, its chief enabling technology, will evolve over the coming years, is of paramount concern. The quantum internet of the future, and by extension the Web, will be shaped to extraordinary degree by US–Chinese competition in a world which, regrettably, is increasingly marked by hostility and tension. But whilst being critical were it needs to be, Web Science as a discipline has always been optimistic about the potential of technology for the public good. As far as promises go, the quantum internet may indeed offer more than a quantum of hope for better research in many important areas of global concern, and for a better future.

Bibliography

Aaronson, S. (2018), Introduction to Quantum Information Science Lecture Notes.
URL: *https://www.scottaaronson.com/qclec.pdf*

Abbas, A., Zhang, L. & Khan, S. U. (2014), 'A literature review on the state-of-the-art in patent analysis', *World Patent Information* **37**, 3–13.
URL: *http://www.sciencedirect.com/science/article/pii/S0172219013001634*

Abbate, J. (2000), *Inventing the Internet*, MIT Press, Cambridge MA.

Academy, Q. (2022), 'Introduction to the Quantum Internet'.
URL: *https://www.qutube.nl/quantum-internet-14/introduction-to-the-quantum-internet-105*

Administration, I. T. (2021), 'United Kingdom Cloud Services Market'.
URL: *https://www.trade.gov/market-intelligence/united-kingdom-cloud-services-market*

Ahmadpoor, M. & Jones, B. F. (2017), 'The dual frontier: Patented inventions and prior scientific advance', *Science* **357**(6351), 583–587.
URL: *https://www.science.org/doi/10.1126/science.aam9527*

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. & Ayyash, M. (2015), 'Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications', *IEEE Communications Surveys Tutorials* **17**(4), 2347–2376.

Alavi, M., Archibald, M., McMaster, R., Lopez, V. & Cleary, M. (2018), 'Aligning theory and methodology in mixed methods research: Before Design Theoretical Placement', *International Journal of Social Research Methodology* **21**(5), 527–540.

URL: *https://www.tandfonline.com/doi/full/10.1080/13645579.2018.1435016*

Alcácer, J. & Gittelman, M. (2006), 'Patent Citations as a Measure of Knowledge Flows: The Influence of Examiner Citations', *The Review of Economics and Statistics* **88**(4), 774–779.
URL: *https://econpapers.repec.org/article/tprrestat/v_3a88_3ay_3a2006_3ai_-3a4_3ap_3a774-779.htm*

Alsop, T. (2022), 'Top barriers to adopting quantum computing 2021'.
URL: *https://www.statista.com/statistics/1287490/hurdles-quantum-computing/*

Altuntas, S., Dereli, T. & Kusiak, A. (2015), 'Forecasting technology success based on patent data', *Technological Forecasting and Social Change* **96**, 202–214.
URL: *https://linkinghub.elsevier.com/retrieve/pii/S0040162515000700*

Andrews, E. L. (2022), China and the United States: Unlikely Partners in AI, Technical report, Stanford University, Stanford CA.
URL: *https://hai.stanford.edu/news/china-and-united-states-unlikely-partners-ai*

ANI (2022), 'China attempting to influence 'international standards' institutions', *ThePrint* .
URL: *https://theprint.in/world/china-attempting-to-influence-international-standards-institutions/910021/*

Arcesati, R. (2019), Chinese tech standards put the screws on European companies, Technical report, MERICS, Berlin.
URL: *https://merics.org/en/analysis/chinese-tech-standards-put-screws-european-companies*

Aristodemou, L. & Tietze, F. (2018), 'The state-of-the-art on Intellectual Property Analytics (IPA): A literature review on artificial intelligence, machine learning and deep learning methods for analysing intellectual property (IP) data', *World Patent Information* **55**, 37–51.
URL: *http://www.sciencedirect.com/science/article/pii/S0172219018300103*

ART (2020), THE RISING INFLUENCE OF CHINA IN INTERGOVERNMEN-

TAL ORGANISATIONS AND STANDARDISATION BODIES, Issues paper, Council of the European Union: General Secretariat, Brussels.
URL: *https://www.consilium.europa.eu/media/54626/the-rising-influence-of-china-in-intergovernmental-organisations-and-standardisation-bodies-17-december-2020.pdf*

Ashford, E. (2021), Reality Check #7: Red-teaming the Interim National Security Strategic Guidance, Technical report, Atlantic Council, Washington DC.
URL: *https://www.atlanticcouncil.org/content-series/reality-check/reality-check-7-red-teaming-the-interim-national-security-strategic-guidance/*

Austrian Academy of Science (2019), 'MICIUS PRIZE PRESENTED TO BLATT, ZEILINGER AND ZOLLER'.
URL: *https://www.oeaw.ac.at/en/detail/news/micius-prize-presented-to-blatt-zeilinger-and-zoller-2*

Azuma, K., Tamaki, K. & Lo, H.-K. (2015), 'All-photonic quantum repeaters', *Nature Communications* **6**(1), 6787.
URL: *https://www.nature.com/articles/ncomms7787*

Baker, F., Li, X., Bao, C. & Yin, K. (2011), Framework for IPv4/IPv6 Translation, Technical Report RFC6144, RFC Editor.
URL: *https://www.rfc-editor.org/info/rfc6144*

Balding, C. & Clarke, D. C. (2019), Who Owns Huawei?, SSRN Scholarly Paper ID 3372669, Social Science Research Network, Rochester, NY.
URL: *https://papers.ssrn.com/abstract=3372669*

Ball, J. (2021), 'Facebook and Google's New Plan? Own The Internet', *Wired UK* .
URL: *https://www.wired.co.uk/article/facebook-google-subsea-cables*

Basberg, B. L. (1987), 'Patents and the measurement of technological change: A survey of the literature', *Research Policy* **16**(2), 131–141.
URL: *https://www.sciencedirect.com/science/article/pii/0048733387900278*

Bauer, M. & Erixon, F. (2020), 'Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls', *ECIPE Occasional Paper* (02), 42.

URL: *https://ecipe.org/wp-content/uploads/2020/05/ECI_20_OccPaper_02_-2020_Technology_LY02.pdf*

Beamer, G. (2002), 'Elite Interviews and State Politics Research', *State Politics & Policy Quarterly* **2**(1), 86–96.
URL: *https://doi.org/10.1177/153244000200200106*

Beardsworth, A. & Keil, T. (1992), 'The Vegetarian Option: Varieties, Conversions, Motives and Careers', *The Sociological Review* **40**(2), 253–293.
URL: *https://doi.org/10.1111/j.1467-954X.1992.tb00889.x*

Bellac, M. L. (2006), *A Short Introduction to Quantum Information and Quantum Computation*, Cambridge University Press, Cambridge, UK ; New York.

Berners-Lee, T. (2019), '30 years on, what's next #ForTheWeb?'.
URL: *https://webfoundation.org/2019/03/web-birthday-30/*

Berners-Lee, T., Weitzner, D. J., Hall, W., O'Hara, K., Shadbolt, N. & Hendler, J. A. (2006), 'A Framework for Web Science', *Foundations and Trends® in Web Science* **1**(1), 1–130.
URL: *http://www.nowpublishers.com/article/Details/WEB-001*

Bernstein, D. J. (2018), 'Is the security of quantum cryptography guaranteed by the laws of physics?', *arXiv:1803.04520 [quant-ph]* .
URL: *http://arxiv.org/abs/1803.04520*

Bernstein, D. J. & Lange, T. (2017), 'Post-quantum cryptography', *Nature* **549**(7671), 188–194.
URL: *http://www.nature.com/articles/nature23461*

Bienenstock, E. J. & Bonacich, P. (2021), 'Eigenvector centralization as a measure of structural bias in information aggregation', *The Journal of Mathematical Sociology* **0**(0), 1–19.
URL: *https://doi.org/10.1080/0022250X.2021.1878357*

Bikard, M. & Fernandez-Mateo, I. (2022), Standing on the Shoulders of (Male) Giants: Gender Inequality and the Technological Impact of Scientific Ideas, SSRN Scholarly Paper 4059813, Social Science Research Network, Rochester,

NY.
URL: *https://papers.ssrn.com/abstract=4059813*

Blakely, R. (2022), "Quantum cryptography' raises possibility of unbreakable codes', *The Times* .
URL: *https://www.thetimes.co.uk/article/quantum-cryptography-raises-possibility-of-unbreakable-codes-jrxx8mw20*

Boellstorff, T., Nardi, B., Pearce, C., Taylor, T. L. & Marcus, G. E. (2012), *Ethnography and Virtual Worlds: A Handbook of Method*, Princeton University Press, Princeton.

Bokulich, A. & Jaeger, G., eds (2010), *Philosophy of Quantum Information and Entanglement*, Cambridge University Press.

Bouwmeester, D., Ekert, A. K. & Zeilinger, A., eds (2013), *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*, Springer Science & Business Media.

Brady, H. E. & Collier, D., eds (2010), *Rethinking Social Inquiry: Diverse Tools, Shared Standards, Second Edition*, second edn, Rowman & Littlefield Publishers, Lanham, MD.

Breitzman, A. F. & Mogee, M. E. (2002), 'The many applications of patent analysis', *Journal of Information Science* **28**(3), 187–205.
URL: *https://doi.org/10.1177/016555150202800302*

Breslin, S. & Croft, S., eds (2013), *Comparative Regional Security Governance*, Routledge, Abingdon.

Bridge, M. (2018), 'I created a monster, admits Tim Berners-Lee, inventor of the world wide web', *The Times* .
URL: *https://www.thetimes.co.uk/article/i-created-a-monster-admits-tim-berners-lee-inventor-of-the-world-wide-web-ps2ht88pq*

Briegel, H. J., Cirac, J. I., Dür, W., Giedke, G. & Zoller, P. (1999), Quantum Repeaters for Quantum Communication, *in* D. Greenberger, W. L. Reiter & A. Zeilinger, eds, 'Epistemological and Experimental Perspectives on Quantum

Physics', Vienna Circle Institute Yearbook [1999], Springer Netherlands, Dordrecht, pp. 147–154.
URL: *https://doi.org/10.1007/978-94-017-1454-9_11*

Brinkmann, S. (2008), Interviewing, *in* 'The SAGE Encyclopedia of Qualitative Research', SAGE Publications, Thousand Oaks CA, pp. 470–472.

Brodie, B. & Brodie, F. M. (1973), *From Crossbow to H-Bomb, Revised and Enlarged Edition*, second edn, Indiana University Press, Bloomington.

Brookshear, G. & Brylow, D. (2020), *Computer Science: An Overview, Global Edition*, thirteenth edn, Pearson, Harlow.

Brose, C. (2020), *The Kill Chain: Defending America in the Future of High-Tech Warfare*, Hachette Books, New York.

Bryman, A. (2012), *Social Research Methods*, fourth edn, Oxford University Press, Oxford, New York.

Buchanan, B. & Corken, R. (2010), 'A toolkit for the systematic analysis of patent data to assess a potentially disruptive technology', *Intellectual Property Office Publications* p. 16.
URL: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_-data/file/312333/informatic-techtoolkit.pdf*

Burgess, M. (2022), 'Iran's Internet Shutdown Hides a Deadly Crackdown — WIRED UK', *WIRED UK* (Security).
URL: *https://www.wired.co.uk/article/iran-protests-2022-internet-shutdown-whatsapp*

Buzan, B. & Hansen, L. (2009), *The Evolution of International Security Studies*, Cambridge University Press, Cambridge.
URL: *https://www.cambridge.org/core/books/evolution-of-international-security-studies/BB04557E83B673F58799E2B62FA83DA1*

Bygrave, L. A. & Bing, J., eds (2009), *Internet Governance: Infrastructure and Institutions*, illustrated edition edn, Oxford University Press, Oxford, New York.

Caimo, A. & Friel, N. (2014), 'Bergm: Bayesian Exponential Random Graphs in

R', *Journal of Statistical Software* **61**(1), 1–25.
URL: *https://www.jstatsoft.org/index.php/jss/article/view/v061i02*

Calderaro, A. & Blumfelde, S. (2022), 'Artificial intelligence and EU security: The false promise of digital sovereignty', *European Security* **31**(3), 415–434.
URL: *https://doi.org/10.1080/09662839.2022.2101885*

Calderaro, A. & Marzouki, M. (2022), Global Internet governance: An unchartered diplomacy terrain, Rowman & Littlefield.
URL: *https://orca.cardiff.ac.uk/id/eprint/146693/*

Calvo, M. A. M. & Rodriguez, E. S. (2006), 'TUGlab User Guide'.
URL: *http://mmiras.webs.uvigo.es/TUGlab/*

Campagna, M., Chen, L., Dagdelen, Ö., Ding, J., Fernick, J. K., Gisin, N., Hayford, D., Jennewein, T., Lütkenhaus, N., Mosca, M., Neill, B., Pecen, M., Perlner, R., Ribordy, G., Schanck, J. M., Stebila, D., Walenta, N., Whyte, W. & Zhang, Z. (2015), Quantum Safe Cryptography and Security - An introduction, benefits, enablers and challenges - June 2015, Technical Report, European Telecommunications Standards Institute.
URL: *https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf*

Carr, M. (2015), 'Power Plays in Global Internet Governance', *Millennium* **43**(2), 640–659.
URL: *https://doi.org/10.1177/0305829814562655*

Carter, W. (2018), Chinese Advances in Emerging Technologies and their Implications for U.S. National Security, Statement Before The House Armed Services Committee, Center for Strategic and International Studies (CSIS), Washington DC.
URL: *https://www.jstor.org/stable/resrep37496*

Castells, M. (2002), *The Internet Galaxy: Reflections on the Internet, Business, and Society*, Oxford University Press, Oxford.

Castelvecchi, D. (2018), 'The quantum internet has arrived (and it hasn't)', *Nature* pp. 289–293.
URL: *http://www.nature.com/articles/d41586-018-01835-3*

Castree, N., Kitchin, R. & Rogers, A. (2013), 'Research Guides: Human Geography: Geopolitics'.
URL: *https://researchguides.dartmouth.edu/human_geography/geopolitics*

Cavelty, M. D. & Balzacq, T., eds (2017), *Routledge Handbook of Security Studies*, Routledge, London.

Cavelty, M. D. & Wenger, A. (2020), 'Cyber security meets security politics: Complex technology, fragmented politics, and networked science', *Contemporary Security Policy* **41**(1), 5–32.
URL: *https://doi.org/10.1080/13523260.2019.1678855*

Centre for Quantum Technologies (2021), 'Introduction to Superconducting Quantum Circuits'.
URL: *https://www.youtube.com/watch?v=TrB2NvR-P5A*

Cerf, V. & Aboba, B. (1993), How the Internet Came to Be, *in* 'The Online User's Encyclopedia', Addison-Wesley.
URL: *http://elk.informatik.hs-augsburg.de/tmp/cdrom-oss/CerfHowInternetCame2B.html*

Chadwick, J. (2020), 'Quantum breakthrough paves way for safer online communication', *Mail Online* .
URL: *https://www.dailymail.co.uk/sciencetech/article-8690343/Quantum-breakthrough-paves-way-safer-online-communication.html*

Chakraborty, M., Byshkin, M. & Crestani, F. (2020), 'Patent citation network analysis: A perspective from descriptive statistics and ERGMs', *PLOS ONE* **15**(12), e0241797.
URL: *https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0241797*

Chi, D. P., Choi, J. W., Kim, J. S. & Kim, T. (2015), 'Lattice Based Cryptography for Beginners'.
URL: *https://eprint.iacr.org/undefined/undefined*

Chiang, M.-H. (2022), Exposing China's Semiconductor Vulnerabilities, Technical report, The Heritage Foundation, Washington DC.
URL: *https://www.heritage.org/asia/commentary/exposing-chinas-*

semiconductor-vulnerabilities

Chivvis, C. S. (2021), 'Biden's Forthcoming National Security Strategy: Making It Real', *Carnegie Endowment for International Peace* .
URL: *https://carnegieendowment.org/2021/11/10/biden-s-forthcoming-national-security-strategy-making-it-real-pub-85734*

Choi, J., Jang, D., Jun, S. & Park, S. (2015), 'A Predictive Model of Technology Transfer Using Patent Analysis', *Sustainability* **7**(12), 16175–16195.
URL: *https://www.mdpi.com/2071-1050/7/12/15809*

Cirac, J. I. & Zoller, P. (1995), 'Quantum Computations with Cold Trapped Ions', *Physical Review Letters* **74**(20), 4091–4094.
URL: *https://link.aps.org/doi/10.1103/PhysRevLett.74.4091*

Claessen, E. (2020), 'Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: The case of Russia and the EU', *Journal of Cyber Policy* **5**(1), 140–157.
URL: *https://doi.org/10.1080/23738871.2020.1728356*

Cohen-Almagor, R. (2011), 'Internet History', *International Journal of Technoethics* **2**(2), 45–64.
URL: *https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/jte.2011040104*

Cohen, E. A. (1996), 'A Revolution in Warfare', *Foreign Affairs* **75**(2), 37–54.
URL: *https://www.jstor.org/stable/20047487*

Čolaković, A. & Hadžialić, M. (2018), 'Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues', *Computer Networks* **144**, 17–39.
URL: *http://www.sciencedirect.com/science/article/pii/S1389128618305243*

Commission, E. (2022), 'The European Quantum Communication Infrastructure (EuroQCI) Initiative — Shaping Europe's digital future'.
URL: *https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci*

Conaway, R. N. & Wardrope, W. J. (2010), 'Do Their Words Really Matter?

Thematic Analysis of U.S. and Latin American CEO Letters', *The Journal of Business Communication (1973)* **47**(2), 141–168.
URL: *https://journals.sagepub.com/doi/abs/10.1177/0021943610364523*

Corden, A. & Sainsbury, R. (2006), 'Using verbatim quotations in reporting qualitative social research: Researchers' views', *ESRC 2136: University of York* p. 37.
URL: *https://www.york.ac.uk/inst/spru/pubs/pdf/verbquotresearch.pdf*

Costello, J. K. & Kania, E. B. (2018), Quantum Hegemony: China's Ambitions and the Challenge to U.S. Innovation Leadership, Technology & National Security, Center for a New American Security, Washington DC.
URL: *https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Quantum-Tech_FINAL.pdf?mtime=20180912133406*

Costigan, S. S. & Lindstrom, G. (2016), 'Policy and the Internet of Things', *Connections* **15**(2), 9–18.
URL: *https://www.jstor.org/stable/26326436*

Craig, W. (2022), 'The History of the Internet in a Nutshell'.
URL: *https://www.webfx.com/blog/web-design/the-history-of-the-internet-in-a-nutshell/*

Crisman-Cox, C. & Gibilisco, M. (2019), 'Estimating signaling games in international relations: Problems and solutions', *Political Science Research and Methods* pp. 1–18.
URL: *https://www.cambridge.org/core/product/identifier/S204984701900058X/type/journal_article*

Dafoe, A. (2015), 'On Technological Determinism: A Typology, Scope Conditions, and a Mechanism', *Science, Technology, & Human Values* **40**(6), 1047–1076.
URL: *http://journals.sagepub.com/doi/10.1177/0162243915579283*

Das, K., Samanta, S. & Pal, M. (2018), 'Study on centrality measures in social networks: A survey', *Social Network Analysis and Mining* **8**(1), 13.
URL: *https://doi.org/10.1007/s13278-018-0493-2*

DCMS, U. G. (2020), Huawei to be removed from UK 5G networks by 2027,

Technical report, DCMS.
URL: *https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027*

DeNardis, L. (2014*a*), *The Global War for Internet Governance*, Yale University Press, New Haven.

DeNardis, L. (2014*b*), *Global War for Internet Governance — Yale University Press*, Yale University Press, New Haven CT.
URL: *https://yalebooks.yale.edu/book/9780300181357/global-war-internet-governance*

DeNardis, L. (2020), *The Internet in Everything: Freedom and Security in a World with No Off Switch*, Yale University Press, New Haven, CT.

DeNardis, L., Cogburn, D. L., Levinson, N. S. & Musiani, F., eds (2020), *Researching Internet Governance: Methods, Frameworks, Futures*, MIT Press, Cambridge MA.

Deutsch, D. (1997), *The Fabric of Reality*, Penguin Books, New York.

Devitt, S. J., Munro, W. J. & Nemoto, K. (2013), 'Quantum error correction for beginners', *Reports on Progress in Physics* **76**(7), 076001.
URL: *http://stacks.iop.org/0034-4885/76/i=7/a=076001*

Dietz, M., Henke, N., Moon, J., Backes, J., Pautasso, L. & Sadeque, Z. (2020), How quantum computing could change financial services — McKinsey, Technical report, McKinsey Insights.
URL: *https://www.mckinsey.com/industries/financial-services/our-insights/how-quantum-computing-could-change-financial-services*

Ding, J., Triolo, P. & Sacks, S. (2018), Chinese Interests Take a Big Seat at the AI Governance Table, Technical report, New America.
URL: *http://newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/*

Durand, A. (2020), New IP, OCTO OCTO-017, ICANN.

Dwyer, S. C. & Buckle, J. L. (2009), 'The Space Between: On Being an Insider-

Outsider in Qualitative Research', *International Journal of Qualitative Methods* **8**(1), 54–63.
URL: *https://doi.org/10.1177/160940690900800105*

Easley, D. & Kleinberg, J. (2010), *Networks, Crowds, and Markets: Reasoning about a Highly Connected World*, Cambridge University Press, Cambridge.

Economides, N. (2001), 'The Microsoft Antitrust Case', *Journal of Industry, Competition and Trade* **1**(1), 7–39.
URL: *https://doi.org/10.1023/A:1011517724873*

Economist, T. (2021), 'China's rulers want more control of big tech', *The Economist* .
URL: *https://www.economist.com/business/2021/04/08/chinas-rulers-want-more-control-of-big-tech*

Economy, E. C. (2018), 'The great firewall of China: Xi Jinping's internet shutdown', *The Guardian* .
URL: *https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown*

EGSA (2011), 'Galileo is the European global satellite-based navigation system'.
URL: *https://www.gsa.europa.eu/european-gnss/galileo/galileo-european-global-satellite-based-navigation-system*

Enemark, C. (2022), 'The enduring problem of 'grey' drone violence', *European Journal of International Security* **7**(3), 304–321.
URL: *https://www.cambridge.org/core/journals/european-journal-of-international-security/article/enduring-problem-of-grey-drone-violence/8E842572F02B1DE5471F40D056EEC1C5*

Ensafi, R., Winter, P., Mueen, A. & Crandall, J. R. (2015), 'Analyzing the Great Firewall of China Over Space and Time', *Proceedings on Privacy Enhancing Technologies* **2015**(1), 61–76.
URL: *https://content.sciendo.com/view/journals/popets/2015/1/article-p61.xml*

Farrell, J. & Saloner, G. (1986), 'Standardization and variety', *Economics Letters*

20(1), 71–74.
URL: *http://www.sciencedirect.com/science/article/pii/0165176586900844*

Feickert, A., Kapp, L., Elsea, J. K. & Harris, L. A. (2018), 'U.S. Ground Forces Robotics and Autonomous Systems (RAS) and Artificial Intelligence (AI): Considerations for Congress', *US Congressional Research Service* (R45392), 47.
URL: *https://fas.org/sgp/crs/weapons/R45392.pdf*

Feldman, M. S., Bell, J. & Berger, M. T. (2003), *Gaining Access: A Practical and Theoretical Guide for Qualitative Researchers*, AltaMira Press, Walnut Creek CA.

Feynman, R. P. (1982), 'Simulating physics with computers', *International Journal of Theoretical Physics* **21**(6-7), 467–488.
URL: *http://link.springer.com/10.1007/BF02650179*

Fitzsimons, J. F. (2017), 'Private quantum computation: An introduction to blind quantum computing and related protocols', *npj Quantum Information* **3**(1), 23.
URL: *https://www.nature.com/articles/s41534-017-0025-3*

Flagship, E. Q. (2022), 'Quantum Repeaters'.
URL: *https://qt.eu/discover-quantum/underlying-principles/quantum-repeaters/*

Flamm, K. (2018), Measuring Moore's Law: Evidence from Price, Cost, and Quality Indexes, Working Paper 24553, National Bureau of Economic Research.
URL: *http://www.nber.org/papers/w24553*

Flick, U. (2008), *Designing Qualitative Research*, SAGE.

Freist, R. (2019), AI & Machine Learning: China, the US, and Japan in the lead with AI patents, Technical report, Hannover Messe, Hanover.
URL: *https://www.hannovermesse.de/en/news/news-articles/china-the-us-and-japan-in-the-lead-with-ai-patents*

Fudenberg, D. (1991), *Game Theory*, 1st edn, MIT Press, Cambridge MA.

Gargeyas, A. (2021), 'China's 'Standards 2035' Project Could Result in a Technological Cold War', *The Diplomat* .

URL: *https://thediplomat.com/2021/09/chinas-standards-2035-project-could-result-in-a-technological-cold-war/*

Gartzke, E. A., Carcelli, S., Gannon, J. A. & Zhang, J. J. (2017), Signaling in Foreign Policy, *in* 'Oxford Research Encyclopedia of Politics', Oxford University Press.
URL: *http://politics.oxfordre.com/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-481*

Gerry, C. C. & Bruno, K. M. (2016), *The Quantum Divide: Why Schrodinger's Cat Is Either Dead or Alive*, reprint edition edn, Oxford University Press, Oxford.

Gertner, J. (2013), *The Idea Factory: Bell Labs and the Great Age of American Innovation*, reprint edn, Penguin, London.

Gibney, E. (2016), 'Chinese satellite is one giant step for the quantum internet', *Nature* **535**(7613), 478–479.
URL: *https://www.nature.com/articles/535478a*

Gibney, E. (2020), 'Quantum computer race intensifies as alternative technology gains steam', *Nature* **587**(7834), 342–343.
URL: *https://www.nature.com/articles/d41586-020-03237-w*

Giles, M. (2019), 'The US and China are in a quantum arms race that will transform warfare', *MIT Technology Review* .
URL: *https://www.technologyreview.com/s/612421/us-china-quantum-arms-race/*

Given, L. M., ed. (2008), *The SAGE Encyclopedia of Qualitative Research Methods*, SAGE Publications, Thousand Oaks CA.

Gnidenko, A. A., Chibisov, A. N., Chibisova, M. A. & Prokhorenko, A. V. (2021), 'Quantum mechanical modelling of phosphorus qubits in silicene under constrained magnetization', *RSC Advances* **11**(54), 33890–33894.
URL: *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9042333/*

Godwin, C. & Clayton, J. (2021), 'Microsoft-led team retracts quantum 'breakthrough'', *BBC News* .

URL: *https://www.bbc.com/news/technology-56328980*

Goldsmith, J. & Wu, T. (2008), *Who Controls the Internet?: Illusions of a Borderless World*, illustrated edition edn, Oxford University Press, New York.

Goldstein, A. (2020), 'China's Grand Strategy under Xi Jinping: Reassurance, Reform, and Resistance', *International Security* **45**(1), 164–201.
URL: *https://www.mitpressjournals.org/doix/abs/10.1162/isec_a_00383*

Gorman, L. (2021), China's Data Ambitions: Strategy, Emerging Technologies, and Implications for Democracies, Technical report, National Bureau of Asian Research, Washington DC.
URL: *https://www.nbr.org/publication/chinas-data-ambitions-strategy-emerging-technologies-and-implications-for-democracies/*

Government, U. (2018), National Strategic Overview for Quantum Information Science, Technical report, National Science and Technology Council, Washington DC.
URL: *https://www.quantum.gov/wp-content/uploads/2020/10/2018_NSTC_National_Strategic_Overview_QIS.pdf*

Government, U. (2021), 'Interim National Security Strategic Guidance'.
URL: *https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf*

Greengard, S. (2015), *The Internet of Things*, MIT Press, Cambridge MA.

Griliches, Z. (1990), 'Patent Statistics as Economic Indicators: A Survey', *Journal of Economic Literature* **28**(4), 1661–1707.
URL: *https://www.jstor.org/stable/2727442*

Gross, A., Murgia, M. & Yang, Y. (2019), 'Chinese tech groups shaping UN facial recognition standards', *Financial Times* .
URL: *https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67*

Grover, L. K. (1996), A Fast Quantum Mechanical Algorithm for Database Search, *in* 'Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing', STOC '96, ACM, New York, NY, pp. 212–219.
URL: *http://doi.acm.org/10.1145/237814.237866*

Hammersley, M. & Atkinson, P. (2007), *Ethnography: Principles in Practice*, 3rd edition edn, Routledge, London, New York.

Han, L. (2020), 'New IP for Future Vehicular Networking'.
URL: *https://www.iaria.org/conferences2020/filesVEHICULAR20/LinHan_-Keynote_NewIP.pdf*

Handcock, M. S., Hunter, D. R., Butts, C. T., Goodreau, S. M. & Morris, M. (2008), 'Statnet: Software Tools for the Representation, Visualization, Analysis and Simulation of Network Data', *Journal of Statistical Software* **24**(1), 1–11.
URL: *https://www.jstatsoft.org/index.php/jss/article/view/v024i01*

Hanson, B. A. (2020), 'The HiveR Package', *CRN R Project* p. 21.
URL: *https://cran.r-project.org/web/packages/HiveR/vignettes/HiveR.pdf*

Hauben, R., Hauben, J., Zorn, W., Chon, K. & Ekeland, A. (2007), 'The Origin and Early Development of the Internet and of the Netizen: Their Impact on Science and Society', *ResearchGate* .

He, Y., Gorman, S. K., Keith, D., Kranz, L., Keizer, J. G. & Simmons, M. Y. (2019), 'A two-qubit gate between phosphorus donor electrons in silicon', *Nature* **571**(7765), 371–375.
URL: *https://www.nature.com/articles/s41586-019-1381-2*

Hendler, J. & Hall, W. (2016), 'Science of the World Wide Web', *Science* **354**(6313), 703–704.
URL: *http://www.sciencemag.org/lookup/doi/10.1126/science.aai9150*

Hermans, S. L. N., Pompili, M., Beukers, H. K. C., Baier, S., Borregaard, J. & Hanson, R. (2022), 'Qubit teleportation between non-neighbouring nodes in a quantum network', *Nature* **605**(7911), 663–668.
URL: *https://www.nature.com/articles/s41586-022-04697-y*

Hill, S. (2022), 'Here's What the 'Matter' Smart Home Standard Is All About', *Wired* .
URL: *https://www.wired.com/story/what-is-matter/*

HM Government (2021*a*), *Defence and Security Industrial Strategy: A Strategic*

Approach to the UK's Defence and Security Industrial Sectors, number CP 410, Ccrown Copyright, London.

HM Government (2021*b*), *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*, number CP 403, HM Stationery Office, London.
URL: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_-data/file/969402/The_Integrated_Review_of_Security__Defence__Development_-and_Foreign_Policy.pdf*

Hoffman, M. (2021*a*), *Methods for Network Analysis.*
URL: *https://bookdown.org/markhoff/social_network_analysis/*

Hoffman, M. (2021*b*), *Methods for Network Analysis.*
URL: *https://bookdown.org/markhoff/social_network_analysis/*

House, U. W. (2021), 'Remarks by President Biden in Address to a Joint Session of Congress'.
URL: *https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/04/29/remarks-by-president-biden-in-address-to-a-joint-session-of-congress/*

Howell, S. T., Rathje, J., Van Reenen, J. & Wong, J. (2021), 'Opening up military innovation: Causal effects of 'bottom-up' reforms to U.S. defense research', *Centre for Economic Performance* **Discussion Paper**(1760).
URL: *http://eprints.lse.ac.uk/114430/1/dp1760.pdf*

Huang, J., Li, W., Huang, X., Wang, Y. & Guo, L. (2020), 'Technology and Innovation in China: A Patent Citation-based Analysis', *Science, Technology and Society* p. 0971721820932020.
URL: *https://doi.org/10.1177/0971721820932020*

Huang, Y. & Smith, J. (2019), 'China's Record on Intellectual Property Rights Is Getting Better and Better', *Foreign Policy* .
URL: *https://foreignpolicy.com/2019/10/16/china-intellectual-property-theft-progress/*

Hui, J. (2019), 'QC — How to build a Quantum Computer with Superconducting

Circuit?', *Medium* .
URL: *https://jonathan-hui.medium.com/qc-how-to-build-a-quantum-computer-with-superconducting-circuit-4c30b1b296cd*

Hunter, D. R., Handcock, M. S., Butts, C. T., Goodreau, S. M. & Morris, M. (2008), 'Ergm: A Package to Fit, Simulate and Diagnose Exponential-Family Models for Networks', *Journal of Statistical Software* **24**(1), 1–29.
URL: *https://www.jstatsoft.org/index.php/jss/article/view/v024i03*

IBM (2022), 'Eagle's quantum performance progress'.
URL: *https://research.ibm.com/blog/eagle-quantum-processor-performance*

IDC (2019), The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, Technical report.
URL: *https://www.idc.com/getdoc.jsp?containerId=prUS45213219*

Insights, F. B. (2020), 'Patent Analytics Market Size, Growth, Share — Industry Report, 2027'.
URL: *https://www.fortunebusinessinsights.com/patent-analytics-market-102774*

Jaffe, A. B. & Trajtenberg, M. (1996), 'Flows of knowledge from universities and federal laboratories: Modeling the flow of patent citations over time and across institutional and geographic boundaries', *Proceedings of the National Academy of Sciences* **93**(23), 12671–12677.
URL: *https://www.pnas.org/content/93/23/12671*

Jaffe, A. B., Trajtenberg, M. & Henderson, R. (1993), 'Geographic Localization of Knowledge Spillovers as Evidenced by Patent Citations', *The Quarterly Journal of Economics* **108**(3), 577–598.
URL: *https://www.jstor.org/stable/2118401*

Jasanoff, S. (2016), *The Ethics of Invention: Technology and the Human Future*, W. W. Norton & Company, New York.

Jasanoff, S., ed. (2004), *States of Knowledge: The Co-production of Science and the Social Order*, 1st edn, Routledge, London.

Jasanoff, S. & Kim, S.-H., eds (2015), *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*, University of Chicago Press, Chicago, London.

Jensen, D. (2008), Access, *in* 'The SAGE Encyclopedia of Qualitative Research', SAGE Publications, Thousand Oaks CA, pp. 1–3.

Ji, Y., Yu, X., Sun, M. & Zhang, B. (2022), 'Exploring the Evolution and Determinants of Open Innovation: A Perspective from Patent Citations', *Sustainability* **14**(3), 1618.
URL: *https://www.mdpi.com/2071-1050/14/3/1618*

Jiang, S. (2019), 'New IP Networking for Network 2030'.
URL: *https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019101416/Documents/Sheng_Jiang_Presentation.pdf*

Jilbert, I. & Lizardo, O. (2020), *Social Networks: An Introduction*, Bookdown.
URL: *https://bookdown.org/omarlizardo/_main/*

Johnson, R. B., Onwuegbuzie, A. J. & Turner, L. A. (2007), 'Toward a Definition of Mixed Methods Research', *Journal of Mixed Methods Research* **1**(2), 112–133.
URL: *https://doi.org/10.1177/1558689806298224*

Kania, E. (2018), 'The Right to Speak: Discourse and Chinese Power', *ccpwatch: Center for Advanced China Research* .
URL: *https://www.ccpwatch.org/single-post/2018/11/27/the-right-to-speak-discourse-and-chinese-power*

Kania, E. B. (2021), 'China's quest for quantum advantage—Strategic and defense innovation at a new frontier', *Journal of Strategic Studies* **44**(6), 922–952.
URL: *https://doi.org/10.1080/01402390.2021.1973658*

Kennedy, S. (2015), 'Made in China 2025'.
URL: *https://www.csis.org/analysis/made-china-2025*

Keohane, R. (2003), *Power and Governance in a Partially Globalized World*, Routledge, London, New York.

Kersten, A., Athanasia, G. & Arcuri, G. (2022), 'What Can Patent Data Reveal

about U.S.-China Technology Competition?'.
URL: *https://www.csis.org/analysis/what-can-patent-data-reveal-about-us-china-technology-competition*

Kimble, H. J. (2008), 'The quantum internet', *Nature* **453**(7198), 1023–1030.
URL: *http://www.nature.com/articles/nature07127*

Kirchner, E. J. & Sperling, J., eds (2007), *Global Security Governance — Taylor & Francis Group*, 1st edn, Routledge, London.
URL: *https://www.taylorfrancis.com/books/global-security-governance-emil-kirchner-james-sperling/e/10.4324/9780203964705*

Kitaev, A. (2022), 'Shor's algorithm'.
URL: *https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm*

Kolodziej, E. A. (1992), 'Renaissance in Security Studies? Caveat Lector!', *International Studies Quarterly* **36**(4), 421–438.
URL: *https://doi.org/10.2307/2600733*

Kolodziej, E. A. (2005), *Security and International Relations*, Cambridge University Press, Cambridge.

Kramp, T., van Kranenburg, R. & Lange, S. (2013), Introduction to the Internet of Things, *in* A. Bassi, M. Bauer, M. Fiedler, T. Kramp, R. van Kranenburg, S. Lange & S. Meissner, eds, 'Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model', Springer, Berlin, Heidelberg, pp. 1–10.
URL: *https://doi.org/10.1007/978-3-642-40403-0_1*

Krause, J. (2021*a*), 'The Quantum Internet: A Network for All?'.
URL: *https://www.ippi.org.il/the-quantum-internet-a-network-for-all/*

Krause, J. (2021*b*), Trusted autonomous systems in defence: A policy landscape review, Technical report, King's College London, London.
URL: *https://doi.org/10.18742/pub01-063*

Kuo, M. A. (2022), 'The Difference Between America's 2 Cold Wars'.

URL: *https://thediplomat.com/2022/05/the-difference-between-americas-2-cold-wars/*

Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C. & O'Brien, J. L. (2010), 'Quantum computers', *Nature* **464**(7285), 45–53.
URL: *https://www.nature.com/articles/nature08812*

Lamont, C. K. (2015), *Research Methods in International Relations*, 1st edn, Sage, Los Angeles. Research methods in international relations – Research questions and research design – Research ethics – Writing a literature review – Qualitative methods in international relations – Quantitative methods in international relations – Mixed methods research in international relations – Case study research in international relations – Field research in international relations – Writing up your research.

Laplante, P. A., ed. (2018), *Comprehensive Dictionary of Electrical Engineering*, CRC Press.

Le, D.-N., Pandey, A. K., Tadepalli, S., Rathore, P. S. & Chatterjee, J. M. (2019), *Network Modeling, Simulation and Analysis in MATLAB: Theory and Practices*, Wiley-Scrivener.

Lehman II, R. F. (2013), Future Technology and Strategic Stability, *in* 'Strategic Stability: Contending Interpretations', U.S. Army War College Press, Carlisle Barracks PA, pp. 147–200.

Leifeld, P. (2013), '**Texreg** : Conversion of Statistical Model Output in *R* to L A T E X and HTML Tables', *Journal of Statistical Software* **55**(8).
URL: *http://www.jstatsoft.org/v55/i08/*

Lele, A. (2021), *Quantum Technologies and Military Strategy*, 1st ed edn, Springer.

Lerner, J. & Seru, A. (2017), 'The Use and Misuse of Patent Data: Issues for Corporate Finance and Beyond', *Harvard Business School Working Paper Series* (18-042), 129.

Levy, I. (2022), 'Advanced Technologies and Geostrategic Instability: A Conversation with Dr Ian Levy OBE'.

URL: *https://rusi.org/events/open-to-all/null*

Li, Z. & Qi, H. (2022), 'Platform power: Monopolisation and financialisation in the era of big tech', *Cambridge Journal of Economics* p. beac054.
URL: *https://doi.org/10.1093/cje/beac054*

Liao, S.-K., Cai, W.-Q., Handsteiner, J., Liu, B., Yin, J., Zhang, L., Rauch, D., Fink, M., Ren, J.-G., Liu, W.-Y., Li, Y., Shen, Q., Cao, Y., Li, F.-Z., Wang, J.-F., Huang, Y.-M., Deng, L., Xi, T., Ma, L., Hu, T., Li, L., Liu, N.-L., Koidl, F., Wang, P., Chen, Y.-A., Wang, X.-B., Steindorfer, M., Kirchner, G., Lu, C.-Y., Shu, R., Ursin, R., Scheidl, T., Peng, C.-Z., Wang, J.-Y., Zeilinger, A. & Pan, J.-W. (2018), 'Satellite-Relayed Intercontinental Quantum Network', *Physical Review Letters* **120**(3), 030501.
URL: *https://link.aps.org/doi/10.1103/PhysRevLett.120.030501*

Liao, S.-K., Cai, W.-Q., Liu, W.-Y., Zhang, L., Li, Y., Ren, J.-G., Yin, J., Shen, Q., Cao, Y., Li, Z.-P., Li, F.-Z., Chen, X.-W., Sun, L.-H., Jia, J.-J., Wu, J.-C., Jiang, X.-J., Wang, J.-F., Huang, Y.-M., Wang, Q., Zhou, Y.-L., Deng, L., Xi, T., Ma, L., Hu, T., Zhang, Q., Chen, Y.-A., Liu, N.-L., Wang, X.-B., Zhu, Z.-C., Lu, C.-Y., Shu, R., Peng, C.-Z., Wang, J.-Y. & Pan, J.-W. (2017), 'Satellite-to-ground quantum key distribution', *Nature* **549**(7670), 43–47.
URL: *https://www.nature.com/articles/nature23655*

Lin, Y., Chen, J. & Chen, Y. (2011), 'Backbone of technology evolution in the modern era automobile industry: An analysis by the patents citation network', *Journal of Systems Science and Systems Engineering* **20**(4), 416–442.
URL: *http://link.springer.com/10.1007/s11518-011-5181-y*

Lindsay, J. R. (2020), 'Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage', *Security Studies* **29**(2), 335–361.
URL: *https://doi.org/10.1080/09636412.2020.1722853*

Lindsay, J. R., ed. (2015), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford University Press, New York.

Liu, N., Shapira, P., Yue, X. & Guan, J. (2021), 'Mapping technological innovation dynamics in artificial intelligence domains: Evidence from a global patent analysis', *PLOS ONE* **16**(12), e0262050.

URL: *https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0262050*

Lo, H.-K., Popescu, S. & Spiller, T., eds (2000), *Introduction to Quantum Computation and Information*, World Scientific Publishing, Singapore.

Lusher, D., Koskinen, J. & Robins, G., eds (2012*a*), *Exponential Random Graph Models for Social Networks: Theory, Methods, and Applications*, Structural Analysis in the Social Sciences, Cambridge University Press, Cambridge.
URL: *https://www.cambridge.org/core/books/exponential-random-graph-models-for-social-networks/9296EE2B53CDEF9FE9E2E981E2FDB8A8*

Lusher, D., Koskinen, J. & Robins, G., eds (2012*b*), *Exponential Random Graph Models for Social Networks: Theory, Methods, and Applications: 35*, illustrated edition edn, Cambridge University Press, Cambridge.

MacKenzie, D. & Wajcman, J. (1999), *The Social Shaping of Technology*, second edn, Open University Press, Buckingham, Philadelphia PA.

Madden, R. (2010), *Being Ethnographic: A Guide to the Theory and Practice of Ethnography*, SAGE Publications, London.

Marmor, A. C., Lawson, W. S. & Terapane, J. F. (1979), ‘The technology assessment and forecast program of the United States patent and trademark office’, *World Patent Information* **1**(1), 15–23.
URL: *https://www.sciencedirect.com/science/article/pii/0172219079900061*

Maschler, M., Solan, E. & Zamir, S. (2013), *Game Theory*, Cambridge University Press, Cambridge.

Mason, J. (2002), *Qualitative Researching*, SAGE Publications, London.

Maxcy, S. (2003), Pragmatic Threads in Mixed Method Research in the Social Sciences: The Search for Multiple Modes of Inquiry and the End of the Philosophy of Formalism, *in* ‘Handbook of Mixed Methods in the Social and Behavioural Sciences’, SAGE Publications, Thousand Oaks CA, pp. 51–89.

Mbeba (2021), ‘China Standards 2035 – Shaping the World of Tomorrow?’.
URL: *https://eac-consulting.de/china-standards-2035/*

McCambridge, J., Witton, J. & Elbourne, D. R. (2014), 'Systematic review of the Hawthorne effect: New concepts are needed to study research participation effects', *Journal of Clinical Epidemiology* **67**(3), 267–277.
URL: *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3969247/*

Meddeb, A. (2016), 'Internet of things standards: Who stands out from the crowd?', *IEEE Communications Magazine* **54**(7), 40–47.

Meghanathan, N. (2016), 'Assortativity Analysis of Real-World Network Graphs based on Centrality Metrics', *Computer and Information Science* **9**(3), p7.
URL: *https://ccsenet.org/journal/index.php/cis/article/view/59661*

Mehta, R. N. (2021), 'Extended deterrence and assurance in an emerging technology environment', *Journal of Strategic Studies* **44**(7), 958–982.
URL: *https://www.tandfonline.com/doi/full/10.1080/01402390.2019.1621173*

Meinhardt, H. I. (n.d.), 'The Matlab Game Theory Toolbox MatTuGames Version 0.4: An Introduction, Basics, and Examples', p. 161.

Mermin, N. D. (2007), *Quantum Computer Science: An Introduction*, Cambridge University Press, Cambridge.

Metz, C. (2022), "Quantum Internet' Inches Closer With Advance in Data Teleportation', *The New York Times* .
URL: *https://www.nytimes.com/2022/05/25/technology/quantum-internet-teleportation.html*

MOD Developments, Concepts and Doctrine Centre (2018), Human-Machine Teaming, Joint Concept Note 1/18, Ministry of Defence, Swindon.
URL: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_-data/file/709359/20180517-concepts_uk_human_machine_teaming_jcn_1_18.pdf*

Moore, G. E. (1965), 'Cramming more components onto integrated circuits', *Electronics* **38**(8).
URL: *https://drive.google.com/file/d/0By83v5TWkGjvQkpBcXJKT1I1TTA/view*

Mortimer, H. (2019), 'Competition policy in the age of digital platforms: What's at stake'.

URL: *https://blogs.lse.ac.uk/businessreview/2019/08/19/competition-policy-in-the-age-of-digital-platforms-whats-at-stake/*

Mosley, L. (2013), *Interview Research in Political Science*, illustrated edition edn, Cornell University Press, Ithaca.

Mueller, M. (2017), *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*, 1st edn, Polity, Cambridge, Malden MA.

Mueller, M. (2022), 'What Is Internet Governance?'.
URL: *https://www.internetgovernance.org/what-is-internet-governance/*

Mukhopadhyay, S. C., ed. (2014), *Internet of Things: Challenges and Opportunities*, Smart Sensors, Measurement and Instrumentation, Springer International Publishing.
URL: *https://www.springer.com/gb/book/9783319042220*

Musiani, F., Cogburn, D. L., DeNardis, L. & Levinson, N. S., eds (2015), *The Turn to Infrastructure in Internet Governance*, 1st edn, Palgrave Macmillan, New York, NY.

Mussmann, S., Moore, J., Iii, J. J. P. & Neville, J. (2015), 'Incorporating Assortativity and Degree Dependence into Scalable Network Models', *Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence* p. 9.
URL: *https://www.aaai.org/ocs/index.php/AAAI/AAAI15/paper/viewFile/9999/9250*

NATO Allied Command Transformation (2016), *Autonomous Systems: Íssues for Defence Policymakers*, NATO HG SACT, Norfolk, Va.
URL: *https://www.act.nato.int/images/stories/media/capdev/capdev_02.pdf*

Naughton, J. (2016), 'The evolution of the Internet: From military experiment to General Purpose Technology', *Journal of Cyber Policy* **1**(1), 5–28.
URL: *http://www.tandfonline.com/doi/full/10.1080/23738871.2016.1157619*

Nazareth, D. L. & Choi, J. (2021), 'Market Share Strategies for Cloud Computing Providers', *Journal of Computer Information Systems* **61**(2), 182–192.
URL: *https://doi.org/10.1080/08874417.2019.1576022*

NCSC (2020), Quantum security technologies, White Paper, GCHQ.

URL: *https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies*

News, B. (2020), 'China attacks UK's 'groundless' Huawei 5G ban', *BBC News* .
URL: *https://www.bbc.com/news/technology-53412678*

News, B. (2022*a*), 'Two Huawei 5G kit-removal deadlines put back', *BBC News* .
URL: *https://www.bbc.com/news/technology-63242336*

News, B. (2022*b*), 'US bans sale of Huawei, ZTE tech amid security fears', *BBC News* .
URL: *https://www.bbc.com/news/world-us-canada-63764450*

Nielsen, M. A. & Chuang, I. L. (2010), *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th anniversary edition edn, Cambridge University Press, Cambridge, New York.

Niemietz, D., Farrera, P., Langenfeld, S. & Rempe, G. (2021), 'Nondestructive detection of photonic qubits', *Nature* **591**(7851), 570–574.
URL: *https://www.nature.com/articles/s41586-021-03290-z*

NIST (2022), 'NIST Announces First Four Quantum-Resistant Cryptographic Algorithms'.
URL: *https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms*

Nordrum, A. (2016), 'Quantum Computer Comes Closer to Cracking RSA Encryption', *IEEE Spectrum: Technology, Engineering, and Science News* .
URL: *https://spectrum.ieee.org/tech-talk/computing/hardware/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment*

Normile, D. (2017), 'Science suffers as China's internet censors plug holes in Great Firewall', *Science — AAAS* .
URL: *https://www.sciencemag.org/news/2017/08/science-suffers-china-s-internet-censors-plug-holes-great-firewall*

NSF (2020), 'Invention, Knowledge Transfer, and Innovation'.
URL: *https://ncses.nsf.gov/pubs/nsb20204/invention-u-s-and-comparative-global-trends*

NSTC (2022), Critical and Emerging Technologies List Update, Technical report, Executive Office of the President of the United States, Washington DC.
URL: *https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf*

Nye, J. S. (2005), *Soft Power: The Means To Success In World Politics*, illustrated edition edn, Public Affairs, New York.

Nye, J. S. (2019), 'Soft Power and Public Diplomacy Revisited', *The Hague Journal of Diplomacy* **14**(1-2), 7–20.
URL: *https://brill.com/view/journals/hjd/14/1-2/article-p7_2.xml*

O'Hara, K. & Hall, W. (2014), Web Science, *in* W. H. Dutton, ed., 'The Oxford Handbook of Internet Studies', reprint edition edn, Oxford University Press, Oxford, pp. 48–68.

O'Hara, K. & Hall, W. (2018), 'Four Internets: The Geopolitics of Digital Governance', *Centre for International Governance Innovation* **CIGI 206**.
URL: *https://www.cigionline.org/publications/four-internets-geopolitics-digital-governance*

Osborne, M. J. & Rubinstein, A. (1994), *A Course in Game Theory*, The MIT Press, Cambridge MA.

Pang, X.-L., Yang, A.-L., Zhang, C.-N., Dou, J.-P., Li, H., Gao, J. & Jin, X.-M. (2020), 'Hacking Quantum Key Distribution via Injection Locking', *Physical Review Applied* **13**(3), 034008. Comment: 10 pages, 8 figures, 4 tables.
URL: *http://arxiv.org/abs/1902.10423*

Parker, E., Gonzales, D., Kochhar, A. K., Litterer, S., O'Connor, K., Schmid, J., Scholl, K., Silberglitt, R., Chang, J., Eusebi, C. A. & Harold, S. W. (2022), *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology*, number RR-A869-1, RAND Corporation.
URL: *https://www.rand.org/pubs/research_reports/RRA869-1.html*

Patton, M. Q. (2015), *Qualitative Research & Evaluation Methods: Integrating Theory and Practice*, fourth edn, SAGE Publications, Thousand Oaks CA.

Paul, C., Schwille, M., Vasseur, M., Bartels, E. M. & Bauer, R. (2022), The Role of Information in U.S. Concepts for Strategic Competition, Technical report, RAND Corporation.
URL: *https://www.rand.org/pubs/research_reports/RRA1256-1.html*

Pavitt, K. (1984), 'Sectoral patterns of technical change: Towards a taxonomy and a theory', *Research Policy* **13**(6), 343–373.
URL: *https://www.sciencedirect.com/science/article/pii/0048733384900180*

Peleg, B. & Sudhölter, P. (2007), *Introduction to the Theory of Cooperative Games*, Springer, Berlin.

Peng Er, L. (2021), 'Singapore-China relations in geopolitics, economics, domestic politics and public opinion: An awkward "special relationship"?', *Journal of Contemporary East Asia Studies* **10**(2), 203–217.
URL: *https://doi.org/10.1080/24761028.2021.1951480*

Pereira, M., Curty, M. & Tamaki, K. (2019), 'Quantum key distribution with flawed and leaky sources', *npj Quantum Information* **5**(1).
URL: *http://www.nature.com/articles/s41534-019-0180-9*

Peyman, H. (2018), *China's Change: The Greatest Show On Earth*, World Scientific.

Pires, F. (2021), 'IBM Announces 127-qubit "Eagle" Quantum Processor', *Tom's Hardware* .
URL: *https://www.tomshardware.com/news/ibm-127-qubit-eagle-quantum-processor*

Pompili, M., Hermans, S. L. N., Baier, S., Beukers, H. K. C., Humphreys, P. C., Schouten, R. N., Vermeulen, R. F. L., Tiggelman, M. J., dos Santos Martins, L., Dirkse, B., Wehner, S. & Hanson, R. (2021), 'Realization of a multinode quantum network of remote solid-state qubits', *Science* **372**(6539), 259–264.
URL: *https://www.science.org/doi/10.1126/science.abg1919*

Ponnusamy, K. & Rajagopalan, N. (2018), Internet of Things: A Survey on IoT Protocol Standards, *in* K. Saeed, N. Chaki, B. Pati, S. Bakshi & D. P. Mohapatra, eds, 'Progress in Advanced Computing and Intelligent Engineering', Advances in Intelligent Systems and Computing, Springer, Singapore, pp. 651–663.

Porter, A. L., Garner, J., Carley, S. F. & Newman, N. C. (2019), 'Emergence scoring to identify frontier R&D topics and key players', *Technological Forecasting and Social Change* **146**, 628–643.
URL: *https://www.sciencedirect.com/science/article/pii/S0040162517314804*

Preskill, J. (2004), Chapter 7: Quantum Error Correction.
URL: *http://www.theory.caltech.edu/people/preskill/ph229/notes/chap7.pdf*

Preskill, J. (2013), 'Quantum Computing & the Entanglement Frontier - Institute for Quantum Computing and California Institute of Technology Public Engagement Lecture'.
URL: *https://www.youtube.com/watch?v=3XbQpUtqgnU*

Preskill, J. (2021), 'Quantum computing 40 years later'. Comment: 49 pages. To appear in Feynman Lectures on Computation, 2nd edition, published by Taylor & Francis Group, edited by Anthony J. G. Hey. (v2) typos corrected.
URL: *http://arxiv.org/abs/2106.10522*

Radu, R. (2019), *Negotiating Internet Governance*, illustrated edition edn, Oxford University Press, Oxford, New York.

Radu, R., Chenou, J.-M. & Weber, R. H., eds (2014), *The Evolution of Global Internet Governance: Principles and Policies in the Making*, Springer-Verlag, Berlin, Heidelberg.
URL: *https://www.springer.com/gp/book/9783642452987*

Radu, R., Kettemann, M. C., Meyer, T. & Shahin, J. (2021), 'Normfare: Norm entrepreneurship in internet governance', *Telecommunications Policy* **45**(6), 102–148.
URL: *https://www.sciencedirect.com/science/article/pii/S0308596121000525*

Raymond, M. & Welch, D. A. (2022), 'What's Really Going On in the South China Sea?', *Journal of Current Southeast Asian Affairs* **41**(2), 214–239.
URL: *https://doi.org/10.1177/18681034221086291*

Richards, L. & Morse, J. M. (2012), *README FIRST for a User's Guide to Qualitative Methods*, 3rd edn, SAGE Publications, Los Angeles.

Rivest, R. L., Shamir, A. & Adleman, L. (1978), 'A Method for Obtaining Digital Signatures and Public-Key Cryptosystems', *Communications of the ACM* **21**(2), 15.

Robbins, C., Hill, D. & Boroush, M. (2020), 'Invention, Knowledge Transfer, and Innovation — NSF - National Science Foundation'.
URL: *https://ncses.nsf.gov/pubs/nsb20204/invention-u-s-and-comparative-global-trends*

Rochet, J.-C. & Tirole, J. (2003), 'Platform Competition in Two-Sided Markets', *Journal of the European Economic Association* **1**(4), 990–1029.
URL: *https://academic.oup.com/jeea/article/1/4/990/2280902*

Roffe, J. (2019), 'Quantum Error Correction: An Introductory Guide', *Contemporary Physics* **60**(3), 226–245. Comment: 29 pages, 10 figures. Comments welcome! Provisionally accepted by Contemporary Physics journal.
URL: *http://arxiv.org/abs/1907.11157*

Rothe, J., ed. (2015), *Economics and Computation: An Introduction to Algorithmic Game Theory, Computational Social Choice, and Fair Division*, Springer, Berlin.

Rotman, D. (2020), 'We're not prepared for the end of Moore's Law', *MIT Technology Review* .
URL: *https://www.technologyreview.com/2020/02/24/905789/were-not-prepared-for-the-end-of-moores-law/*

Rotolo, D., Hicks, D. & Martin, B. R. (2015), 'What is an emerging technology?', *Research Policy* **44**(10), 1827–1843.
URL: *https://www.sciencedirect.com/science/article/pii/S0048733315001031*

Roughgarden, T. (2016), *Twenty Lectures on Algorithmic Game Theory*, Cambridge University Press, Cambridge, New York.

Ruf, M., Wan, N. H., Choi, H., Englund, D. & Hanson, R. (2021), 'Quan-

tum networks based on color centers in diamond', *Journal of Applied Physics* **130**(7), 070901.
URL: *https://aip.scitation.org/doi/10.1063/5.0056534*

Ryu, W. & Kim, Y. (2022), 'A study of factors affecting citation of patents: Focusing on US automotive patents', *Journal of Digital Convergence* **20**(3), 283–295.
URL: *https://www.koreascience.or.kr/article/JAKO202210451639592.page*

Saldana, J. (2012), *The Coding Manual for Qualitative Researchers*, 2nd edition edn, Sage Publications Ltd, Los Angeles.

Schaake, M. (2021), 'Big Tech is trying to take governments' policy role', *Financial Times* .
URL: *https://www.ft.com/content/7f85a5ff-326f-490c-9873-013527c19b8f*

Schaefer, B. D. & Pletka, D. (2022), Countering China's Growing Influence at the International Telecommunication Union, Backgrounder 3689, The Heritage Foundation, Washington DC.

Schmid, C. S. & Desmarais, B. A. (2017), 'Exponential Random Graph Models with Big Networks: Maximum Pseudolikelihood Estimation and the Parametric Bootstrap', *arXiv:1708.02598 [stat]* .
URL: *http://arxiv.org/abs/1708.02598*

Schneider-Petsinger, M., Wang, J., Jie, Y. & Crabtree, J. (2019), 'US–China Strategic Competition: The Quest for Global Technological Leadership', *Chatham House Research Paper* p. 45.
URL: *https://www.chathamhouse.org/sites/default/files/publications/research/CHHJ7480-US-China-Competition-RP-WEB.pdf*

Schroeder, U. C. (2011), *The Organization of European Security Governance: Internal and External Security in Transition*, Routledge, Abingdon.

Schwartz, H. A. & Montfort, P. (2022), 'Significant Cyber Incidents — Center for Strategic and International Studies'.
URL: *https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents*

Scott, M. (2019), 'What's driving Europe's new aggressive stance on tech', *POLITICO* .
URL: *https://www.politico.eu/article/europe-digital-technological-sovereignty-facebook-google-amazon-ursula-von-der-leyen/*

Searle, N. (2021), The economic and innovation impacts of trade secrets, Technical report, HM Government's Intellectual Property Office, London.
URL: *https://www.gov.uk/government/publications/economic-and-innovation-impacts-of-trade-secrets/the-economic-and-innovation-impacts-of-trade-secrets*

Shane, S. & Wakabayashi, D. (2018), "The Business of War': Google Employees Protest Work for the Pentagon', *The New York Times* .
URL: *https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html*

Shapiro, C. & Varian, H. R. (1999*a*), 'The Art of Standards Wars', *California Management Review* **41**(2), 8–32.
URL: *https://doi.org/10.2307/41165984*

Shapiro, C. & Varian, H. R. (1999*b*), 'The Art of Standards Wars', *California Management Review* **41**(2), 8–32.
URL: *https://faculty.haas.berkeley.edu/shapiro/wars.pdf*

Sharp, H. & Kolkman, O. (2020), Discussion Paper: An analysis of the "New IP" proposal to the ITU-T, *in* 'Internet Society', Internet Society.
URL: *https://www.internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/*

Shenton, A. K. & Hayter, S. (2004), 'Strategies for Gaining Access to Organisations and Informants in Qualitative Studies', *Education for Information* **22**, 223–231.

Shivakumar, S. (2022), 'Securing Global Standards for Innovation and Growth', *CSIS Research* (Renewing American Innovation Project).
URL: *https://www.csis.org/analysis/securing-global-standards-innovation-and-growth*

Shor, P. (1994), Algorithms for quantum computation: Discrete logarithms and

factoring, *in* 'Proceedings 35th Annual Symposium on Foundations of Computer Science', IEEE Comput. Soc. Press, Santa Fe, NM, USA, pp. 124–134.
URL: *http://ieeexplore.ieee.org/document/365700/*

Shor, P. W. (1997), 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer', *SIAM Journal on Computing* **26**(5), 1484–1509. Comment: 28 pages, LaTeX. This is an expanded version of a paper that appeared in the Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. 20–22, 1994. Minor revisions made January, 1996.
URL: *http://arxiv.org/abs/quant-ph/9508027*

Shuliang, L. (2022), 'The Metaverse: Framework, quantum strategies, technologies and analytics. Keynote Speech Cambridge England March 2022'.

Shy, O. (2011), 'A Short Survey of Network Economics', *Review of Industrial Organization* **38**(2), 119–149.
URL: *http://link.springer.com/10.1007/s11151-011-9288-6*

Siow, E., Tiropanis, T. & Hall, W. (2019), 'Analytics for the Internet of Things: A Survey', *ACM Computing Surveys* **51**(4), 1–36.
URL: *https://dl.acm.org/doi/10.1145/3204947*

Smith, L. (2018), 'Text - H.R.6227 - 115th Congress (2017-2018): National Quantum Initiative Act'.
URL: *https://www.congress.gov/bill/115th-congress/house-bill/6227/text*

Sobel, J. (2009), Signaling Games, *in* R. A. Meyers, ed., 'Encyclopedia of Complexity and Systems Science', Springer, New York, NY, pp. 8125–8139.
URL: *https://doi.org/10.1007/978-0-387-30440-3_481*

Solon, O. (2017), 'Tim Berners-Lee on the future of the web: 'The system is failing'', *The Guardian* .
URL: *https://www.theguardian.com/technology/2017/nov/15/tim-berners-lee-world-wide-web-net-neutrality*

Sperling, J. & Webber, M. (2014), 'Security governance in Europe: A return to system', *European Security* **23**(2), 126–144.

URL: *http://www.tandfonline.com/doi/abs/10.1080/09662839.2013.856305*

Spoehr, T. (2021), 'Hits & Misses in Biden's Interim National Security Guidance'.
URL: *https://www.heritage.org/defense/commentary/hits-misses-bidens-interim-national-security-guidance*

Srivastava, S. (2021), 'Algorithmic Governance and the International Politics of Big Tech', *Perspectives on Politics* pp. 1–12.
URL: *https://www.cambridge.org/core/journals/perspectives-on-politics/article/algorithmic-governance-and-the-international-politics-of-big-tech/3C04908735A5F2EE8A70AFED647741FB*

Stake, R. E. (1995), *The Art of Case Study Research*, 1st edn, SAGE Publications, Thousand Oaks CA.

Statista (2022*a*), 'IoT connected devices worldwide 2019-2030'.
URL: *https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/*

Statista (2022*b*), 'Public cloud computing market size 2023'.
URL: *https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/*

Statnet, D. T. (2021), 'Introduction to Exponential-family Random Graph Models with ergm'.
URL: *https://cran.r-project.org/web/packages/ergm/vignettes/ergm.pdf*

Stebbins, R. A. (2008), Exploratory Research, *in* 'The SAGE Encyclopedia of Qualitative Research', SAGE Publications, Thousand Oaks CA, pp. 327–329.

Steff, R., Burton, J. & Soare, S. R., eds (2021), *Emerging Technologies and International Security: Machines, the State, and War*, Routledge Studies in Conflict, Security and Technology, 1st edn, Routledge, London, New York.

Stivala, A., Robins, G. & Lomi, A. (2020), 'Exponential random graph model parameter estimation for very large directed networks', *PLOS ONE* **15**(1), e0227804.
URL: *https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0227804*

Talmadge, C. (2019), 'Emerging technology and intra-war escalation risks: Evidence from the Cold War, implications for today', *Journal of Strategic Studies* **42**(6), 864–887.
URL: *https://doi.org/10.1080/01402390.2019.1631811*

Taylor, S. J., Bogdan, R. & DeVault, M. (2016), *Introduction to Qualitative Research Methods: A Guidebook and Resource*, fourth edn, John Wiley & Sons.

Teddlie, C. & Yu, F. (2007), 'Mixed Methods Sampling: A Typology With Examples', *Journal of Mixed Methods Research* **1**(1), 77–100.
URL: *https://doi.org/10.1177/1558689806292430*

Thaler, K. M. (2017), 'Mixed Methods Research in the Study of Political and Social Violence and Conflict', *Journal of Mixed Methods Research* **11**(1), 59–76.
URL: *https://doi.org/10.1177/1558689815585196*

Times, G. (2020), 'China won't passively watch UK's Huawei ban', *The Global Times* p. 1.
URL: *https://www.globaltimes.cn/content/1194569.shtml*

Timmer, J. (2021), 'Google tries out error correction on its quantum processor', *Ars Technica* .
URL: *https://arstechnica.com/science/2021/07/google-tries-out-error-correction-on-its-quantum-processor/*

Travagnin, M. (2019), Patent analysis of selected quantum technologies., JRC Technical Reports JRC115251, EU Publications Office, Luxembourg.
URL: *https://data.europa.eu/doi/10.2760/938284*

UNODC (2016), 'Internet Governance – Why the Multistakeholder Approach Works'.
URL: *https://www.unodc.org/e4j/data/_university_uni_/internet_governance_-why_the_multistakeholder_approach_works.html*

US Department of State (2020), 'Welcoming the United Kingdom Decision To Prohibit Huawei From 5G Networks'.
URL: *https://www.state.gov/welcoming-the-united-kingdom-decision-to-prohibit-huawei-from-5g-networks/*

US Executive Office of the President of the United States (2020), A Strategic Vision for America's Quantum Networks, Technical report, White House National Quantum Coordination Office, Washington DC.
URL: *https://www.quantum.gov/wp-content/uploads/2021/01/A-Strategic-Vision-for-Americas-Quantum-Networks-Feb-2020.pdf*

Useche, D. (2014), 'Are patents signals for the IPO market? An EU–US comparison for the software industry', *Research Policy* **43**(8), 1299–1311.
URL: *https://www.sciencedirect.com/science/article/pii/S0048733314000572*

Vailshery, L. S. (2022), 'Topic: Cloud computing in the United Kingdom (UK)'.
URL: *https://www.statista.com/topics/3164/cloud-computing-in-the-united-kingdom-uk/*

van Amerongen, M. (2021), 'NATO Review - Quantum technologies in defence & security', *NATO Review* .
URL: *https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html*

Varian, H. R. (2014), *Intermediate Microeconomics: A Modern Approach*, ninth international student edition edition edn, W. W. Norton & Company, New York, NY.

Vega Yon, G. G., Slaughter, A. & de la Haye, K. (2021), 'Exponential random graph models for little networks', *Social Networks* **64**, 225–238.
URL: *https://www.sciencedirect.com/science/article/pii/S0378873320300496*

Wæver, O. (1995), Securitization and Desecuritization, *in* R. D. Lipschutz, ed., 'On Security', Columbia University Press, New York, pp. 46–86.

Wakefield, J. (2019), 'Russia 'successfully tests' its unplugged internet', *BBC News* .
URL: *https://www.bbc.co.uk/news/technology-50902496*

Wang, Y. (2020), 'In China, the 'Great Firewall' Is Changing a Generation', *POLITICO* .
URL: *https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385*

Ward, M. D., Stovel, K. & Sacks, A. (2011), 'Network Analysis and Political Science', *Annual Review of Political Science* **14**(1), 245–264.
URL: *https://www.annualreviews.org/doi/10.1146/annurev.polisci.12.040907.115949*

Wehner, S. (2019), 'To Invent a Quantum Internet'.
URL: *https://www.quantamagazine.org/stephanie-wehner-is-designing-a-quantum-internet-20190925/*

Weinberg, J. (2000), 'ICANN and the Problem of Legitimacy', *Duke Law Journal* **50**(1), 187–260.
URL: *https://www.jstor.org/stable/1373114*

Weinland, D. (2021), 'Chinese firms are quietly pursuing a new global strategy', *The Economist* (The World Ahead).
URL: *https://www.economist.com/the-world-ahead/2021/11/08/chinese-firms-are-quietly-pursuing-a-new-global-strategy*

WGIG (2005), Report of the Working Group on Internet Governance, Technical Report 05.41622, United Nations Working Group on Internet Governance, Château de Bossey.
URL: *http://www.wgig.org/docs/WGIGREPORT.pdf*

Whalen, J. (2020), 'U.S. hatches plan to build a quantum Internet that might be unhackable', *Washington Post* .
URL: *https://www.washingtonpost.com/technology/2020/07/23/us-plan-quantum-internet/*

Whang, T. (2010), 'Empirical Implications of Signaling Models: Estimation of Belief Updating in International Crisis Bargaining', *Political Analysis* **18**(3), 381–402.
URL: *https://www.cambridge.org/core/journals/political-analysis/article/empirical-implications-of-signaling-models-estimation-of-belief-updating-in-international-crisis-bargaining/4AEE1DA330F7D337859693DF118078CC*

What Is a Quantum Internet? (2020).
URL: *https://www.qutube.nl/quantum-internet-14/what-is-a-quantum-internet-107*

William, O. & Chuang, I. L. (2021), *Quantum Computing Fundamentals*, MIT xPRO Quantum Fundamentals Training Program, MIT Press, Boston MA.
URL: *https://learn-xpro.mit.edu/quantum-computing*

Williams, P. D., ed. (2013), *Security Studies: An Introduction*, second edn, Routledge, London, New York.

Winkler, G. (2022), 'Internet governance'.
URL: *https://www.centr.org/policy/internet-governance.html*

WIPO (2021), 'Patents'.
URL: *https://www.wipo.int/patents/en/index.html*

Wirsching, E. M. (2018), 'The Revolving Door for Political Elites: An Empirical Analysis of the Linkages between Government Officials' Professional Background and Financial Regulation', *2018 OECD Anti-Corruption and Integrity Forum* p. 19.
URL: *https://www.oecd.org/corruption/integrity-forum/academic-papers/Wirsching.pdf*

Wren, D. (2021), 'National rejuvenation to have a profound impact on world', *China Daily* .
URL: *https://www.chinadaily.com.cn/a/202109/08/WS6137f4e9a310efa1bd66dfb9.html*

Wright, J. & Ding, Y. (2015), Lecture 2: Quantum Math Basics.
URL: *https://www.cs.cmu.edu/ odonnell/quantum15/lecture02.pdf*

Wu, Y. (2022), 'The China Standards 2035 Strategy: Analyzing Recent Developments', *China Briefing News* (China Briefing).
URL: *https://www.china-briefing.com/news/china-standards-2035-strategy-recent-developments-and-their-implications-foreign-companies/*

Xi, J. (2021), 'Full text of Xi Jinping's speech on the CCP's 100th anniversary. Official translation'.
URL: *https://asia.nikkei.com/Politics/Full-text-of-Xi-Jinping-s-speech-on-the-CCP-s-100th-anniversary*

Xinhua.Net (2020), 'During the twenty-fourth collective study of the Political Bu-

reau of the Central Committee, Xi Jinping emphasized a profound understanding of the great significance of advancing the development of quantum science and technology, and strengthened the strategic planning and system layout of quantum science and technology development.', *Xinhua.Net* .
URL: *http://www.xinhuanet.com/politics/2020-10/17/c_1126623288.htm*

XQ (2020), 'Understanding The Theory And Math Behind Qubits', *The Research Nest* .

Yannakogeorgos, P. A. (2012), 'Internet Governance and National Security', *Strategic Studies Quarterly* **6**(3), 102–125.
URL: *https://www.jstor.org/stable/26267264*

Yin, J., Li, Y.-H., Liao, S.-K., Yang, M., Cao, Y., Zhang, L., Ren, J.-G., Cai, W.-Q., Liu, W.-Y., Li, S.-L., Shu, R., Huang, Y.-M., Deng, L., Li, L., Zhang, Q., Liu, N.-L., Chen, Y.-A., Lu, C.-Y., Wang, X.-B., Xu, F., Wang, J.-Y., Peng, C.-Z., Ekert, A. K. & Pan, J.-W. (2020), 'Entanglement-based secure quantum cryptography over 1,120 kilometres', *Nature* **582**(7813), 501–505.
URL: *https://www.nature.com/articles/s41586-020-2401-y*

Yon, G. G. V. (2022), *Applied Network Science with R*.
URL: *https://gvegayon.github.io/appliedsnar/*

Zeilinger, A. (2010), *Dance of the Photons: From Einstein to Quantum Teleportation*, Farrar, Straus and Giroux.
URL: *https://us.macmillan.com/books/9781429963794/danceofthephotons*

Zhang, Q., Xu, F., Li, L., Liu, N.-L. & Pan, J.-W. (2019), 'Quantum information research in China', *Quantum Science and Technology* **4**(4), 040503.
URL: *https://doi.org/10.1088/2058-9565/ab4bea*

Zusmann, J. U. (1982), 'Let's keep those systems open', *InfoViews* pp. 29–30.

Appendix A

Data sources

The thesis analysed a corpus of interviews and patent dataset of quantum internet technologies that was assembled using raw data retrieved from the European Patent Office's Global Patent Index.

The audio recordings of the interviews were destroyed following transcription. Transcripts in the .pdf file format are stored on the author's personal 2FA-secured Google cloud account.

The data downloads from the European Patent Office are proprietary, which means they cannot be made publicly available. The R and Matlab code files that were written for the analysis of the datasets, however, were submitted to the University of Southampton's data repository service Pure. The files are available from the following link.

https://doi.org/10.5258/SOTON/D2556

The project ID is 118531515.

The raw data from the European Patent Office required considerable cleaning and editing to prepare them for the analysis in R. This was done using MS Excel and OpenRefine[1], 'an open-source desktop application for data cleanup and transformation to other formats'.

[1] https://openrefine.org/

General guidance on transforming .csv files into network objects and analysing them in R was obtained from (Hoffman 2021*b*, Jilbert & Lizardo 2020, Le et al. 2019, Lusher et al. 2012*a*, Yon 2022).

For the analysis in R, the following packages and documentation was used: (Hanson 2020, Handcock et al. 2008, Hunter et al. 2008, Leifeld 2013, Statnet 2021).

For the computations of the coalitional game theory model in Chapter 7 (and the rendering of the figures in that chapter), the following Matlab programs were used: (Calvo & Rodriguez 2006, Le et al. 2019, Meinhardt n.d.)