US Technology Policy in the Age of the US-China Tech War



Virginia Consuelo Nizza

Balliol College

University of Oxford

December 2023

Thesis submitted in partial fulfilment of the requirements for the degree of DPhil in International Relations in the Department of Politics and International Relations at the University of Oxford

Word Count: 60,049

Abstract

My DPhil thesis critically examines the United States' technology policy in the context of the US-China Tech War. I investigate how the US approach to tech policy, particularly in relation to the tech private sector, has affected its standing in this ongoing rivalry.

The thesis is divided into two parts, encompassing a total of three articles. The first part, represented by Article 1, delves into the decline in US influence among its allies, evidenced by European Union member states adopting data localisation policies targeting US tech companies. I argue that these policies represent a form of soft balancing against US technological dominance, reflecting allies' waning confidence in US leadership in the tech war.

Recognising the strategic losses experienced by the US in Part 1, Part 2 examines one possible explanation for the US decline in the tech war. Building on existing scholarship pointing to the lack of a consistent, unifying approach to tech policy, I examine US tech policy in two key areas: alliance management and private sector management. Article 2 characterises US alliance management as non-cooperative, revealing the challenges of successfully influencing allies to counteract Chinese tech companies' presence in their own critical national infrastructures. Article 3 characterises the US approach to its private sector as laissez-faire, showing that US Big Tech companies operate under rational profit maximisation irrespective of their alignment with the US government.

My findings reveal that the US's non-cooperative approach to alliance management and its laissez-faire approach to private sector management have negatively affected its standing in the tech war. This thesis provides insights into the foreign policy dimensions of tech policy and demonstrates the analytical benefits of anchoring technology-related studies in theoretical frameworks derived from International Relations.

Acknowledgements

Throughout my DPhil journey, I have been very fortunate to have had the unwavering support of an exceptional group of individuals and institutions, without whom this academic pursuit would not have been possible.

First and foremost, I would like to express my profound gratitude to my supervisor, Janina Dill. Her guidance and mentorship have been instrumental in shaping my research and personal growth. From the MPhil to the DPhil, her expertise, endless patience, and belief in my potential have been the foundation of my academic journey. Janina's ability to balance constructive criticism with genuine encouragement was invaluable in helping me navigate the challenges I faced. I deeply valued her consistent support, which ensured I never felt isolated. I am incredibly fortunate to have had her as a mentor and a role model. The lessons she taught me, particularly the importance of holding courage in my convictions, will continue to resonate with me in every walk of life.

I extend my heartfelt appreciation to the Department of Politics and International Relations for providing an intellectually stimulating environment that contributed immensely to my academic growth. I am particularly grateful to Todd Hall and Dominic Johnson, whose insightful feedback during the Confirmation of Status stage was absolutely crucial in shaping my theoretical framework, as well as challenging me to see the forest for the trees. Their mentorship and support were truly indispensable.

Furthermore, I am deeply grateful to the ESRC Grand Union Doctoral Training Partnership for awarding me their studentship and to Balliol College for the Dervorguilla Scholarship. Their generous financial support was instrumental in enabling my research.

To my family, friends, and furry companion, your unwavering love and patience have been the bedrock of my academic journey. Your comforting and joyful presence, coupled with your belief in me, has meant everything.

Finally, I owe a profound debt of gratitude to my fellow DPhil in International Relations cohort. Their camaraderie and support have been invaluable throughout this journey. A special mention goes to all those with whom I embarked on this academic adventure, starting with the MPhil in 2019. We have all evolved and grown from where we started, and I could not have navigated this path without the laughter, the pub nights, and the shared experiences that lightened our toughest days.

This DPhil journey has been one of immense growth, challenge, and discovery. Words can hardly express my immense gratitude to everyone who has been a part of it.

Table of Contents

1. INTRODUCTION 6

1.1. Context and Objective 6

1.2. Theoretical Framework 9

1.3. Thesis Argument 17

1.4. Methods and Sources 23

1.5. Significance and Contribution 25

2. LITERATURE REVIEW 29

2.1. Contextualising the US-China Tech War 30

2.2. The Role of Tech Companies in the US-China Tech War 33

2.3. US Approach to Tech Policy 44

2.4. Conclusion 56

3. TARGETING US TECH COMPANIES: EUROPE'S SOFT BALANCING VIA DATA LOCALISATION 58

3.1. Introduction 59

3.2. Literature Review 63

3.3. Theory and Methods: Data Localisation as Soft Balancing 73

3.4. Case Study: The European Cybersecurity Certification Scheme for Cloud Services (EUCS) 79

3.5. Conclusion 91

4. MY WAY OR THE HUAWEI: US INFLUENCE ON CHINA'S INVOLVEMENT IN THE UK'S CRITICAL NATIONAL INFRASTRUCTURE 94

4.1. Introduction 95

4.2. Literature Review 98

4.3. Theory 105

4.4. Research Design 108

4.5. Case Study 111

4.6. Broader Implications 134

4.7. Conclusion 135

Appendix 137

5. DO BIG TECH COMPANIES' GEOPOLITICAL POSTURES MATTER? MICROSOFT AND GOOGLE'S CONDUCT IN CHINA 138

5.1. Introduction 139

5.2. Literature Review 142

5.3. Theory and Methods 145

5.4. Overview of Universe of Cases 153

5.5. Case Study 1: Microsoft 157

5.6. Case Study 2: Google 164

5.7. Discussion 174

5.8. Conclusion 175

Appendix 178

6. CONCLUSION 179

6.1. Summary and Discussion of Findings 180

6.2. Limitations and Directions for Future Research 189

6.3. Implications of Findings 190

BIBLIOGRAPHY 196

1. Introduction

1.1. Context and Objective

The current landscape of international relations is increasingly defined by the ongoing competition between the United States and China. Within this competition, core technologies are a central issue, with both powers competing for technological superiority. This is often referred to as the 'US-China Tech War.'[1] This competition is playing out across a wide range of domains, including supply chains, semiconductor production, artificial intelligence leadership, and global internet governance. Whilst both the US and China have implemented strategic technology policies to advance their respective goals in this tech war, the US has experienced strategic losses in recent years, particularly in the realms of government-industry relations and international partnerships.

Central to this tech war are tech companies themselves, exerting significant economic, technological, and global influence. The differing roles these companies play in the US and China's tech policies raise critical questions about their influence and strategic importance. Whilst there is extensive literature on China's strategic approach to its tech companies,[2] how they fit into US tech policy has not been analysed to the same degree. This imbalance is critical, particularly in light of evidence of US strategic losses. This leads to my overarching research question: *how has the US approach to tech policy regarding the tech private sector affected its standing in the technological competition with China?*

[1] Haiyong Sun, "US-China tech war: Impacts and prospects." *China Quarterly of International Strategic Studies* 5, no. 02 (2019): 197-212.
[2] Francisco Urdinez, Fernando Mouron, Luis L. Schenoni, and Amâncio J. de Oliveira, "Chinese economic statecraft and US hegemony in Latin America: an empirical analysis, 2003–2014." *Latin American Politics and Society* 58, no. 4 (2016): 3-30.; Johannes Petry, "Beyond ports, roads and railways: Chinese economic statecraft, the Belt and Road Initiative and the politics of financial infrastructures." *European Journal of International Relations* 29, no. 2 (2023): 319-351; Priscilla Roberts, "Economic statecraft with Chinese characteristics: Strange, new, and different, or old wine in new bottles?." *Journal of Current Chinese Affairs* 50, no. 3 (2021): 267-293.

My thesis is divided into two parts, encompassing a total of three articles. The first part of the thesis establishes the reality of the US decline in the tech war. Existing data indicates a loss of confidence in US leadership among its allies,[3] but how does this affect its standing in the tech war against China? I address this question in the first article, presenting empirical evidence that European Union member states are adopting data localisation policies as a means to soft balance against US technological leadership. I argue that these policies reflect allies' waning confidence in US leadership, with the consequences falling on the US tech private sector.

Recognising the strategic losses experienced by the US in the first part, in the second part of the thesis I examine one possible explanation for the US decline in the tech war: its decentralised and inconsistent approach to tech policy.[4] Although the US approach has been criticised for lacking a solid, unifying strategy, the topic of tech policies and their different elements has not been theoretically or empirically explored. I therefore examine US tech policy in two key areas: alliance management and private sector management. Both these areas are very broad themselves, so I limit my enquiry to cases pertaining to the tech private sector.

In the second article, I characterise US alliance management as non-cooperative. I examine US efforts to influence its allies to counterbalance Chinese tech companies. I show that even with the closest of its allies, the UK, successfully influencing their domestic decisions was contingent on specific background conditions, which does not make for an easily replicable strategy. In the third article, I characterise US private sector management as laissez-faire, to add a measure of comparison to China's top-down approach. I show that the US does not use its companies as conduits for foreign policy objectives, allowing companies to operate in third countries with minimal alignment to the US government. This laissez-faire approach has helped

[3] Brian Klaas, "The world is horrified by the dysfunction of American democracy" *The Washington Post* (11 June 2021) <https://www.washingtonpost.com/opinions/2021/06/11/pew-research-global-opinion-us-democracy/> (accessed 02/10/23)
[4] Robert H. Wade, "The Paradox of US Industrial Policy: The Developmental State in Disguise." In *Transforming Economies*, edited by Nübler, Irmgard, José Manuel Salazar-Xirinachs, and Richard Kozul-Wright. Switzerland: International Labour Organisation (ILO), 2014. Print. p.382

the US tech sector to thrive, but it has also made it more difficult for the government to coordinate its efforts to compete with China.

The purpose of this research is to contribute to the study of technological strategy and policy, an emerging field that will become increasingly important for International Relations (IR). Technology policy as a specific field has been neglected by IR scholars – as Daniel R. McCarthy notes, 'the politics of technology are all too often treated as exogenous to the concerns of IR theorists – an environmental condition or set of instrumental possibilities rather than the product of political contestation in which the International itself is central.'[5] My work provides insights into technology and tech companies' roles in American foreign policy. Whilst these insights are rooted to the specific context of the US-China tech war, they also provide valuable perspectives for future comparative studies with other democratic states.

In presenting my findings, I do not endorse a specific policy direction for the US, nor do I advocate for reduced market liberalism, constraining the independence of the private sector, or increase the US ability to influence its allies' domestic decisions. Rather, my focus is on empirically exploring and critically assessing the current US tech policy and its effects on alliance dynamics and international relations more broadly. As I will elaborate in the conclusion chapter, I propose that any alternative approaches to tech policy for democratic states like the US instead be tailored to their own political and economic systems, accounting for the aim of the policy. My findings suggest that this would mean an agile tech policy focusing on strengthening alliances, fostering public-private sector collaboration, and promoting data privacy and democratic values.

[5] Daniel R. McCarthy, *Power, information technology, and international relations theory: The power and politics of US Foreign policy and internet*. Palgrave Macmillan, 2015. p.2

In the following sections, I will first delineate the theoretical framework and then present the thesis argument. This will be followed by a discussion of the methods and sources used in the three papers. Finally, I will explore the broader implications of the thesis.

1.2. Theoretical Framework

In this section, I begin by presenting an overview of technology policy. Subsequently, I expound existing perspectives concerning the US standing in the tech war, the dependent variable. Subsequently, I present prevailing viewpoints on the US approach to tech policy, the independent variable.

1.2.1. Technology Policy

In the context of IR, technology policy can be defined as the strategic framework and set of guidelines adopted by states to govern the development, acquisition, and use of technology in the international arena. This also includes the formulation of policies and regulations that influence the creation, dissemination, and transfer of technology across borders, as well as the management of technological resources to advance national interests and enhance global competitiveness.[6] Crafting tech policy is becoming increasingly challenging, as policymakers must grapple with regulatory fragmentation between cities, regions and countries, as well as rely on the services of 'the same technology firms that (policymakers) would like to influence.'[7] Given its growing importance, the lack of scholarly engagement with the concept of tech policy in IR is surprising. In this thesis, I shed light on the foreign policy components of tech policy,

[6] Heleen De Coninck, Carolyn Fischer, Richard G. Newell, and Takahiro Ueno. "International technology-oriented agreements to address climate change." *Energy Policy* 36, no. 1 (2008): 335-356.
[7] Nicholas Davis, Landry Signé, and Mark Esposito, "Rethinking technology policy and governance for the 21st century" *Brookings Institute* (11 January 2022) <https://www.brookings.edu/articles/rethinking-technology-policy-and-governance-for-the-21st-century/> (accessed 11/09/23)

as well as apply traditional IR concepts like soft balancing to show the analytical gains of grounding technology-related studies on more robust IR theoretical underpinnings.

Tech policy is a critical component of US-China great power competition. Both governments are heavily investing in technology and developing their own tech policies. The US government is focusing on maintaining its technological leadership in key areas such as artificial intelligence, quantum computing, and semiconductors.[8] The Chinese government is aiming to become the world's leading technological power by 2049.[9] In the context of US-China great power competition, tech policy is used by both governments to achieve their strategic goals. For example, the US government uses tech policy to promote the adoption of American technology standards and products around the world (norm-setting), to build alliances with other states by sharing technology and collaborating on research and development, and to export cybersecurity technologies to other countries to help them defend themselves against cyberattacks. The Chinese government uses tech policy to develop its own technological standards and to compete with the US in key areas such as artificial intelligence and quantum computing.

The central focus of this thesis revolves around the convergence of tech policy and foreign policy, particularly on the strategies employed by states in harnessing the potential of their respective tech private sectors. On one front, governments are competing to regulate tech companies in ways that benefit their own national interests.[10] Some governments, such as the US, have a more 'hands-off' approach, allowing tech companies to operate with little

[8] The White House, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," (4 May 2022) <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/> (accessed 09/10/23)
[9] Global Times, "China aims to become world leading technological power by 2049" *Global Times* (24 September 2012) <https://www.globaltimes.cn/content/734882.shtml> (accessed 09/10/23)
[10] Davis, et. al. "Rethinking technology policy and governance for the 21st century"

interference.[11] Others, such as China, have a more interventionist approach, seeking to direct the development and deployment of technology by domestic companies. This approach can be understood as a 'military-civil fusion'[12] in which there is no clear distinction between the state's public and private sectors. Importantly, whilst there is an extensive body of literature examining China's strategic approach to its tech companies, often through the lens of economic statecraft, the US strategic approach has not been thoroughly analysed or empirically explored to the same degree.

On another front, governments are using a variety of measures to undermine the tech companies of other states. These measures can include trade protectionism, export controls, cyber espionage, and pressuring allies not to do business with foreign tech companies. The use of allies in efforts to undermine the others' tech companies is important because it allows governments to amplify their reach and impact. For example, if the US government is able to convince its allies not to do business with Huawei, it will have a much greater impact on Huawei's business than if the US government were to try to undermine Huawei on its own.

Finally, companies themselves are also involved in this tech war, seeking to protect their interests and gain advantage over competitors. Luciano Floridi explains that companies may trick or bypass government regulations, they may rely on their home states to defend them against foreign governments, and sometimes they 'fight their own "home" states.'[13] Indeed, governments and companies are clashing themselves over 'digital sovereignty,' defined very broadly as 'control of the digital.'[14] Discussing the private sector's role in state tech policies therefore requires an acknowledgement of the agency of tech companies themselves.

---

[11] Klon Kitchen, "The New Superpowers: How and Why the Tech Industry is Shaping the International System" *National Affairs,* Number 29 (Fall 2021) <https://nationalaffairs.com/the-new-superpowers-how-and-why-the-tech-industry-is-shaping-the-international-system> (accessed 29/11/21)

[12] *ibid.*

[13] Luciano Floridi, "The fight for digital sovereignty: What it is, and why it matters, especially for the EU." *Philosophy & technology* 33 (2020): 369-378.

[14] *ibid.* p.371

1.2.2. Dependent Variable: US Standing in Tech War

The US-China tech war is a complex and multifaceted issue. Whilst some scholars frame discussions in terms of wins and losses, others reject the confrontational Cold War framing.[15] When comparing the two great powers, the US is often seen as having 'foundational advantages' over China's centralised, top-down coordination model, as the US's 'decentralised, bottom-up approach' lends itself to 'routinized technological development.'[16] However, numerous reports show that 'China's early mobilisation allowed it to narrow the technological gap with the United States,'[17] and research by the United Nations Conference on Trade and Development shows 'the biggest global economic winners over the past three decades have been China and large corporations,' with the US lagging behind.[18]

Given the complexity of all the moving parts of the US-China tech war, we must refer to tangible indicators to assess the current dynamics between the US and China. A report published by a US think tank, the Centre for Strategic and Budgetary Assessments (CSBA), evaluated China's and the US's techno-security systems, evaluating five factors: external threat perceptions and threat environment; leadership and management coordination; governance regime; public-private partnerships and civil-military integration; and techno-national versus global engagement approaches.[19] Within the subset of public-private partnerships and global engagement approaches, the report highlighted two areas that are crucial to US strategy against China: government-industry relationships and international partnerships.

---

[15] Caitlin Lee, "Winning the Tech Cold War" *The Rand Blog* (17 August 2023) <https://www.rand.org/blog/2023/08/winning-the-tech-cold-war.html> (accessed 03/10/23)

[16] Josh Luckenbaugh, "US better positioned for tech competition than China, report finds" *National Defense* (22 June 2023) <https://www.nationaldefensemagazine.org/articles/2023/6/22/us-better-positioned-for-technological-competition-than-china-report-finds> (accessed 03/10/23)

[17] *ibid.*

[18] Rana Foroohar, "Concentrated Power in Big Tech Harms the US." *Financial Times* (Sep 27, 2020). <https://www.proquest.com/trade-journals/concentrated-power-big-tech-harms-us/docview/2467985467/se-2.> (accessed 01/10/23)

[19] Luckenbaugh, "US better positioned for tech competition than China, report finds"

Recent government-industry dynamics indicate a rise of scepticism and tension. Regarding the government-industry relationship, the CSBA report noted that 'recently the government-industry relationship has been marked more by suspicion that collaboration.'[20] Indeed, as I will explore further in the literature review, tensions between government and industry can be understood from the increasingly bipartisan support for higher levels of Big Tech companies' regulation.[21] Data from the Pew Research Centre found that Democrats and Republicans do not differ in their opinions about the impact of breaking up major tech companies.[22] From a public opinion standpoint, it was found in July 2021 that 56% of Americans support more regulation of major technology companies and 68% believe these firms 'have too much power and influence in the economy.'[23] Overall, in 2021 it was reported that the divide between Silicon Valley and Washington D.C. is 'as deep as ever' as 'officials in Washington are more keyed on the society-wide risks tech cooperation poses, while workers in tech are focused on shipping products and making money.'[24]

Regarding international partnerships, the CSBA report deemed allies as a 'core strength' of the US, which must be fostered to ensure it does not become a weakness.[25] Indeed, many have pointed to the importance of US allies, as the consequences of declining faith in American democracy 'hurts the United States' authority and legitimacy, which it needs to convince other countries to do difficult things that support US interests.'[26] Importantly, research institutes have

[20] Luckenbaugh, "US better positioned for tech competition than China, report finds"
[21] Shira Ovide, "Why Washington Hates Big Tech" *The New York Times* (23 October 2020) <https://www.nytimes.com/2020/10/23/technology/why-washington-hates-big-tech.html> (accessed 19/12/21)
[22] Emily A. Vogels, "56% of Americans support more regulation of major technology companies" *Pew Research Centre* (20 July 2021) <https://www.pewresearch.org/fact-tank/2021/07/20/56-of-americans-support-more-regulation-of-major-technology-companies/> (accessed 26/12/21)
[23] *ibid.*
[24] David Wertime and Protocol China Staff, "US Tech Wants to Work More With China" *Protocol* (17 March 2021) <https://www.protocol.com/newsletters/protocol-china/tech-workers-on-china?rebelltitem=2#rebelltitem2> (accessed 03/01/22)
[25] *ibid.*
[26] Laura Silver and Aidan Connaughton, "Most Americans continue to think the US is less respected today than in the past," *Pew Research Centre* (22 June 2022) <https://www.pewresearch.org/short-reads/2022/06/22/most-americans-continue-to-think-the-u-s-is-less-respected-today-than-in-the-past/> (accessed 02/10/23)

reported that 'the United States' appeal and credibility in the world have taken a significant hit. Even US allies do not always see the United States as a good model for democracy or a very reliable partner.'[27] Data released from Pew Research in 2021 shows that despite confidence in US leadership increasing following the end of the Trump presidency, 'the United States has lost the moral high ground.'[28] Just 14 percent of Germans see American democracy as a desirable model for other countries, and 'public opinion in France, Britain, South Korea, Japan and Australia is similarly bleak.'[29] The Washington Post reported such numbers as 'a foreign policy disaster.'[30]

Bruce Stokes, a senior fellow at the German Marshall Fund of the US, wrote in 2022 that American leadership is suffering a crisis of legitimacy.[31] Drawing on polls and interviews, he claimed that 'publics and elites in countries that consider themselves US allies harbour doubts about the state and direction of American democracy.'[32] In the past, international attitudes toward the US have fluctuated considerably according to changes in American administrations,[33] but views about American democracy remained steady. Now, there is a 'steady decline in the international assessment of the strength of the US political system.'[34] Indeed, 'while a median of 61 percent of publics in 13 transatlantic countries polled in 2022 by the German Marshall Fund thought the United States was the most influential actor in global affairs today, just 35 percent expect it to be the most influential in five years.'[35] Stokes argues that the revelations by National Security Agency contractor Edward Snowden in 2013 that the

[27] Patricia M. Kim, Matthew Turpin, Joseph S. Nye Jr., Jessica Chen Weiss, and Eun A Jo Ryan Hass and Emilie Kimball, "Should the US pursue a new Cold War with China?" *Brookings Institute* (1 September 2023) <https://www.brookings.edu/articles/should-the-us-pursue-a-new-cold-war-with-china/> (accessed 02/10/23)
[28] Klaas, "The world is horrified by the dysfunction of American democracy"
[29] *ibid.*
[30] *ibid.*
[31] Bruce Stokes, "The Decline of the City Upon a Hill: As American Democracy Loses its Shine, American Power Suffers" *Foreign Affairs* (17 October 2022) <https://www.foreignaffairs.com/united-states/decline-city-upon-hill> (accessed 02/10/23)
[32] *ibid.*
[33] Silver and Connaughton, "Most Americans continue to think the US is less respected today than in the past"
[34] Stokes, "The Decline of the City Upon a Hill"
[35] *ibid.*

US government was listening in on the phone calls of foreign leaders caused significant damage to the 'important aspect of American soft power,'[36] that of protecting the rights of its own people.

In sum, despite the ambivalence in evaluating the 'losses and wins' of both China and the US in their so-called 'tech war', the evidence I presented above points to the US incurring losses in government-industry relations and in international partnerships. Throughout the thesis, whilst 'US Standing in the Tech War' remains the overarching dependent variable (DV), my focus is specifically on the loss of confidence in US leadership, which contributes to the decline in US standing. As I have argued in this section, confidence in a state's leadership can enhance or diminish its strategic position, thereby weakening its position in global competitions such as the tech war. Accordingly, in the first article I provide an empirical case of the US loss of credibility and appeal in technological leadership and consider the implications on its standing in the tech war.

1.2.3. Independent Variable: US Approach to Tech Policy

When finding possible causes for the shortcomings in US government-industry relations and international partnerships, the US has often been described as adopting a 'laissez-faire'[37] approach in economic and tech policy, which, whilst not indicative of a chaotic or negligent stance, suggests the lack of a solid, unifying strategy. Robert H. Wade has elaborated on the 'paradox' of US industrial policy, pointing out that despite apparent reluctance to deploy an industrial policy, the US has effectively employed it in certain instances to advance major technological innovations.[38] Other scholars have echoed this 'paradox' in the realm of alliance-building as well, pointing to disconnect between the country's emphasis on democratic values

[36] Stokes, "The Decline of the City Upon a Hill"
[37] Wade, "The Paradox of US Industrial Policy: The Developmental State in Disguise"
[38] *ibid.* p.378

and its inconsistent adherence to them, arguing that 'contradictions, internal tensions, and even hypocrisy have become deeply woven into US soft power.'[39]

The US inconsistent approach in the context of the US-China tech war has garnered widespread criticism. Michael Brown and Robert Atkinson argued in an article published by *Foreign Affairs* that 'the United States can no longer expect a laissez-faire approach to be successful when competing with China's top-down, well-articulated industrial strategy reinforced by consistent, large investments.'[40] The authors emphasise the pressing need to align the private sector with national leadership,[41] as they assert that the profit-driven strategies of advanced technology companies are unlikely to be in alignment with US national strategic interests if left unchecked.[42] Additionally, they underline the significance of collaborating with allies, advocating for the US to work with its partners to uphold the economic dominance of the West over China.[43] In summary, they suggest that US leadership should create an integrated strategy that harmonises policy decisions across government departments and motivates private sector entities and research institutions to align with national priorities.[44]

The criticisms resonate with other scholars and pundits. A policy report from an American public policy think tank highlighted that the approach taken by the Biden administration forces zero-sum choices between a stronger geopolitical approach to technology competition and adherence to a global open rules-based system, as well as between strengthening domestic industry and working with allies.[45] Robert M. Gates, a former US Secretary of Defense,

[39] Wade, "The Paradox of US Industrial Policy: The Developmental State in Disguise" p.378
[40] Michael Brown and Robert Atkinson, "The Real Contest with China," *Foreign Affairs* (28 August 2023) <https://www.foreignaffairs.com/china/real-contest-beijing-industrial-strategy> (accessed 28/09/23)
[41] *ibid.*
[42] *ibid.*
[43] *ibid.*
[44] *ibid.*
[45] Karen Kornbluh and Julia Tréhu, "The New American Foreign Policy of Technology: Promoting Innovation, National Security and Democratic Values in a Digital World" GMF Policy Report (March 2023). p.6

described the US as 'the dysfunctional superpower.'[46] He explains that the US government's 'fractured political leadership' have 'failed to articulate a long-term strategy to ensure that the United States, and democratic values more broadly, will prevail.'[47] He compared the present context to the Cold War, observing that the US succeeded back then thanks to a consistent strategy supported by both political parties across nine presidencies, a unity and strength noticeably absent today.[48] In particular, he points to the lack of 'certainty of commitments and constancy of response,' as well as 'erratic and unreliable.'[49] Overall, he asserts that 'America's political dysfunction and policy failures are undermining its success.'[50]

As I will elaborate on in the next section, I expand upon these existing criticisms of the US approach to tech policy by analysing how this approach is empirically manifested in different facets of its tech policy. As the US has incurred strategic losses in government-industry relations and international partnerships, I focus on two aspects of its tech policy: alliance management and private sector management.

1.3. Thesis Argument

My thesis is divided into two parts. In the first part, comprising Article 1, I focus on the dependent variable (US standing in the tech war). I provide an empirical case of the erosion of US credibility and appeal as a tech leader and consider the implications on its standing in the tech war. Whilst in previous sections I presented data on the strategic losses suffered by the US, there is very little empirical, qualitative evidence of this decline. It was therefore crucial

[46] Robert M. Gates, "The Dysfunctional Superpower: Can a Divided America Deter China and Russia?" *Foreign Affairs* (29 September 2023) <https://www.foreignaffairs.com/united-states/robert-gates-america-china-russia-dysfunctional-superpower#author-info> (accessed 29/09/23)
[47] *ibid.*
[48] Gates, "The Dysfunctional Superpower: Can a Divided America Deter China and Russia?"
[49] *ibid.*
[50] *ibid.*

to present evidence of this loss of credibility to delve into the specific characteristics of US tech policy that can help to explain the decline.

In the second part of the thesis, I address the limitations of the current definition of the independent variable (US approach to the tech war) by breaking it down into more observable and measurable variables. Specifically, I focus on US tech policy in the two areas of the tech war that I identified are areas of strategic weakness for the US: government-industry relations and international partnerships. By analysing the empirical manifestations of the US inconsistent approach in these two domains, I characterise US tech policy as non-cooperative in alliance management (Article 2) and laissez-faire in private sector management (Article 3). Both facets that I analyse (alliance management and private sector management) fall within a specific tech policy field, that of the tech private sector. This entails the US approach to leveraging its tech private sector for strategic success, which includes US relationship to its tech companies, attempts to undermine China's tech companies, and the agency of tech companies themselves.

Each article employs a qualitative case study approach, offering unique insights and contributions to the field. Whilst each article independently addresses specific questions and presents unique findings, together they form a narrative highlighting the shortcomings of the US approach to tech policy. These shortcomings are essential to understand the US's declining influence in the context of the US-China tech war.

1.3.1. Empirical Representation of US Losses

First, I address the following question: how is the US' declining appeal and credibility among its allies affecting its standing in the tech war against China? Drawing on the statistics indicating the loss of confidence in the US by its allies, in the first article I provide an empirical representation of what occurs as a consequence of this loss of confidence. I show that US allies,

more specifically EU member states, are explicitly seeking to curtail the presence of US tech firms in their cloud infrastructures. I show that the rise of data localisation policies among US European allies is not a side-effect, but a purposeful strategy of soft balancing against US leadership in tech. This article therefore focuses on the *effects* of the US approach to tech policy. Counterfactually, more collaborative approaches by the US may have yielded different outcomes. My findings confirm US allies' loss of confidence in US leadership in tech, empirically presenting US strategic losses in the tech war with China especially as it relates to 'US efforts to lead on global rules and values.'[51] Indeed, allies' support is considered central to US tech policies ranging from 'restricting Chinese access to critical semiconductor technology to contesting efforts in standards organisations to approve surveillance technologies.'[52]

Specifically, I examine the European Union's data localisation policies – regulations mandating the storage and processing of digital data within a state's territorial jurisdiction – as they pertain to US technology companies. I investigate why US allies are choosing to adopt data localisation policies despite their evident economic drawbacks and security inefficiencies. I focus on US allies, in particular EU member states, as they were relatively less likely to adopt such policies given their previous ideologies on data governance as well as their relative likelihood to want to support the US in its tech war with China. Support from its European allies is crucial to US tech leadership, as data localisation laws that hurt US private firms also hinder US attempts to maintain its technological edge in the ongoing competition against China. I posit that data localisation policies adopted by EU member states serve as a form of 'soft balancing' against US technological hegemony. To substantiate this argument, I conduct

[51] Karen Kornbluh and Julia Tréhu, "The New American Foreign Policy of Technology: Promoting Innovation, National Security and Democratic Values in a Digital World" *GMF Policy Report* (March 2023) <https://www.gmfus.org/sites/default/files/2023-03/Report%20-%20The%20New%20American%20Foreign%20Policy%20of%20Technology_1.pdf> (accessed 15/04/23)
[52] *ibid.*

a case study of the European Cybersecurity Certification Scheme for Cloud Services (EUCS), drawing on both primary and secondary qualitative data. My findings indicate that the sovereignty requirements within the EUCS aim to reduce reliance on US tech companies, hinder the US's surveillance capabilities, and promote European tech industries. Despite facing significant criticisms for potentially disrupting global cybersecurity cooperation and creating divisions among EU member states, their persistence reveals a deliberate strategy of soft balancing.

1.3.2. International Partnerships: Non-Cooperative Alliance Management

Recognising the strategic losses experienced by the US in the first part of the thesis, in the second part I examine the US approach to its tech policy as a potential cause. I analyse US conduct in the two areas I identified of strategic loss for the US: international partnerships and government-industry relations.

First, I focus on international partnerships. The way in which I assessed the strength of the US' international partnerships was to see how effective the US was at preventing allies from accepting Chinese tech in their critical national infrastructures. I show that these attempts have been inconsistent, with US success in the UK being highly contingent on very specific background conditions. This suggests that the US's current alliance management strategy is not sustainable in the long term, even among its closest of allies, the Five Eyes (FVEY). I therefore characterise the US approach to alliance management in its tech policy as non-cooperative.

The second article's research question is the following: to what extent can the US effectively influence the UK's decision-making about letting Chinese technology companies partake in their domestic critical national infrastructures (CNI)? I draw on the case of the UK's policy reversal from accepting the Chinese company Huawei's involvement in building its

national 5G telecommunications networks in January 2020 to banning it in July. This specific case interrupted the UK's previous policy pattern of warmly accepting Chinese investments across different sectors of the CNI. By employing within-case process tracing, I argue that US influence was a necessary condition in the UK's policy reversal on Huawei. However, it was not sufficient, as it interacted with favourable background conditions: the behaviour of other Five Eyes (FVEY) members, geopolitical developments at the time and the interests of and division among domestic actors. I conclude that under such favourable background conditions, the US can potentially have influence on its allies' decision on whether to let Chinese companies partake in their CNI. However, even in the most likely case of US influence to yield results – in the special relationship with the UK – the configuration of sufficient conditions is highly contingent, suggesting that this strategy of pressuring allies against allowing Chinese investment in critical infrastructure is unlikely to work in other contexts.

1.3.3. Government-Industry Relations: Laissez-Faire Private Sector Management

For government-industry relations, I analyse the US bottom-up approach towards private sector management, which stands in stark contrast to China's top-down approach. Economic statecraft literature shows that one of China's cornerstones of tech policy is its centralised relationship with national tech champions. I focused on the question of the extent to which US Big Tech companies are aligned to the US government to the degree that this alignment affects its business decisions. We know that there are tensions between government and industry.[53] But how is that reflected in foreign policy? Are tech companies 'conduits' of sorts of US foreign policy?

[53] Ovide, "Why Washington Hates Big Tech"

To answer these questions, I built on the debate emerging among scholars and pundits on whether US Big Tech companies have 'geopolitical postures' that drive their business interactions in third countries. My findings reveal that, regardless of their respective geopolitical postures, the alignment, or lack thereof, of US Big Tech companies with the US government does not affect their business decisions. These findings contribute to the characterisation of US tech policy, revealing that these companies operate independently from the influence of US foreign policy. Whilst the implications of this autonomy for the US are beyond the scope of this article, my research enriches the understanding of the dynamics between the US and its tech industry, which is pivotal for shaping tech policy. In contrast to China's strategic use of tech companies as instruments for exerting institutional influence, the US adopts a distinct approach. My findings offer a basis for further exploration into the differences between the US and China's tech policies. In addition, I contribute to the literature by developing a theory to understand whether tech companies have foreign policies, or 'geopolitical postures.' This endeavour represents a first attempt at doing so in a methodologically rigorous way.

The research question guiding my third article is the following: what explains the behaviour of Microsoft and Google in China? I primarily challenge the argument that these companies have geopolitical postures that drive their business interactions in third countries and that these postures are an independent factor in US-China strategic competition over technological superiority. I define geopolitical posture as a set of purposely crafted and defined *a priori* policies, or code of conduct, intended to inform and influence a company's decisions, constraining its behaviour vis-à-vis its business interactions in third countries. I assess the postures using the benchmark of whether the company explicitly refers to the US government as a partner and source of its outlook. Consequently, I class the company as either independent, apolitical, or aligned. Through a small-N case study comparison, using semi-structured

interviews and secondary sources to carry out within-case process tracing, I find that their geopolitical postures have no influence on their business decisions in China. Instead, I show that each company's decision-making in China was led by rational profit maximisation under constraints, which include the companies' business models, relevant Chinese legislation, and the company's internal structure. Strategically, the findings reveal a lack of alignment between the US government and its national tech champions, underscoring the differences in economic statecraft tools available to the US as opposed to China.

1.4. Methods and Sources

All three papers follow a qualitative approach. I used both single case studies and case study comparisons, primarily employing within-case process tracing, defined as 'techniques for examining the intermediate steps in cognitive mental processes to understand better the heuristics through which humans make decisions.'[54] In this section I briefly discuss the main methods and sources I used, their potential limitations and how I addressed them.

It is important to consider the nature of the causal inference made in process tracing. Beach and Pedersen explain that with this method, we are 'making inferences about whether causal mechanisms are present in a single case, but we are not interested in assessing the magnitude of the causal effects of the combination of an independent variable and the ensuing mechanism on a dependent variable.'[55] The scope of inferences that can be made using theory-centric variants of process tracing is restricted to whether or not a mechanism is present in a case – neither inferences about necessity nor sufficiency of a mechanism in relation to the population of a phenomenon can be made.[56] The specific kind of process tracing employed in this thesis

[54] Andrew Bennett and Jeffrey T. Checkel, eds. *Process tracing*. Cambridge University Press, 2015. P.5
[55] Derek Beach and Rasmus Brun Pedersen, *Process-tracing methods: Foundations and guidelines*. University of Michigan Press, 2019. p.75
[56] *ibid.* p.89

is theory-building, as it is used to 'build a theorised causal mechanism that is potentially generalisable outside of the individual case' and the scholar seeks inspiration from 'existing theoretical work and previous observations for what to look for.'[57] I collect Causal Process Observations (CPOs) and subject them to process tracing tests to assess the relevance of the hypotheses. These tests, in order of ascending strength, are: (1) the straw-in-the-wind test, which, if the CPO passes, affirms the relevance of the hypothesis but does not confirm it, (2) the hoop test, which is slightly stronger as failing it eliminates the hypothesis, (3) the smoking gun test, which confirms the hypothesis, and (4) the doubly decisive test, which confirms the hypothesis and eliminates the rival hypotheses.

Process tracing requires rich contextual data, which I found in primary data collected in semi-structured elites interviews,[58] and secondary sources including newspaper articles, policy documents, company documents, policymakers' and company representatives' statements and speeches, open-source intelligence reports and other forms of government documents. I provide a list of interviews in the appendix of each article. There were obstacles to data collection due to how contemporary the issues are and the difficulty in accessing the relevant interviewees, which are both political elite and tech companies' representatives. Gaining access to current employees and leading figures in the Big Tech industry was particularly difficult due to the risks associated with obtaining opinions and information which could potentially jeopardise their careers. Moreover, policymakers' and company representatives' thoughts are recent, and the primary shortcoming of this is that their words will often have been tailored to their political and/or corporate affiliations and aims, and not revelatory of their true convictions. However, the contemporary nature of the topic also presents an advantage: interviewees did not have to recall past events, which often may distort reality and generate further methodological hurdles.

[57] Beach and Pedersen, *Process-tracing methods*, pp.271-273
[58] Ethical approval of research involving human participants was granted (Central University Research Ethics Committee Approval Reference: SSH_DPIR_C1A_21_053)

I dealt with the limitations of data collection through interviews in the following ways. Firstly, I ensured that the aim of the interviews was not to obtain the opinion of a large cohort of policymakers and company representatives, which instead can easily be collected through parliamentary debates and public statements. Rather, my priority was to talk to high-level officials and employees which could reveal information I would otherwise be unable to obtain and shed light on the decision-making process of the relevant individuals. Furthermore, I triangulated the words of high-level officials and employees with colleagues to ensure the information was truthful. Finally, my use of interviews is supplemented by an extensive use of secondary sources, which I carefully analysed as public sources, thus acknowledging that they may be calculated and not necessarily revelatory of decision-makers' personal thoughts.

1.5. Significance and Contribution

This thesis makes a theoretical and empirical contribution to the study of technological strategy and policy. First, I reveal the complexities faced by states in an increasingly technology-driven international landscape. We are currently experiencing what the World Economic Forum dubbed the 'fourth industrial revolution,'[59] which poses great risks to economic development, national security, social cohesion, and human rights, due to 'the speed and scale at which digital applications and systems can be deployed across traditional borders.'[60] Policymakers now face the complex task of developing tech policies whilst grappling with moving parts such as technical complexities, the agency of non-state actors such as tech companies, and the agency of allies and how they will respond to such strategies.

The need for new regulatory forms and governance models is evident, as traditional approaches struggle to keep pace with the technological and regulatory changes occurring

[59] Klaus Schwab and Nicholas Davis, *Shaping the future of the fourth industrial revolution*. Currency, 2018.
[60] Davis, et. al. "Rethinking technology policy and governance for the 21st century"

globally. As former US Secretary of State Madeleine Albright stated, 'people are talking to their governments on 21st century technology. The government listens to them on 20th century technology and provides 19th century responses.'[61] Indeed, scholars have stated before that 'effective technology policy requires close collaboration across jurisdictions.'[62] As my thesis shows, this also means that policymakers need to develop a deeper understanding of technology and its implications for foreign policy. Indeed, in Article 1 I consider the possibility of policymakers misunderstanding technical complexities, which can have significant negative consequences. Although I do not find sufficient evidence to invalidate my hypothesis of EU member states' purposefully soft balancing against the US, there was some evidence of technical misunderstandings among European policymakers.[63]

Second, my thesis shows that traditional alliance dynamics can be seriously challenged and undermined as a result of mismanagement in crafting tech policies that pay attention to allies. I empirically demonstrate that the US is losing ground with its allies in the context of its strategic competition with China. For the US, this is a concerning trend, as the US needs the support of its allies to maintain its global leadership in technology.[64] The US' diminishing appeal and credibility among its allies represents a critical development in the field of IR, signalling a potential shift in global alliances and power dynamics.

Third, my thesis contributes to debates on tech companies' growing influence in IR. Tech companies possess an unprecedented level of economic might, technological prowess, and global influence. As a result, governments around the world are grappling to understand the type of power that these companies possess and how to manage their relationship with them.

---

[61] Maggie Tennis, "Madeleine Albright on fascism, democracy and diplomacy." *Brookings Institute* (11 September 2018) <https://www.brookings.edu/articles/madeleine-albright-on-fascism-democracy-and-diplomacy/> (accessed 11/10/23)
[62] Davis, et. al. "Rethinking technology policy and governance for the 21st century"
[62] *ibid.*
[63] Nigel Cory, "Europe's Cloud Security Regime Should Focus on Technology, Not Nationality" *Information Technology and Innovation Foundation* (27 March 2023) <https://itif.org/publications/2023/03/27/europes-cloud-security-regime-should-focus-on-technology-not-nationality/> (accessed 12/04/23)
[64] *ibid.*

Some have gone so far as to advocate for companies like Amazon and Facebook to have a seat at the United Nations due to their emergence 'as global players in their own right.'[65] Others have expressed fear towards tech companies because of their ability to make 'decisions that take on democratic governments.'[66] Importantly, the relationship between tech companies and their respective governments is complex and characterised by significant power imbalances and questions of agency. For example, decisions made by these companies can have wide-reaching implications for the policy options available to officials in Washington and Beijing.

The critical role of tech companies in the US-China competition raises questions about their strategic role and how the two powers have leveraged it differently. Although it is widely acknowledged that 'the subject matter in international relations, the execution of foreign policies, and even the conduct of diplomacy directly involve, or are heavily influenced by, science and technology'[67] scholars have observed a limited systematic exploration of the interplay between science, technology, and the substance of foreign policy.[68] This thesis offers valuable insights into the role of tech companies within the tech policy of a democratic state.

Finally, the thesis as a whole raises a number of important questions about the future of states' tech policies and their effects on international relations. Understanding tech policies is a challenging task, as the US government, like most states, does not have a single, coherent tech policy. However, I provide insights on how we can deconstruct its elements and understand the different ways in which states use technology to achieve their foreign policy goals. In the case of the US, my findings show that to mitigate strategic losses, it should develop a tailored, flexible tech policy centred on working more closely with allies, especially on

[65] Ben Schott, "Give Amazon and Facebook a Seat at the United Nations" *Bloomberg* (3 October 2021) <https://www.bloomberg.com/opinion/articles/2021-10-03/give-amazon-and-facebook-a-seat-at-the-united-nations> (accessed 28/09/22)
[66] Foreign Affairs Committee, "Oral Evidence: Tech and the future of UK foreign policy, HC 201" *House of Commons* (2 November 2021) <https://committees.parliament.uk/oralevidence/2955/pdf/> (accessed 10/11/21)
[67] Eugene B. Skolnikoff, *Science, technology, and American foreign policy*. MIT Press, 1967. p.4
[68] *ibid*.

developing international norms and standards for technology, and building collaborative, mutually beneficial partnerships with its tech champions.

2. Literature Review

The objective of my DPhil project is to analyse the US approach to tech policy in the context of the US-China tech war, with a specific focus on US policy concerning tech companies. This encompasses the US relationship with its domestic tech companies, efforts to undermine foreign tech companies, and the agency of the tech companies themselves in shaping these dynamics.

In this chapter, I provide an in-depth exploration of the relevant bodies of literature to this enquiry. The chapter is structured into three sections. The first section contextualises the US-China Tech War, drawing from literature that helps us understand the broader geopolitical landscape and the stakes involved in the competition between the US and China within the technological realm. The second section centres on the role of the tech private sector in the US-China great power competition. I discuss literature that provides insights into the evolving role of tech companies in the international arena, focusing particularly on American Big Tech companies. This section focuses on the companies themselves rather than states' approach towards them. I firstly explore why tech companies matters in IR more broadly. Subsequently, I move to why specifically the United States' 'Big Tech' matters in IR. I address why tech companies are strategic actors in international relations and how these actors navigate geopolitical tensions. The third section focuses on the US approach to leveraging the tech private sector. In this final section, I delve into the literature that discusses how the US government approaches and leverages its tech sector in its strategic competition with China, which is the component of US tech policy that I focus on throughout the thesis. This section further explores the potential impacts of these approaches on US influence and strategic position in this competition.

2.1. Contextualising the US-China Tech War

First, I delve into the broader literature surrounding the so-called US-China tech war. This literature provides context for the technological competition between the US and China from different angles. It also provides an understanding of why US government policy targets Chinese companies in the technological realm. However, whilst the tech war context is vital, this body of literature does not explicitly address how the US leverages its tech sector in this strategic competition. The focus often remains on the state-to-state level, ignoring the potential influence of tech firms.

The role of technology in China-US strategic competition has drawn much attention from scholars. The notion of great power competition between the US and China emerged in the policy world with Washington's release of its National Security Strategy in 2017 and the publication of the Pentagon's National Defence Strategy emphasising 'the re-emergence of long-term strategic competition as the central challenge to US prosperity and security.'[1] From a US perspective, some have argued that the end of the Cold War brought the emergence of multiple threats from lesser adversaries as opposed to the perception of an existential threat, causing the displacement of 'the strategic focus on advancing the US technological frontier and reducing the external pressure that made science and technology innovation a national security priority for both sides of politics.'[2] This created the circumstances in which the US fell relatively behind in the technological sector.

There is a body of literature that points to the US' attempts to securitise Chinese tech companies within the US-China competitive dynamic. Andrew Stephen Campion used critical discourse analysis to examine how China has been constructed as an existential threat, by

[1] Linda Weiss, "Re-emergence of Great Power Conflict and US Economic Statecraft." *World Trade Review* 20.2 (2021): 152-68. p.154
[2] *ibid.* p.156

drawing on US reactions to CNOOC in 2005 and to Huawei more recently.[3] He argues that a coherent 'China Threat Discourse', which portrays the state 'as a belligerent and capable actor with interests running counter to the interests of the Self,' [4] has been employed in the US to protect its interests. He pinpoints the emergence of the China threat in the late 1990s, through the characterisation of China as 'providing an alternative model to Western governance' in conjunction to the 'West's impotence to continue its subjugation of China.'[5] Campion argues that the 'securitising steps taken against CNOOC directly informed responses to Huawei'[6] and explains that both companies operate in critical infrastructure, which in the US are viewed under negative security perceptions.

The tensions between the US and China over 5G are representative of a much more expansive landscape that will underpin the future of the world's digital infrastructures, including quantum computing, artificial intelligence, the Internet of Things, big data and biotechnology.[7] Intensifying strategic competition between the US and China has 'lent new momentum to a US whole-of-government effort to curb the use of technology built or maintained by leading Chinese tech firms.'[8] Yan Xuetong argues that 'digital mentality', defined as 'the way of perceiving and responding to international strategic issues from the perspective of cybersecurity and digital economy'[9] influences foreign policy decision-making. This implies that the mentality leads to policymakers' consideration of cyberspace as more strategically important to national survival than the geophysical world, and this characterises

[3] Andrew Stephen Campion, "From CNOOC to Huawei: securitization, the China threat, and critical infrastructure." *Asian Journal of Political Science*28, no.1 (2020) p.52
[4] *ibid.* p.52
[5] *ibid.* p.53
[6] *ibid.* p.59
[7] Yu Jie and Joyce Hakmeh, "The UK's Huawei Decision: Why the West is Losing the Tech Race" *Chatham House* (17 July 2020) <https://www.chathamhouse.org/2020/07/uks-huawei-decision-why-west-losing-tech-race> (accessed 17/07/20)
[8] Robert Greene and Paul Triolo, "Will China Control the Global Internet Via its Digital Silk Road?" *Carnegie Endowment for International Peace*. (8 May 2020). <https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857> (accessed 22/09/20)
[9] Yan Xuetong, "Bipolar rivalry in the early digital age." *The Chinese Journal of International Politics* 13, no. 3 (2020): 313-341. p.5

the struggle between the US and China, just as Cold War mentality, which rested on ideological biases and beliefs, defined US-Soviet competition. This is particularly helpful in understanding the centrality of technology in US foreign policymaking. However, there is a lack of empirical testing of Xuetong's concept of digital mentality.

A final concept which is central to the thesis for the purpose of understanding *why* the US and China seek to achieve global technological primacy over the other is that of 'weaponised interdependence', which Henry Farrell and Abraham L. Newman coin to explain that 'states with political authority over the central nodes in the international networked structures through which money, goods and information travel are uniquely positioned to impose costs on others.'[10] They reveal the power dynamics that shape the relationship between the US and online communications networks, explaining that the US has 'systematically exploited the panopticon effect' even when its 'allies have formally objected.'[11] Most importantly, they point out that if its allies decide that the US has been 'abusing' weaponised interdependence in ways that conflict their core interests, they will defect. US' West European allies are most likely to have control 'over key nodes in global networks, or to be credibly able to set up their own alternatives.'[12] The concept not only provides insights on the motivations behind the US' pressure to ban Huawei, but also delivers a stark warning that this pressure may be counterproductive to the United States' larger strategic aims.

The concept of weaponised interdependence provides a crucial background for my research. It sets the stage for the strategic position the US held in past decades and provides a warning for the importance of US allies' support to the US for the US to retain this position. However, this body of literature falls short in directly addressing how the US strategic position in the tech war may be weakened. In the next thesis chapters, I shed light on the US's

[10] Henry Farrell and Abraham L. Newman. "Weaponized interdependence: How global economic networks shape state coercion." *International Security* 44, no. 1 (2019): 42-79. p.45
[11] *ibid.* p.74
[12] *ibid.* p.78

mishandling of the tech private sector as a contributing factor to the weakening of its influence and strategic position.

2.2. The Role of Tech Companies in the US-China Tech War

In this section, I examine the literature dedicated to understanding the strategic value of tech companies in the context of international relations and the US-China competition. These works provide insights into why Big Tech companies matter in the larger geopolitical landscape. However, they often do not specifically focus on how the US government navigates the challenges and opportunities posed by its own tech giants within its strategic contest with China. First, I explore why tech companies matters in IR more broadly. Subsequently, I move to why specifically the United States' 'Big Tech' matters in IR.

2.2.1. Tech Companies in IR

Despite widespread use of Cold War analogies to understand the current 'great power competition' between the US and China, current conditions are, in numerous ways, different from the past. Importantly for this research project, we have never had tech giants like this. Tech companies reject the idea that they are monopolies on the basis that customers 'are free to come and go as they please.'[13] However, what renders them truly distinctive compared to previous commercial monopolies is the role of data. Data is not tangible; it does not fit within our current understanding of sovereign borders. Tech companies need to navigate ongoing regulatory environments, poorly understood and sparingly managed, and rely on sustained access to such data, thus are more vulnerable than others in the past. Major tech firms are

[13] Olivia Solon and Sabrina Siddiqui, "Forget Wall Street – Silicon Valley is the new political power in Washington" *The Guardian* (3 September 2017) <https://www.theguardian.com/technology/2017/sep/03/silicon-valley-politics-lobbying-washington> (accessed 27/11/21)

'essentially dual-use assets' as their 'civilian technologies can be repurposed as powerful weapons of asymmetric warfare.'[14] Apple CEO Tim Cook stated that 'scraps of data, each one harmless enough on its own, can be aggregated and synthesised to derive and develop to algorithms that know you better than you know yourself.'[15] Moreover, Big Tech exercises a form of sovereignty over digital space, and thus governments eye global tech companies as 'proxies – and potential targets – of their respective national power.'[16]

A substantial amount of articles have been written on the power of the tech industry in comparison to business empires such as General Electric, Toshiba, Johnson & Johnson, Siemens, DowDuPont and United Technologies.[17] It has been argued that 'they boast valuations bigger than any other companies in history' and that the way that today's big tech conglomerates 'glue their products together into "platforms" makes them potentially much more dominant and long-lasting than the industrial conglomerates' whose sibling businesses were not as interconnected or mutually supporting.[18] Moreover, they can 'take advantage of "network effects" such that every additional user they add potentially brings greater value than the previous one.'[19] They are able to exploit something unique to the internet age – 'demand-side economies of scale' arising from network effects. They also add new businesses that can 'plug directly into their platforms, while capturing more of our time and money.'[20]

Some scholars have emphasised the importance of understanding companies as political actors who can 'significantly influence decisions, policies and outcomes, as opposed to being

[14] Jacob Helberg, "Silicon Valley Can't Be Neutral in the US-China Cold War" *Foreign Policy* (June 22, 2020) <https://foreignpolicy.com/2020/06/22/zoom-china-us-cold-war-unsafe/> (accessed 04/12/21)
[15] *ibid.*
[16] *ibid.*
[17] Christopher Mims, "Move Over, GE. The Tech Conglomerates Are the New Leaders of Industry" *The Wall Street Journal* (November 27, 2021) <https://www.wsj.com/articles/move-over-ge-tech-conglomerates-amazon-apple-microsoft-are-the-new-leaders-of-industry-11637965497> (accessed 27/11/21)
[18] Mims, "Move Over, GE. The Tech Conglomerates Are the New Leaders of Industry"
[19] *ibid.*
[20] *ibid.*

simply profit-driven entities,'[21] rather than tools to be used by their governments. John Mikler, in his book *The Political Power of Global Corporations,* argues that global corporations have leveraged their power to shape markets around their economic interests.[22] A particularly interesting aspect that he identifies is the ability of corporations to create 'truths' about themselves, truths 'that their interests are aligned with those of states and citizens, and that they have the capacity and are already self-regulating their operations to ensure such alignment.'[23] Through investment in cultivating a positive public image and forms of private authority, global corporations possess the legitimacy and authority to wield political power. In 1975, Richard J. Barnet and Ronald E. Müller, in their book *Global Reach: The Power of Multinational Corporations*, also argue that global corporations constituted the most potent forces in the world economy, posing an important threat to national sovereignty.[24] However, such discourses of the demise of the nation-state have since been challenged and are overall not necessarily useful in understanding the complexities of business-government relations.

Finally, very little literature in IR focuses on commercial entities as agents in geopolitics. Literature which does do so focuses predominantly on China, as 'China appears ideally structured to use economic resources strategically to advance its foreign policy goals.'[25] It is important not to underestimate or take US cases for granted, as we must remember that 'China is a diligent student of the US system and according to experts, its innovation ecosystem might not stray too far from America's, at least not as far as some believe.'[26] More specifically, Big Tech companies are often treated as if they were created equal. However, there are important differences and nuances between them which, if discerned, can help us understand their role in

[21] Iris May Ellen Y. Caluag, "The Political Power of Global Corporations, written by John Mikler." *Philippine Political Science Journal* 42, no. 1 (2021): 90-94. p.90
[22] John Mikler, *The political power of global corporations*. John Wiley & Sons, 2018.
[23] Caluag, "The Political Power of Global Corporations." p.91
[24] Richard J. Barnet and Ronald E. Müller. *Global Reach: The Power of the Multinational Corporations*. London: Jonathan Cape, 1975.
[25] James Reilly, *Orchestration: China's Economic Statecraft Across Asia and Europe*. Oxford University Press, 2021. p.1
[26] Weiss, "Re-emergence of Great Power Conflict and US Economic Statecraft." p.165

US-China great power competition. Indeed, 'when we talk about the tech industry, there is a danger of conflating the Facebooks, Googles, and Twitters of the world with "small-t technology."'[27] Therefore, the next paragraphs look specifically at the role of US Big Tech in IR.

2.2.2. US Tech Companies in IR

I now turn to the existing literature on US tech companies, or 'Big Tech,' in IR, which is relatively sparse but includes some interesting insights. In the past, technology companies distanced themselves from politics, but the more technology became inherently political, the more Big Tech companies have taken a role in geopolitics.[28] Some argue that 'while the national security background runs deep in the veins of some Silicon Valley tech platforms, and Chinese companies are perceived as closely associated with their government, still, most tech giants prefer to appear politically neutral and to be independent.'[29] Since political action has become progressively more accessible to non-state actors 'it makes sense that these new players are seeking to expand the sphere of their political influence.'[30] Nancy Ayer Fairbank has argued that Microsoft, for example, although it is 'not attempting to act exactly like a nation state' seems to be seeking an 'expansion and consolidation of its role as a quasi-public actor.'[31] This sort of political engagement seems necessary for corporations to 'maintain moral legitimacy, which nurtures societal acceptance and subsequently increases profitability.'[32]

---

[27] Katy Cook, *The Psychology of Silicon Valley: Ethical Threats and Emotional Unintelligence in the Tech Industry*. Basingstoke, 2020. p.3
[28] Greg Williams, "Big Tech is now a geopolitical force – and that should worry us all" *Wired* (9 April 2020) <https://www.wired.co.uk/article/big-tech-geopolitics> (accessed 01/12/21)
[29] Gregory F. Treverton and Pari Esfandiari, "Viewing tech giants as a geopolitical force" *The Hill* (31 January, 2020) <https://thehill.com/opinion/technology/480823-viewing-tech-giants-as-a-geopolitical-force> (accessed 01/12/21)
[30] Nancy Ayer Fairbank, "The state of Microsoft?: the role of corporations in international norm creation." *Journal of Cyber Policy* 4, no. 3 (2019): 380-403. p.396
[31] *ibid.* p.397
[32] *ibid.*

Stephanie Hare analysed the tension between states and private corporations in the context of data protection, which is most relevant to the idea of the weaponization of data localisation. She argues that the battle over data protection, i.e. 'who owns an individuals' electronic communications data, who should have access to it, and what can be done with it' is a 'wicked problem.'[33] She explains that before former US National Security Agency contractor Edward J. Snowden revealed US intelligence agencies' mass surveillances of Americans and non-Americans, companies benefited from a 'closer degree of complicity with the US government, which promoted their products and services as tools to further US foreign policy democracy.'[34] After Snowden, companies 'have tried to convince their customers within and outside the United States of their independence from the US government, to varying degrees of success.'[35] This provides an insight on the companies' motivations to retain independence, at least in public framing, from the US government.

The rhetoric on geopolitical actorness of Big Tech firms has increased in recent years. A controversial article was published in the Economist which argued that 'democracies must team up to take on China in the technosphere,'[36] as cooperation between like-minded states was absolutely essential to countering China's rise. Interestingly, the article argued that 'the units of analysis for today's nascent technopolitics are platforms: the technologies on which other technologies are built.'[37] The authors wrote that, like geographical territories, these platforms, such as Facebook, have their own politics: 'they have their own populations, mostly users, coders and other firms. They have their own laws, which lay out who can change code and access data. They have a position with respect to other platforms which underpin, compete with

[33] Stephanie Hare, "For your eyes only: US technology companies, sovereign states, and the battle over data protection." *Business Horizons* 59, no. 5 (2016): 549-561. p.550
[34] *ibid.* p.551
[35] *ibid.*
[36] The Economist, "Democracies must team up to take on China in the technosphere" (19 November 2020) <https://www.economist.com/briefing/2020/11/19/democracies-must-team-up-to-take-on-china-in-the-technosphere> (accessed 30/10/21)
[37] *ibid.*

or build on them, just as territories have defined relationships with their neighbours.'[38] Overall, they argue that 'their dominant positions in this world of platforms gives companies like Facebook and Google powers approaching or surpassing those of many countries.'[39]

The following sub-sections provide an overview of the current landscape of debates which are currently emerging in scholarly and policymaking realms on Big Tech's geopolitical postures.

Bremmer v. Walt

An example of scholars' engagement with the topic of Big Tech geopolitical postures is the debate between Ian Bremmer and Stephen M. Walt. Bremmer argued that a handful of technology companies now rival states as the primary actors of global affairs, having taken control of aspects of society, the economy, and national security.[40] In the context of US-Chinese technological competition, Bremmer argues that tech companies are not foot soldiers nor tools, but rather shape the 'global environment in which governments operate.'[41] We can identify their state-like status due to their sovereignty over digital space, the resources and constraints they face, their maintenance over foreign relations and accountability towards shareholders, employees, users and advertisers.[42] Bremmer classifies tech companies into different worldviews: globalism, nationalism and techno-utopianism.[43]

Globalism entails firms that operate on a truly international scale by creating and populating digital space, 'allowing their business presence and revenue streams to become untethered from physical territory'[44] such as Apple, Facebook and Google. These firms compete fiercely and

[38] The Economist, "Democracies must team up to take on China in the technosphere"
[39] *ibid.*
[40] Ian Bremmer, "The Technopolar Moment: How Digital Powers Will Reshape the Global Order." *Foreign* Affairs (New York, N.Y.) 100.6 (2021): 112-28.
[41] *ibid.*
[42] *ibid.*
[43] *ibid.*
[44] *ibid.*

operate in as many countries as possible within the constraints of local regulations. Nationalism, on the other hand, entails firms more willing to align themselves explicitly with the priorities of their home governments by partnering with their governments in both selling their products and guiding government actions.[45] The most fitting examples are Chinese firms, such as Huawei, SMIC, Alibaba, and so on; however, Bremmer argues that some historically globalist US companies, most prominently Amazon and Microsoft, are now inching towards nationalism. The third category is techno-utopianism, which is championed by firms which consider technology 'not just as a global business opportunity but also a potentially revolutionary force in human affairs.'[46] The CEOs of these firms, such as Elon Musk (CEO of Tesla and SpaceX) do not seek to fit within the statist paradigm by gaining independence or seeking profit-driven opportunities from their governments, but rather envision a future where the nation-state is dislodged and replaced altogether. Overall, Bremmer concludes that 'it is simply no longer tenable to talk about big technology companies as pawns their government masters can move around on a geopolitical chessboard.'[47]

Stephen M. Walt, a post-Cold War realist, countered Bremmer's account. He argued that Big Tech firms will not supplant or replace the nation-state at any point in the foreseeable future and that states will remain the dominant unit of analysis for the geopolitical realm.[48] Walt's criticisms of Bremmer's argument include that as opposed to digital space, physical space is essential to human life, that the ultimate tool of statecraft, the legitimate use of force, is retained by states, and 'when there are trade-offs between security and political authority and technological innovation – and clearly there are – governments (and societies) are likely to accept somewhat less of the latter to preserve the former.'[49] Governments provide human

[45] Bremmer, "The Technopolar Moment"
[46] *ibid.*
[47] *ibid.*
[48] Stephen M. Walt, "Big Tech Won't Remake the Global World Order" *Foreign Policy* (8 November 2021) <https://foreignpolicy.com/2021/11/08/big-tech-wont-remake-the-global-order/> (accessed 27/12/21)
[49] *ibid.*

beings with basic security; firms, on the other hand, are 'backstopped' by rules enacted and enforced by governments.[50]

Walt also questions whether Big Tech is truly an unprecedented phenomenon in human history. He turns to the 1970s, when scholars such as Raymond Vernon, Richard J. Barnet and Ronald E. Muller exaggerated claims that multinational corporations were imposing constraints on states, and the 20th century, when we witnessed the United States Steel Corp. eventually be tamed to the current 8 percent of share of domestic steel consumption. Another example was provided by Brooke Masters, who argued that in the 19th century, for-profit railway companies wielded monopoly power, yet were later subjected to federal regulation.[51] By pointing to China and Russia's crackdown on their respective tech sectors, despite the technical challenges, Walt argues that 'the unfettered environment in which these firms have grown is disappearing, as states around the world assert their authority over a wide range of activities in the digital space.'[52] Walt uses the historical human tendency to see scientific or technological revolutions as transforming the geopolitical map yet not resulting in such drastic consequences. Overall, he concludes that 'nonstate actors of all types – including Big Tech firms – will continue to operate in a political and institutional framework set by national governments.'[53]

This debate explicitly lays out two opposite camps in the analysis of the importance of geopolitical postures of private sector actors. Importantly for this project, Bremmer introduces a broad theorisation and categorisation of geopolitical postures. Other scholars have approached the topic from different angles. Nancy Ayer Fairbank has argued that Microsoft, for example, seems to be seeking an 'expansion and consolidation of its role as a quasi-public

[50] Walt, "Big Tech Won't Remake the Global World Order"
[51] Brooke Masters, "Apple has too much power over its rivals" *Financial Times* (1 November 2021) <https://www.ft.com/content/94d9f964-10d8-4ff3-9781-821f3fc9ee3a> (accessed 27/12/21)
[52] Walt, "Big Tech Won't Remake the Global World Order"
[53] *ibid.*

actor,'[54] and since political action has become progressively more accessible to non-state actors, 'these new players are seeking to expand the sphere of their political influence.'[55] ShinJoung Yeo instead analysed the 'geopolitics of search' through the case of Google's struggles in China, arguing that the 'structure of political economy that animates relations between Google, the US, the transnational Internet industry, and China is, in fact, suggestively ambiguous by illuminating the changing dynamics of the US-led trans-nationalising capitalism.'[56] In other words, Yeo explains that Google's case reveals the fragility and volatility of the US-dominant information and communication, to which the US is responding by 'retooling and readjusting to accommodate China.'[57] Although this perspective maintains the view of companies as tools or victims of geopolitical dynamics, it moves away from a state paradigm and introduces the importance of the 'trans-nationalised global economy' as shaping the political dynamics between the US and China rather than the other way around.

Policymakers

Policymakers have also increasingly devoted attention to the geopolitical actorness of the private sector. The heightened focus on the importance of the private sector is perceived in several states, such as the UK, whose Foreign Affairs Committee launched an enquiry on tech and UK foreign policy. During a hearing, Tobias Feakin, Ambassador for Cyber Affairs and Critical Technology at the Australian Department of Foreign Affairs and Trade, argued that tech companies are 'growing to extraordinary levels and sizes, and having the kind of influences on our societies that I imagine many governments could only dream of.'[58] He points

[54] Fairbank, "The State of Microsoft?" p.397
[55] *ibid.*
[56] ShinJoung Yeo, "Geopolitics of search: Google versus China?." *Media, Culture & Society* 38, no. 4 (2016): 591-605. p.592
[57] *ibid.* p.601
[58] Foreign Affairs Committee, "Oral Evidence: Tech and the future of UK foreign policy, HC 201" *House of Commons* (7 September 2021) <https://committees.parliament.uk/oralevidence/2662/pdf/> (accessed 09/11/21)

out that governments struggle to keep up to date with the technology and producing policy architectures flexible enough to allow them to react in different areas of technology. In terms of the nature of these companies, he claims that 'it is hard at times to pinpoint where certain companies' ethics and standards lie, because it seems to adjust, depending on where the next business opportunity is.'[59] This statement alludes to the tension that firms are increasingly facing between profit maximisation and value-driven geopolitical posturing. Big Tech companies have responded to such concerns through vague concepts such as responsibility; following the Cambridge Analytica scandal of Facebook, CEO Mark Zuckerberg, in a speech to the press, repeated the word 'responsibility' 17 times.[60] Moreover, interest in tech companies has emerged in different parts of government apparatus. In his first public speech since taking up his role in October 2020, Richard Moore, head of the Secret Intelligence Service, argued that MI6 needs to be more 'open' and work with the private sector.[61] As reported in *The Telegraph,* in the future, 'Britain's spies will use the National Security Strategic Investment Fund to reveal "mission problems" to companies in the private sector that would not normally work with national security.'[62]

Importantly, variation in technology companies' approaches towards geopolitics is being identified by policymakers and analysts. Anne Marie Engtoft Larsen, Tech Ambassador at the Ministry of Foreign Affairs in Denmark, alluded to such differences by arguing that tech companies are 'as different from each other as countries' as they have 'different business models, different corporate cultures and different levels of maturity.'[63] Clay Shirky, who teaches at New York University, argued that 'while Microsoft has a mentality in which national

[59] Foreign Affairs Committee, "Oral Evidence" (7 September 2021)
[60] Tomer Shadmy, "The Emergence of Responsibility as a Global Scheme of Governance" in Hannes Hansen-Magnusson and Antje Vetterlein, *The Routledge Handbook on Responsibility in International Relations.* New York, NY: Routledge, 2022. p.43
[61] Dominic Nicholls, "MI6 needs to come out of the shadows and change culture of secrecy, warns spy chief" *The Telegraph* (30 November 2021) <https://www.telegraph.co.uk/news/2021/11/30/mi6-needs-come-shadows-change-culture-secrecy-warns-spy-chief/> (accessed 30/11/21)
[62] *ibid.*
[63] Foreign Affairs Committee, "Oral Evidence" (7 September 2021)

sovereignty still trumps ethical arguments (…) Google is trying to balance the rights of sovereignty against its own evolving set of values.'[64] He further linked variation in US tech companies' approaches towards foreign states to the companies' origins: 'it's no accident that Microsoft was founded during the cold war while Google was founded after the cold war.'[65] Tech companies are also pointing fingers among themselves for value-driven explanations of their business interactions, with Palantir CEO Alex Karp stating, in November 2021, that companies should work where they can 'ethically justify' and if they 'want to work in China or in any other country that is adversarial (to the US)' they should 'disclose it and defend it.'[66]

Policymakers' interest in the geopolitical postures of tech companies has increased further in the context of attempts to understand and explain the role that these actors play in the dynamic of strategic competition over technological superiority between the US and China. Evidence of the potential political agency and influence of tech industry practitioners in this dynamic can be discerned by the circulation in the Biden administration of a report published by the China Strategy Group, a bipartisan group which includes academics, former policymakers, engineers, venture capital investors and technology executives. The report advances policies that position the United States to 'out-compete China' and proposes the creation of a new multilateral forum, named the T-12, 'to strengthen cooperation among like-minded countries.'[67]

Overall, this section shows that there is an increasing interest in the topic among scholars and pundits. Nevertheless, there is a gap in the literature on understanding the strategic role that US private sector actors in the technology industry play in the 21st century. Theorisation

---

[64] Mark Landler, "Google Searches for a Foreign Policy" *New York Times* (27 March 2010) <https://www.nytimes.com/2010/03/28/weekinreview/28landler.html> (accessed 04/11/21)
[65] *ibid.*
[66] Samantha Subin, "Palantir CEO says companies working with US adversaries should justify their position" *CNBC News* (23 November 2021) <https://www.cnbc.com/2021/11/23/palantir-ceo-companies-working-with-us-adversaries-should-justify-their-position-.html> (accessed 02/12/21)
[67] China Strategy Group, "Asymmetric Competition: A Strategy for China and Technology: Actionable Insights for American Leadership" (Fall 2020) <http://industrialpolicy.us/resources/SpecificIndustries/IT/final-memo-china-strategy-group-axios-1.pdf> (accessed 12/10/21)

on companies' geopolitical posturing has hitherto been informal, with a clear lack of consensus on what its definition, scopes, and stakes are.

2.3. US Approach to Tech Policy

The literature exploring the private sector's role in states' foreign policy sheds light on the unique political dynamics these companies bring to the global arena. Yet, it often lacks a comprehensive exploration of how the dynamics of private sector agency are harnessed by states, particularly the US, in the context of strategic competition with rivals like China. I will first provide an overview of tech policy. I then delve into the literature on the US approach to tech companies: economic statecraft, followed by the strategic value of US Big Tech in US-China competition, and finally the relationship between the US government and US Big Tech companies.

2.3.1. Technology Policy

In this thesis, I adopt Charles Weiss' definition of technology as 'any application of organised technical knowledge about the natural world for a practical purpose, or the capacity to develop and use such knowledge.'[68] This definition includes advanced technologies such as space, information and biotechnology.[69] Technology policy can be defined as the strategic framework and set of guidelines adopted by states to govern the development, acquisition, and utilisation of technology in the international arena. This also includes the formulation of policies and regulations that influence the creation, dissemination, and transfer of technology across borders, as well as the management of technological resources to advance national

[68] Charles Weiss, "How Do Science and Technology Affect International Affairs." *Minerva (London)* 53, no. 4 (2015): 411–430. p.412
[69] *ibid.*

interests and enhance global competitiveness.[70] In this light, scholars have argued that that technology policy is rapidly becoming 'everything policy.'[71] Consequently, we are in urgent need of conceptual, theoretical and empirical explorations of tech policy in IR terms. This urgency is equal in academia and policymaking, as the latter must grapple with regulatory fragmentation between cities, regions and countries, as well as rely on the services of 'the same technology firms that (policymakers) would like to influence.'[72]

The concept of technology policy is not widely discussed in IR literature. Despite acknowledgment that science and technology play a significant role in foreign policy matters,[73] scholars have noted that there has been 'little systematic effort to probe the character of the relationship of science and technology to the substance of foreign policy.'[74] Before the explosion of the internet, Eugene Skolnikoff raised concerns about the impact of technological advancements on traditional concepts of national sovereignty,[75] whilst Charles Weiss emphasised the ability of new technologies to alter the practical meaning established IR concepts.[76] Conversely, in this thesis I aim to show the analytical gains of grounding technology-related studies on more robust IR theoretical underpinnings. As Tim Stevens wrote, 'there is room in the literature for preliminary attempts at re-grounding cyber security on firmer ontological foundations,'[77] and this is also true for other forms of technology-related studies.

Throughout my thesis, I centre on the intersection of tech policy and foreign policy, with a specific focus on the US government's interactions with its tech companies, efforts to

[70] Heleen De Coninck, Carolyn Fischer, Richard G. Newell, and Takahiro Ueno. "International technology-oriented agreements to address climate change." *Energy Policy* 36, no. 1 (2008): 335-356.
[71] Nicholas Davis, Landry Signé, and Mark Esposito, "Rethinking technology policy and governance for the 21st century" *Brookings Institute* (11 January 2022) <https://www.brookings.edu/articles/rethinking-technology-policy-and-governance-for-the-21st-century/> (accessed 11/09/23)
[72] *ibid.*
[73] Skolnikoff, Eugene B. *Science, technology, and American foreign policy*. MIT Press, 1967. p.4
[74] *ibid*.
[75] Skolnikoff, Eugene B. *The Elusive Transformation: Science, Technology, and the Evolution of International Politics*. Core Textbook. Princeton, NJ: Princeton University Press, 1994.
[76] Weiss, "How Do Science and Technology Affect International Affairs." p.417
[77] Tim Stevens, *Cyber Security and the Politics of Time*. Cambridge: Cambridge University Press, 2016.

undermine the tech companies of other states, and the independent actions of tech companies. The subsequent sections will delve into relevant literature to provide a comprehensive understanding of these dynamics.

2.3.2. Economic Statecraft

The most insightful literature on companies as agents in the international sphere, and on how states can leverage the position of these actors, is that of economic statecraft, a subfield of foreign policy studies. However, most of this literature focuses on Chinese companies. The independent variable tends to be state control, which in the US, given that it is has a completely different government model, is not a relevant analytical concept.

Economic statecraft is defined as 'the state's intentional manipulation of economic interaction to capitalise on, reinforce, or reduce the associated strategic externalities.'[78] The prerequisite for effective economic statecraft is that states 'must first be able to control the behaviour of commercial actors that conduct the vast majority of international economic activity.'[79] Scholars have primarily employed ideas of economic statecraft to analyse Chinese cases. James Reilly, for example, was inspired by such literature to devise his theory on China's orchestration approach which integrates three core elements: the 'nesting' of orchestration tactics within its hierarchical structures; the use of lucrative 'tournaments' designed to attract eager participants whilst facilitating oversight and discipline; and designing economic statecraft initiatives to maximise interest alignment between central leaders' foreign policy goals and the interests of key implementing actors.[80] However, Norris argues that if a nation has a more liberalised domestic political economy, such as the US or the UK, his theory of economic statecraft might still apply because such cases will 'simply have different values

[78] William J. Norris, *Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control*. Ithaca, NY, 2016. p.13
[79] *ibid.* p.3
[80] Reilly, *Orchestration,* p.1

across many of the independent variables'[81] that he identifies. He explains that applying the theory to more liberal regimes simply 'relaxes some of the fundamental business-government assumptions and the domestic political economic context conditions that are present in the China cases.'[82] No such cases however have emerged in the literature, indicating that it may not be as applicable as Norris argues.

It is interesting to note that the US and China seem to have different approaches to economic statecraft. Whereas the latter has a 'no-holds barred approach to industrial policy to improve its competitive position in the international arena,' for the US 'the very idea of industrial policy is one that raises red flags.'[83] However, some claim that the US has long pursued an industrial policy, as 'what passes for "industrial policy" is a hodge podge of disconnected initiatives that beg a coordinating strategy.'[84] That is what renders this topic ever more significant, as an understanding of the business-government relationship in the tech sector within the US would allow for an identification of the shortcomings of the current strategy.

Linda Weiss argues that 'paying attention to quintessential state purpose is key to understanding the differences between industrial policy and statecraft' as statecraft derives from responding to challenges arising from the international arena, despite the policy focus being domestic. She argues that a statecraft approach allows us to correct two widespread views: the first is that America's post-war technological pre-eminence was the product of free market entrepreneurship. Instead, she argues it 'was the exercise of statecraft that enable the United States to emerge after the Second World War as the world's undisputed high-tech hegemon.'[85] The second is the view that the US pursues an industrial policy as a hidden development state, to which she replies that 'if an industrial sector has little or no relevance to

[81] Norris, *Chinese Economic Statecraft,* p.231
[82] *ibid.*
[83] Weiss, "Re-emergence of Great Power Conflict and US Economic Statecraft." p.163
[84] *ibid.*
[85] *ibid.* p.164

the broader national security enterprise, it is unlikely to attract serious or sustained government support.'[86] Overall, she argues that 'in its American incarnation, economic statecraft prioritises technological superiority as a strategic imperative and enlists in that pursuit the relevant private sector partners and agencies tasked with national security missions.'[87] As such, it differs from industrial policy, which 'encompasses any kind of state support aimed at economic activity regardless of objectives, drivers or motivations.'[88]

Linda Weiss and Elizabeth Thurbon trace security-motivated statecraft in the US. They argue that US statecraft continues to have national security rather than economic competitiveness as its primary mission.[89] They argue that commerce and America's so-called 'national security state' (NSS) have become increasingly integrated, as geopolitical concerns have led policymakers to factor some commercial benefits into national security-related, high-tech programmes. What they emphasise is that without the mindset of security logic and persistent geopolitical stimulus, the US innovation engine would not exist in anything like its present form. This sets it aside from other states. They explain that 'through relationships of governed interdependence, the NSS thus expands its commercial reach to advance its projects, while giving the private sector a stake in the outcomes.'[90] Overall, Weiss and Thurbon conclude that 'technological leadership for the United States can never be a purely commercial matter'[91] and that US support of an industrial technology is critically tested by national security.

Relevant to this project in particular, Weiss and Thurbon point to the controversies of collaboration with private firms. They draw on the example of Silicon Valley's high-tech firms, which grew on the back of defence and space contracts through the 1950s and 1960s,[92] but

[86] Weiss, "Re-emergence of Great Power Conflict and US Economic Statecraft."
[87] *ibid.*
[88] Linda Weiss and Elizabeth Thurbon. "Developmental state or economic statecraft? Where, why and how the difference matters." *New Political Economy* 26, no. 3 (2021): 472-489. p.473
[89] *ibid.* p.479
[90] *ibid.* p.481
[91] *ibid.* p.482
[92] Thomas Heinrich, "Cold war armory: military contracting in Silicon Valley." *Enterprise & Society* 3, no. 2 (2002): 247-284.

have been reluctant to work on NSS projects as profits afforded by new commercial markets have become more attractive.[93] They identify the role of American 'anti-statism' in the valorisation of private initiative, which shapes the way government interacts with the private sector. Rather than heavy-handed top down control or counting on the private sector to foster innovation from bottom up, NSS agencies have carved out a distinctive public-private hybrid approach: either 'a contractual relationship between NSS, industry, and research institutions (…) or a more permanent hybrid arrangement that institutionally fuses public purpose/resources/or ownership with private management/control.'[94] Examples include the privately managed national labs known as Federally Funded Research and Development Centres (FFRDCs), the Stanford Research Institute (so-called star of Silicon Valley) and the much lauded venture capital fund, In-Q-Tel, owned by the CIA.

Overall, this literature provides an understanding of how states can leverage the position of company actors in their foreign policy, predominantly through the concept of economic statecraft. In this section, it becomes clear that whilst China's approach to economic statecraft has been studied, the United States' government use of tech companies as strategic assets, foreign policy-wise, is contested and poorly understood.

2.3.3. The Strategic Role of US Big Tech in US-China Competition

Next, I turn to the literature focusing on the US leveraging of its tech private sector in its strategic competition with China. Although this literature is most closely aligned with the research question, it often lacks rigorous analysis on how the unique characteristics of the US approach impacts its overall strategic position in tech war with China. This section underscores the need for a more detailed examination of the trade-offs and implications tied to the US

[93] Weiss and Thurbon, "Developmental state or economic statecraft?" p.481
[94] *ibid.* p.484

approach, which forms the central focus of this thesis. Although IR literature is rich in analyses of the role of a range of individual and corporate actors in US Foreign Policy,[95] the role of tech companies in particular remains limited.

Klon Kitchen, Director of the Heritage Foundation's Centre for Technology Policy, argues that three trends have led to the rise of tech companies as 'geopolitical stakeholders that often challenge the authority, sovereignty and the capacity of governments.'[96] The three trends are tech companies' expanding global presence, the role of digital and social media in political discussion and action, and finally, the fact that they lie at the centre of critical national security capabilities and methodologies.[97] Kitchen identifies variation in government responses to tech's growing geopolitical influence, rooted in a nation's political form, its relative economic strength, and its broader global ambitions. The US approach, specifically, is summarised as 'engage and invest.'[98] Although the US government is dependent on private sector actors, he argues that big tech responses to government overtures have been uneven; companies like Microsoft and Amazon have clearly signalled their intent to work with federal government, whereas Google has not, as shown by the termination of its participation in the Pentagon's AI research effort, Project Maven, in 2018.[99]

Unlike China, the US has traditionally embraced a more laissez-faire approach toward its technology sector, reflecting its broader commitment to free-market principles. The government's role has been primarily to enforce laws and regulations that promote competition, protect customers, and uphold privacy and security standards, whilst also investing in

---

[95] Andrew Payne, *War on the Ballot: How the Election Cycle Shapes Presidential Decision-Making in War*. Columbia University Press, 2023; Valerie M. Hudson, "Foreign policy analysis: Actor-specific theory and the ground of international relations." *Foreign policy analysis* (2005): 1-30; Karen E. Smith, "Missing in analysis: Women in foreign policy–making." *Foreign Policy Analysis* 16, no. 1 (2020): 130-141.
[96] Klon Kitchen, "The New Superpowers: How and Why the Tech Industry is Shaping the International System" *National Affairs,* Number 29 (Fall 2021) <https://nationalaffairs.com/the-new-superpowers-how-and-why-the-tech-industry-is-shaping-the-international-system> (accessed 29/11/21)
[97] *ibid.*
[98] *ibid.*
[99] *ibid.*

fundamental research that can spur technological innovation. In recent years, however, this approach has come under scrutiny as the tech sector's influence expanded globally. One contentious point revolves around data sovereignty and digital privacy, with laws like the US CLOUD Act of 2018 exemplifying the tension. The Act allows US law enforcement to access data stored overseas by American companies, sparking concerns about data privacy and sovereignty, potentially creating friction between US tech companies and their international users.

The approach of the US has become more fragmented as a result of conflicting regulations at the federal and state levels, inconsistencies in enforcement, and differing company geopolitical stances. These elements contribute to an unpredictable business environment for US tech companies and could potentially weaken their competitive position in the international market. An example of this can be seen in the ongoing debate about the regulation of Big Tech companies and antitrust concerns. At the same time, some US policies can be seen as an attempt to leverage the power of the tech sector in the global arena, similar to China's more overt approach. For example, the Clean Network programme, launched by the State Department, which seeks to exclude Chinese tech firms from Internet infrastructures in other countries. Another example is the Defence Innovation Unit (DIU), an initiative developed by the US Department of Defence aimed at expediting the adoption of cutting-edge technology into the US military. These policies can often clash with the free-market principles that the US traditionally upholds, leading to a somewhat paradoxical and fragmented approach.

Moreover, scholars have called for the US to harness Big Tech to compete with China. Dan Goure has explained that 'US Big Tech companies currently dominate their Chinese rivals in terms of innovation. That could change, however, if the US government undermines Big Tech's

competitive edge.'[100] He explains that the antitrust reforms that Congress is pursuing would greatly harm US advanced tech firms. Overall, the existing scholarship on how the US utilises its private tech sector in strategic rivalry with China is notably fragmented. To construct my thesis, I have pieced together nuanced insights from a diverse array of sources and IR sub-fields, given the absence of consolidated literature on the subject.

2.3.4. The Relationship between the US Government and US Big Tech Companies

Finally, I discuss the existing literature on the US' contemporary domestic relationship with its tech private sector. Whilst these works help to understand the evolving dynamics between the US government and tech firms, they often overlook how these interactions affect the US standing in its competition with China. The literature tends to invariably separate domestic policy and international strategy, resulting in a gap in thorough and holistic analysis.

First, I address the current landscape of domestic relations between Big Tech and different parts of the US government. This exploration will provide insight into the positioning of tech companies with the US' overarching strategic objectives aimed at countering China. For years, major tech firms were treated as 'quasi-sovereigns' with Microsoft proclaiming itself a 'neutral digital Switzerland.'[101] However, there are indications that American policymakers may no longer tolerate the neutrality of US firms. In 2020, Republican Senator Josh Hawley emphasised that the choices lie between 'American principles and free-speech or short-term global profits and censorship.'[102]

On the one hand, we can observe a contemporary trend of governmental crackdown on Big Tech. Some US policymakers advocate for breaking up and regulating Big Tech, as technology

[100] Dan Goure, "The US Needs to Harness Big Tech to Compete with China" *The National Interest* (14 September 2022) <https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/us-needs-harness-big-tech-compete> (accessed 03/07/22)
[101] Helberg, "Silicon Valley Can't Be Neutral in the US-China Cold War"
[102] *ibid.*

companies' growing entanglements in China create vulnerabilities for the US 'by exposing its firms to espionage and economic concern.'[103] There is increasingly bipartisan support for higher levels of Big Tech companies' regulation, stemming from an 'American tradition of suspicion of big corporations.'[104] Data from the Pew Research Centre found that Democrats and Republicans do not differ in their opinions about the impact of breaking up major tech companies.[105] From a public opinion standpoint, it was found in July 2021 that 56% of Americans support more regulation of major technology companies and 68% believe these firms 'have too much power and influence in the economy.'[106]

In policy environments the tension between Big Tech and government is palpable. A view has become widespread that 'unelected, (tech giants) ended up eroding the line between political and commercial.'[107] In the realm of Artificial Intelligence (AI) development, Col. Drew Cukor, who leads the Pentagon team charged with laying out a plan to begin realising the promise of AI for the US military, claimed that 'we are in an AI arms race, and it's happening in industry, in the Big Five' – referring to Amazon, Apple, Facebook, Google and Microsoft – 'the computer science departments of our major universities are wiped out because the professors are all on sabbatical doing this work.'[108] Overall, in 2021 it was reported that the divide between Silicon Valley and Washington D.C. is 'as deep as ever' as 'officials in

[103] Ganesh Sitaraman, "Too big to prevail: The national security case for breaking up big tech." *Foreign Aff.* 99 (2020): 116
[104] Shira Ovide, "Why Washington Hates Big Tech" *The New York Times* (23 October 2020) <https://www.nytimes.com/2020/10/23/technology/why-washington-hates-big-tech.html> (accessed 19/12/21)
[105] Emily A. Vogels, "56% of Americans support more regulation of major technology companies" *Pew Research Centre* (20 July 2021) <https://www.pewresearch.org/fact-tank/2021/07/20/56-of-americans-support-more-regulation-of-major-technology-companies/> (accessed 26/12/21)
[106] *ibid.*
[107] Treverton and Esfandiari, "Viewing tech giants as a geopolitical force"
[108] Bradley Peniston, 'How Will the Pentagon Create its AIs? The Algorithmic-Warfare Team is Charting a Path' (13 July 2017) <https://www.defenseone.com/technology/2017/07/artificial-intelligence-pentagon/139402/> (accessed 15/11/21)

Washington are more keyed on the society-wide risks tech cooperation poses, while workers in tech are focused on shipping products and making money.'[109]

On the other hand, the divide between the US government and Big Tech is less clear. In July 2020, Jack Poulson revealed that numerous Department of Defence and federal law enforcement agencies secured thousands of deals with Google, Amazon, Microsoft, Facebook and others, that had been previously unreported.[110] Poulson found that the majority of the deals with consumer-facing tech companies involved procurement contracts, which he claims mask 'the depth of the ties between tech companies and federal law enforcement agencies and the Department of Defence.'[111]

The history of Silicon Valley can shed light on the close-knit relationship between tech companies and the US military. As argued by Margaret O'Mara, a professor at the University of Washington, 'Silicon Valley has always been in the business of war and the specific process of contracting and subcontracting with the military is familiar in the Valley too, dating back to the 1950s and 60s.'[112] She explains that 'one of the main reasons tech became so adamant about "thinking differently" and emphasising how they are a new style of enterprise, is because tech was so closely intertwined with the military.'[113] Indeed, Silicon Valley companies are said to have been 'built on a foundation of government intervention and public monies,'[114] as during the 1960s, the Advanced Research Projects Agency (DARPA) funnelled funds into the research and development of technologies relied on by tech giants. Yll Bajraktari, executive director of the National Security Commission on Artificial Intelligence, explained that 'Silicon Valley

[109] David Wertime and Protocol China Staff, "US Tech Wants to Work More With China" *Protocol* (17 March 2021) <https://www.protocol.com/newsletters/protocol-china/tech-workers-on-china?rebelltitem=2#rebelltitem2> (accessed 03/01/22)
[110] Jack Poulson, "Reports of a Silicon Valley/Military Divide Have Been Greatly Exaggerated" *Tech Inquiry* (July 7, 2020) <https://techinquiry.org/SiliconValley-Military/> (accessed 26/11/21)
[111] Glenn Harvey, "Thousands of contracts highlight quiet ties between Big Tech and US military" *NBC News* (July 8, 2020) <https://www.nbcnews.com/tech/tech-news/thousands-contracts-highlight-quiet-ties-between-big-tech-u-s-n1233171> (accessed 26/11/21)
[112] *ibid.*
[113] *ibid.*
[114] Solon and Siddiqui, "Forget Wall Street – Silicon Valley is the new political power in Washington"

traces its origins to the Department of Defence and the aerospace and defence industry,' pointing to technologies such as Radar, GPS and Arpanet within which the military's involvement was instrumental.[115] Moreover, the way in which Silicon Valley firms can influence government is through the traditional practice of lobbying. America's most powerful industries influence policymakers in numerous ways, such as funding think tanks and spending their days 'swarming over members of Congress to ensure their private interests are reflected in legislation and regulation.'[116]

As reported in the *Financial Times,* Miriam Vogel, chief executive of EqualAI, describes Silicon Valley's relationship with the government and military as 'deeply interconnected and increasingly fraught.'[117] She explains that highly paid tech employees are voting 'with their feet, pressuring companies to be more vocal about the values they stand for – often in opposition to the concerns of security officials.'[118] This calls on questions which arise on the relationship between tech and federal law enforcement agencies on the domestic level, such as the well-known stand-off between Apple and the FBI, when the former refused to break into an iPhone linked to the 2015 terrorist attack in San Bernardino, California, for the latter.

Overall, at the most basic level, in the US the relationship between private firms and the national security establishment is 'hardly flawless' but in general, 'Americans expect that companies will adhere to free expression, the rule of law, basic protections involving searches and seizures, and the requirements of due process.'[119] From Silicon Valley, we can see some pushback in engaging with governments. In 2019, Palantir CEO Alex Karp stated that 'no company should have to work for the government,' and 'if we want to preserve a democracy in which protests are part of our DNA, we need to make sure the decisions are made by elected

[115] Patrick McGee, "Silicon Valley reboots its relationship with the US military" *The Financial Times* (May 17, 2021) <https://www.ft.com/content/541f0a02-ea27-43a4-b554-96048c40040d> (accessed 30/11/21)
[116] Solon and Siddiqui, "Forget Wall Street – Silicon Valley is the new political power in Washington"
[117] McGee, "Silicon Valley reboots its relationship with the US military"
[118] *ibid.*
[119] Helberg, "Silicon Valley Can't Be Neutral in the US-China Cold War"

representatives and judges, not by unelected engineers running global businesses in a precious corner of a Golden State.'[120]

In sum, this literature helps us understand the domestic relationship between the US government and the US tech private sector. However, it does not address how this domestic relationship affects US foreign policy, or how it influences the way in which the US government leverages its national tech champions as strategic assets.

2.4. Conclusion

In sum, whilst there is an array of rich bodies of literature relevant to my research, they fall short of answering my research question: *how has the US approach to tech policy regarding the tech private sector affected its standing in the technological competition with China?* In the first section, I provided an overview of the literature on the broader geopolitical implications of the US-China tech war. Whilst the tech war context is vital, this body of literature largely overlooks the role of US private tech firms, focusing instead on interactions between states. The concept of weaponised interdependence is particularly crucial for my study, as it sets the stage for the strategic position the US held in past decades and provides the warning for the importance of US allies' support to the US for the US to retain this position. However, this body of literature falls short in directly addressing how the US's strategic position could potentially be compromised.

The second section centres on the significance of the tech private sector in the US-China great power competition. I began by examining why tech companies matter in IR. This included reviewing literature on how tech companies differ from past global corporations, which serves

[120] Alex Karp, "I'm a tech CEO, and I don't think tech CEOs should be making policy" *The Washington Post* (September 5, 2019) < https://www.washingtonpost.com/opinions/policy-decisions-should-be-made-by-elected-representatives-not-silicon-valley/2019/09/05/e02a38dc-cf61-11e9-87fa-8501a456c003_story.html> (accessed 03/05/22)

as important context, however does not answer my research question. I then explored the specific role of US 'Big Tech' firms in IR, highlighting an emerging scholarly and policy interest but also a lack of consensus on their strategic role and influence in the 21st century geopolitical landscape.

The third section focused on the US approach to tech policy, and in particular to leveraging the tech private sector. The existing literature highlight the political dynamics that tech companies introduce, but it generally lacks a thorough exploration of how these dynamics are deployed by the US in its competition with China. I first provided an overview of tech policy and then addressed the literature on economic statecraft. This scholarship offers an understanding of how governments can strategically employ companies in foreign policy. However, whilst China's strategy is well-documented, the US approach remains less understood and is a subject of debate. As I showed in the subsequent section, the most relevant literature to the US often lacks depth, particularly in analysing how the US's unique approach impacts its overall strategic position. This identified gap sets the stage for the core focus of my thesis.

Finally, existing literature on the relationship between the US government and its tech companies tends to be limited to domestic policy considerations. Although this literature is useful for understanding domestic dynamics, they do not extend this understanding to how it affects the US strategic position vis-à-vis China. Overall, given the fragmented nature of the existing scholarship on the strategic use of the US private tech sector, I have synthesised insights from various sources and IR sub-fields to construct my thesis.

3. Targeting US Tech Companies: Europe's Soft Balancing via Data Localisation

Thesis Paper 1

Abstract

In this paper, I examine the European Union's data localisation policies – regulations mandating the storage and processing of digital data within a state's territorial jurisdiction – as they pertain to US technology companies. I specifically investigate why US allies are choosing to adopt data localisation policies despite their evident economic drawbacks and security inefficiencies. My central argument posits that data localisation policies adopted by EU member states serve as a form of 'soft balancing' against US technological hegemony. To substantiate this claim, I conduct a case study of the European Cybersecurity Certification Scheme for Cloud Services (EUCS), drawing on both primary and secondary qualitative data. My findings indicate that the sovereignty requirements within the EUCS aim to reduce reliance on US tech companies, hinder US surveillance capabilities, and promote European tech industries. Despite facing significant criticisms for potentially disrupting global cybersecurity cooperation and creating divisions among EU member states, their persistence reveals a deliberate strategy of soft balancing.

3.1. Introduction

Over the past decade, data localisation policies – laws or regulations that mandate the storage and processing of digital data within a country's borders – have become a popular tool for states looking to exert greater control over their internal data flows. At face value, policymakers justify these policies in terms of enhancing 'data sovereignty,' and protecting sensitive information from external threats. However, data localisation policies can also be seen as a tool for states to manage their relationships with other states, particularly their allies and rivals.

The rise of data localisation policies is puzzling for two reasons. First, scholars expected US allies to broadly maintain an approach to data governance in line with that of the US, which emphasises market-led solutions and seeks to preserve a free internet.[1] Throughout the 2000s and 2010s, the expectation among scholars was that authoritarian states such as China and Russia would be the principal proponents of 'data sovereignty' ideologies – which is an inherently abstract concept. Contrary to these predictions, however, US allies, notably certain members of the European Union, are increasingly becoming staunch supporters of data localisation policies. The change in behaviour was emphasised by Lokke Moerel: 'until recently, Europe favoured the open, liberal market economy, and EU research had to be open to the world. Restoring Europe's digital sovereignty is now a core ambition of the European Commission.'[2]

Second, the growing support for data localisation policies is unexpected given the widespread criticism about their potential negative impacts on economic growth and innovation. Whilst I will elaborate further on the actual costs of data localisation policies in

[1] Dana Polatin-Reuben and Joss Wright. "An Internet with {BRICS} Characteristics: Data Sovereignty and the Balkanisation of the Internet." In *4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14)*. 2014.p.1

[2] Lokke Moerel, "The Ebb and Flow of Trans-Atlantic Data Transfers: It's the Geopolitics, Stupid!" *Future of Privacy Forum* (4 April 2022) <https://fpf.org/blog/the-eb-and-flow-of-trans-atlantic-data-transfers-its-the-geopolitics-stupid/> (accessed 09/03/23)

subsequent sections, to summarise, many economic analyses predict negative economic effects for all parties involved due to further restrictions on cross-border data flows. As Konstantinos Komaitis explained, 'Internet data were never meant to be boxed in or compartmentalised. Forcing data to be localised means going against the network itself. It means imposing a rule that the internet was never designed to follow, and which it does not understand.'[3]

Given these factors, the puzzle I address in this article is why US allies are choosing to adopt data localisation policies despite the overwhelming evidence that they undermine economic growth and innovation, as well as being ineffective at privacy protection and bolstering security. I focus on US allies, in particular EU member states, as they were seemingly least likely to adopt such policies given their previous ideologies on data governance as well as their relative likelihood to want to support the US in its tech war with China. Support from its European allies is crucial to US tech leadership: 'contrary to claims by neoconservatives that a supreme US can neglect a weak Europe, experts from the Council on Foreign Relations and the Brookings Institution argued in favour of respecting the status of Europe as an indispensable ally.'[4] Data localisation laws that hurt US private firms also hinder US attempts to maintain its technological edge in the ongoing competition against China. By introducing obstacles to the free flow of data, US allies risk jeopardising the supremacy of US tech firms and curtailing US influence in the global digital economy. Therefore, understanding and addressing this issue could have far-reaching implications for global tech leadership and the international digital economy.

I show that data localisation policies adopted by European member states can be viewed as a strategic 'soft balancing' act against the US tech dominance. Soft balancing is a strategy in which weaker states seek to constrain the power of a stronger state without resorting to direct

[3] Konstantinos Komaitis, "The 'wicked problem' of data localisation." *Journal of Cyber Policy* 2, no. 3 (2017): 355-365. p.358

[4] Franz Oswald, "Soft balancing between friends: transforming transatlantic relations." *Debatte: journal of contemporary central and Eastern Europe* 14, no. 2 (2006): 145-160.

confrontation. I test this theory through the case study of the European Cybersecurity Certification Scheme for Cloud Services (EUCS). Developed by the European Union Agency for Cybersecurity (ENISA), EUCS is a framework that seeks to ensure high-level cybersecurity for cloud services used by EU institutions, businesses, and citizens. Its 'sovereignty requirements' have sparked debate among policymakers, member states, cybersecurity experts, and industry actors, providing valuable insights into the motivations for and divisions on data localisation policies.

Data localisation policies impose significant economic costs on European states. Do states fully comprehend the magnitude of these costs and deem them a necessary sacrifice in pursuit of their objectives, as the argument that this is soft balancing implies? I consider here the potential counterargument that policymakers, more often focused on security and privacy laws, fail to fully grasp these complexities, leading to potential oversights in policy design.[5] However, the stark division in opinions among European member states on data localisation suggests that policymakers are having comprehensive, informed discussions about the pros and cons of the policy. This suggests that European states are deliberately using data localisation as a costly tool for soft balancing; the perceived gain in sovereignty outweighs the costs.[6]

The finding that European states employ data localisation as a tool for soft balancing against the US in the ongoing US-China competition reveals a critical vulnerability of US tech companies: their susceptibility to the ramifications of poor alliance management by the US government. We can further understand the implications of the findings through the concept of 'weaponised interdependence,'[7] which describes how actors leverage their interconnectedness to exert influence. The US's historical dominance in technology and internet standards

[5] Matthias Bauer, Hosuk Lee-Makiyama, Erik Van der Marel, and Bert Verschelde. *The costs of data localisation: Friendly fire on economic recovery*. No. 3/2014. ECIPE Occasional Paper, 2014. p.10
[6] Whether this is objectively the case and the benefits of 'soft balancing' against the US justify these costs is beyond the scope of this paper.
[7] Henry Farrell and Abraham L. Newman, "Weaponized interdependence: How global economic networks shape state coercion." *International Security* 44, no. 1 (2019): 42-79

positioned it at the centre of these networks. However, as Henry Farrell and Abraham L. Newman warn, this centralised position is precarious.[8] The tension arising from US actions can alienate allies, prompting them to 'defect' and seek alternatives.[9] This paper empirically reveals this phenomenon at play, showing allies' defection from US leadership through European states' move towards data localisation, targeting US tech companies and consequently weakening the US's strategic position. My findings therefore provide evidence towards Farrell and Newman's warning about the potential pitfalls of wielding such influence, highlighting the delicate balance of maintaining 'weaponised interdependence' without overstepping.

From the point of view of European states, this study highlights the challenges they face in navigating a global digital economy dominated by foreign powers. Ultimately, I argue that the adoption of data localisation policies is a significant geopolitical development with far-reaching implications not just for the US tech industry and the US-China rivalry, but also for the policy choices and strategic positioning of European states themselves. This research can inform European policymakers, highlighting the need for careful policy calibration to balance domestic interests, alliance dynamics, and broader ramifications of their decisions on the global digital economy.

In the first section of this paper, I delve into the current literature on data localisation policies and the deteriorating trust between the US and the EU in the tech sector. Subsequently, I introduce the theoretical framework, discussing the theoretical mechanisms that connect data localisation policies to soft balancing against the US. I will then present the case study on the European Cybersecurity Certification Scheme for Cloud Services (EUCS). To conclude, I discuss the policy implications of my findings for European states, as they navigate the complex dynamics of digital sovereignty, international alliances, and global tech competition.

[8] Farrell and Newman, "Weaponized interdependence" p.45
[9] *ibid.*

3.2. Literature Review

3.2.1. Data Localisation Policies

Data localisation policies, or rules necessitating the storage and processing of data within specific territories, have seen a substantial growth in popularity. On the surface, these policies are driven by concerns over foreign interference and the need to limit access to data stored outside a country's jurisdiction. However, my research reveals that the motivations behind these policies might be more strategic than they appear.

Data localisation policies typically target a growing range of specific data types and broad categories of data deemed 'important' or 'sensitive' or related to national security.[10] The number of countries that have enacted data localisation requirements has nearly doubled from 35 in 2017 to 62 in 2021.[11] By June 2022, 75% of all countries had implemented some level of data localisation rules.[12] Current and emerging regulations fall into four broad categories: (1) geographic restrictions on data export, which require data to be stored and processed within a given country or region; (2) geographical restrictions which allow data to be copied outside the country of origin for processing but require a replica in the local infrastructure, (3) permission-based regulations, which require institutions to get consent from specific individuals to transmit data, and finally (4) standards-based regulations which allow institutions to move data more freely outside the originating jurisdictions but require them to ensure the security and privacy of their customers' data.[13]

---

[10] Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them" *Information Technology and Innovation Foundation* (July 2021) <https://www.gmfus.org/sites/default/files/2023-03/Report%20-%20The%20New%20American%20Foreign%20Policy%20of%20Technology_1.pdf> (accessed 11/03/22) p.1

[11] Cory and Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," p.3

[12] McKinsey & Company, "Localisation of data privacy regulations creates competitive opportunities" (30 June 2022) <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities#/> (accessed 16/03/22)

[13] *ibid.*

Regardless of their rise in popularity, data localisation policies carry significant tangible costs. The costs of data localisation policies were summarised in a report by Frontier Economics, where researchers modelled a worst scenario in which the countries and their trade partners move from current policy settings to a high level of restrictiveness on cross-border data flows, essentially mandating local data storage and prohibiting overseas data storage. [14] The study finds that all selected economies, except China (already employing a highly restrictive approach), would face economic losses due to increased cross-border data flow restrictions. Importantly, this report revealed that a country's own data localisation measures tend to impact its exports more than the measures imposed by its partners; data localisation essentially acts as a self-inflicted tax on a country's own exports.[15]

Companies also face extensive costs due to data localisation. Companies often must establish local data centres in each jurisdiction they operate in, requiring a substantial initial investment and ongoing operational costs. They also face high compliance costs as they navigate often conflicting localisation regulations in different jurisdictions. In extreme cases, businesses might choose not to operate in countries with restrictive data localisation laws, leading to potential losses for these countries. For companies, data localisation policies result in a form of market fragmentation which entails an existential threat. Certain data localisation requirements essentially bar them from operating efficiently across multiple territories, eroding their global market advantage. Companies face varied and even contradictory localisation requirements and regulations which are worded vaguely and are applied inconsistently. In addition, data localisation policies undermine security for companies: they are reversing the

[14] Frontier Economics, "The Extent and Impact of Data Localisation: Report prepared for DCMS" (1 June 2022) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1125805/Frontier_Economics_-_data_localisation_report_-_June_2022.pdf> (accessed 15/03/22)
[15] *ibid.*

trend toward centralised security models, resulting in vulnerabilities such as data exfiltration and problems with infrastructure, encryption, and the integrity of source code.[16]

Various institutions highlight that the costs of data localisation are significant. The Information Technology and Innovation Foundation (ITIF), for example, asserts that 'a 1-point increase in a nation's data restrictiveness cuts its gross trade output 7 percent, slows its productivity 2.9 percent, and hikes downstream prices 1.5 percent over five years.'[17] Similarly, a paper by the European Centre for International Political Economy (ECIPE) terms the immediate and long-term economic effects of data localisation as 'dangerous', citing the complex interplay between data flows, supply chain fragmentation, and domestic prices.[18] Scholars also explain that data localisation moves against globalisation: 'for the past several decades, globalisation has encouraged the convergence of standards and lowered trade barriers. Data localisation works in the opposite direction by requiring increasingly local approaches.'[19]

Konstantinos Komaikis identifies three major problems with data localisation. First, attempting to implement data localisation laws compromises the internet's global reach, making enforcement impractical.[20] Secondly, there is a risk of state interference increasing in internet governance due to protectionist policies; this is concerning as favouring domestic companies from regions such as China or even the EU over US-based ones is discriminatory.[21] Third, there is a misconception that the solution to issues of security or economic growth can be found in mandating the localisation of data, which actually 'undermines the social, economic, and civil rights of users, as well as eroding the ability of businesses to compete and have access to a global network of customers.'[22] Data localisation is often the result of

[16] Frontier Economics, "The Extent and Impact of Data Localisation: Report prepared for DCMS"
[17] *ibid.*
[18] Bauer, et. al. *The costs of data localisation: Friendly fire on economic recovery*. p.10
[19] McKinsey & Company, "Localisation of data privacy regulations creates competitive opportunities"
[20] Komaitis, "The 'wicked problem'of data localisation."
[21] *ibid.*
[22] *ibid.*

inadequate or biased economic analysis, with ulterior motives of excluding foreign competitors or creating a few jobs in sectors like e-commerce, data centres or consultancies. However, any job growth resulting from data localisation is negligible compared to the economic and employment losses elsewhere.[23] As Emily Wu explains, rather than making data more secure, 'data localisation laws have handicapped innovation, increased regulatory complexity, and perhaps even threatened security.'[24]

How do policymakers justify these data localisation policies despite such limitations? ITIF outlines five justifications.[25] First, there is a misunderstanding that data localisation is the optimal method for data protection.[26] Second, data localisation is linked to digital protectionism, where policymakers use it to favour local firms and assert digital sovereignty and miss the complex economic, governance, social, and political factors determining a country's stance on digital issues. [27] Third, data localisation can be weaponised to force foreign firms to comply with easier data access for surveillance and political purposes. Digital authoritarian regimes like China and Russia perceive physical access to data centres as a vital facilitator of surveillance and political control. [28] The fourth reason relates to regulatory concerns about cross-border data access; some policymakers argue data localisation is the only way to ensure compliance with data requests from law enforcement and financial regulators.[29] This stems from the misguided belief that companies can evade oversight by merely moving data out of a country. Lastly, data localisation is justified as a preparatory measure for hypothetical international financial sanctions, viewing the national payments system as a part

[23] Komaitis, "The 'wicked problem'of data localisation."
[24] Emily Wu, "Sovereignty and Data Localisation" *Harvard Kennedy School Belfer Center for Science and International Affairs* (July 2021) <https://www.belfercenter.org/sites/default/files/2021-07/SovereigntyLocalization.pdf> (accessed 27/04/22) p.3
[25] Cory and Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," p.6
[26] *ibid.*
[27] *ibid.*p.6
[28] *ibid.*
[29] *ibid.*

of the country's critical infrastructure.[30] In summary, ITIF suggests policymakers often adopt a dual-use approach with an ostensible legitimate objective like data privacy or cybersecurity, while their primary (hidden) motivation may be protectionism, national security, or greater internet control. ITIF states that a tell-tale sign of such hidden motivations is a lack of evidence, transparency, debate, and engagement around a data localisation proposal.[31]

Finally, European policymakers often invoke the concept of digital sovereignty, understood as a state's control over its digital realm, encompassing data, software, standards, services, and infrastructure,[32] as a key rationale for implementing data localisation policies. This trend is amplified by the dominance of US and Chinese tech companies in the European digital market, raising concerns about foreign influence.[33] However, the pursuit of digital sovereignty through data localisation policies presents a paradox. Whilst data localisation offers a pathway to digital sovereignty by giving states more direct control over their data, it may not necessarily fulfil its intended objectives. Policymakers often overlook the economic, technological, and diplomatic implications these policies entail. Localisation may unintentionally foster market fragmentation, disrupt the global digital economy, and strain diplomatic relations. Therefore, despite policymakers' conviction that data localisation is a solution to digital sovereignty concerns, the actual effectiveness and broader impacts of these policies remain a puzzle.

Overall, the costs of data localisation policies seem to be extremely high, and policymakers' stated motivations for the policies do not seem to justify the downsides; their continued use hence presents the puzzle that occupies me here.

---

[30] Cory and Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them,"
[31] *ibid.* p.4
[32] Luciano Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU." *Philosophy & Technology* 33 (2020): 369-78. p.371
[33] *ibid.*

3.2.2. The Erosion of Trust between the US and the EU in Tech

In this section, I turn to the literature on the relationship between the US and the EU regarding the tech industry. This is important context to understand *why* EU allies would want to soft balance against the US. For many years, the US retained international market dominance through its tech companies and led the way in setting internet and data governance standards. However, a series of events contributed to the erosion of trust between the US and the EU, particularly due to issues related to privacy, data protection and government surveillance.

Achieving and retaining tech superiority in great power competition is crucial. As Jakobsson and Stolz explain, 'occupying critical global network nodes (e.g., routers, servers, online cloud services and also powerful roles in for example financial and political networks etc.) powered by advanced technology and knowledge is a primary objective in the global great power competition: node positions and network ties provide power and leverage.'[34] For many years, tech companies were essential to how the US was able to internationalise state power through the internet. Madison Cartwright explains that dominant private firms act as conduits through which states can exercise power: the 'prominent role of private interests in the geopolitics of communications is not novel to the internet. Past technological innovations (…) all involved heavy involvement with private firms which would work with states to "alter established international power relations."'[35]

Retaining tech superiority also entails setting the norms of how the internet and data should be governed. In the recent past, there was a large consensus among scholars that US allies' approach towards 'data sovereignty' was in line with that of the US. In 2014, Dana Polatin-Reuben and Joss Wright wrote that approaches towards 'data sovereignty,' which they defined as 'a catch-all term to describe different state behaviours towards data generated in or passing

[34] A.J. Jakobsson and M. S. Stolz. "Principled Big Tech: European pursuit of technological autonomy." *Finnish Institute of International Affairs* (2021). p.111
[35] Madison Cartwright, "Internationalising state power through the internet: Google, Huawei and geopolitical struggle." *Internet Policy Review* 9, no. 3 (2020): 1-18. p.3

through national internet infrastructure,'[36] can be summarised in the following way: the US and its allies view data localisation as 'a threat to a free and open global internet' whereas countries such as Russia, China and Brazil advocate 'for data sovereignty as a way of securing sensitive national data from foreign surveillance.'[37]

However, three significant events eroded the confidence of EU member states in US leadership and US companies in the technological realm. The first turning point was the release of documents in 2013 by a former National Security Agency (NSA) contractor, Edward Snowden, which provided evidence towards the agency's telephone metadata collection programme (code named PRISM). This programme entailed extensive US government surveillance of electronic communications, causing significant tension and 'political uproar'[38] between the US and the EU. European policymakers and citizens were concerned about the implications of the revelations for privacy and civil liberties, which led to the EU implementing measures aimed at strengthening data protection, including the General Data Protection (GDPR) and ePrivacy regulation. Henry Farrell and Abraham L. Newman, in 2019, wrote that 'American credibility as 'good stewards' has been so damaged by the Snowden revelations that even the EU is considering adopting a local cloud to ensure protection of its sensitive data.'[39]

The second turning point entails the *Schrems* decisions. In 2013, Austrian privacy activist Max Schrems filed a complaint with the Irish Data Protection Commissioner (DPC), arguing that Facebook's data transfers from the EU to the US violated EU privacy law due to the US government's access to the data through the PRISM surveillance programme.[40] The Irish DPC rejected the complaint, citing the adequacy of the Safe Harbor framework between the US and

[36] Polatin-Reuben and Wright, "An Internet with BRICS Characteristics" p.1
[37] *ibid.*
[38] Henry Farrell and Abraham L. Newman, "Weaponized interdependence: How global economic networks shape state coercion." *International Security* 44, no. 1 (2019): 42-79. p.73
[39] Farrell and Newman, "Weaponized interdependence" p.2
[40] Marc Rotenberg, "Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection." *European Law Journal* 26, no. 1-2 (2020): 141-152

the EU for data transfers. The Safe Harbor framework was developed between 1998 and 2000 to prevent private organisations in the EU or US which store customer data from disclosing or losing personal information. Max Schrems appealed to the Irish High Court, which referred the case to the European Court of Justice (ECJ) for a preliminary ruling. In October 2015, the ECJ issued its ruling in the *Schrems I* case, invalidating the Safe Harbor framework on the grounds that it did not provide adequate protection for the EU citizens' data considering US government surveillance practices.[41] The court found that the Safe Harbor framework did not provide sufficient safeguards against such access and that EU data protection authorities had the power to suspend or prohibit data transfers to the US. Commentators at the time described the outcome 'as an earthquake that tossed aside the fragile legal framework for transatlantic data flows.'[42] Marc Rotenberg, the founder and director of the Center for AI and Digital Policy in Washington, explained that the problems with Safe Harbor were well known before the Snowden revelations, however 'the Snowden revelations hit hard particularly with US allies in Europe, who believe that they stood on the same side of the intelligence-gathering enterprise.'[43] The US and the EU subsequently negotiated "Privacy Shield" which was 'an arrangement for transatlantic data flows very similar to the Safe Harbor arrangement.'[44]

In 2020, Max Schrems challenged the novel EU-US Privacy Shield arguing that it did not provide adequate protection for EU citizens' data given US government surveillance practices. The case was heard by the ECJ, which issued its ruling on July 16, 2020. In the *Schrems II* case, the ECJ invalidated the Privacy Shield framework, finding that it did not adequately protect EU citizens' data from access by US intelligence agencies. The court also raised concerns about the ability of EU citizens to seek legal remedies in the US for violations of their data protection rights. As Rotenberg explains, 'Privacy Shield toppled for many of the same

[41] Rotenberg, "Schrems II, from Snowden to China"
[42] *ibid.* p.141
[43] *ibid.* p.143
[44] *ibid.* p.145

reasons as did Safe Harbor.'[45] The *Schrems II* ruling has had significant implications for data transfers between the EU and the US, as well as other countries where data protection laws are not considered adequate. The ruling means that companies must evaluate their data transfer mechanisms to ensure they provide adequate protection for EU citizens' data. The ruling has also led to increased calls for a new data transfer framework between the EU and the US, as well as for the US to strengthen its data protection laws. Overall, following the Snowden revelations, what lied at the centre of the ECJ's *Schrems I* and *Schrems II* decisions was that 'Europeans became aware of the scope of NSA surveillance and the weakness of the self-regulatory approach to privacy protection became apparent: even companies with the best of intentions cannot safeguard data that is subject to government surveillance.'[46]

The third turning point in the relationship between the US and the EU in the tech sector was the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), a US law passed in 2018. One of its main provisions is that it allows US law enforcement agencies to access electronic data that is stored by US technology companies, even if the data is stored on servers located outside the US. The US CLOUD Act 'has clarified that US tech companies are subject to US laws no matter where in the world they are operating, or whose data they are storing. This means, for example, a US company storing EU data on EU soil would still be subject to access requests from the US Government.'[47] Indeed, Emily Wu explains that there are two critical elements to the CLOUD Act: firstly, it clarifies that service providers are required to disclose all data in their possession, custody, or control, pursuant to lawful process, regardless of the localisation of the data.[48] The second is that it makes it easier for foreign governments to

[45] Rotenberg, "Schrems II, from Snowden to China" p.148
[46] *ibid.* p.150
[47] Wu, "Sovereignty and Data Localisation" p.3
[48] *ibid.* p.3

request access to data stored by companies in the US.[49] Many European policymakers argued that the CLOUD Act significantly undermines privacy and civil liberties.

Following the Snowden revelations, the *Schrems* decisions and the CLOUD Act, the relationship between the US and the EU in the tech sector was severely weakened. It became clear that data of European citizens, companies and institutions were in the hands of American and Chinese technology corporations.[50] Emily Wu explains that 'foreign nations – both allies and adversaries – are anxious that the US' (and China's) dominance in emerging technologies will be a threat to their own assertion of data sovereignty,' and crucially, that 'concerns about a growing sense of "neocolonial" dependence on multinational tech companies is a motivating force behind much of the proliferation of new data protection and privacy policies globally.'[51]

Indeed, scholars have coined the term digital colonialism in describing how 'EU member states are increasingly dependent on digital infrastructures that are in the hands of a handful of dominant foreign market players.'[52] Moreover, when identifying the main drivers behind forced data localisation, Konstantinos Komaitis highlighted the 'shared view that the internet is an American enterprise. Be it Facebook, Google, Apple, or Uber, the largest companies holding users' data are predominantly American.'[53] Although this is not new, it has been steadily intensifying a sense of unease among certain states, and Komaitis sustains that Snowden proved that this unease is not unwarranted.[54]

The growing unease between the US and the EU, triggered by the Snowden revelations, the Schrems decisions, and the US CLOUD Act, provides a compelling context for understanding why EU member states are choosing to soft balance against US technological influence.

[49] Wu, "Sovereignty and Data Localisation" p.4
[50] Edoardo Celeste, "Digital sovereignty in the EU: challenges and future perspectives." *Data protection beyond borders: Transatlantic perspectives on extraterritoriality and sovereignty* (2021): 211-228 p.16
[51] Wu, "Sovereignty and Data Localisation" p.5
[52] Moerel, "The Ebb and Flow of Trans-Atlantic Data Transfers"
[53] Komaitis, "The 'wicked problem'of data localisation." p.359
[54] *ibid.*

However, the existing literature does not explain why European states are still pursuing data localisation policies, despite other privacy-protecting ways to address the falling out with the US that would be less costly. These other ways include increased cooperation with other allies, investment in domestic research and development, and diplomatic engagement with the US. In addition, the literature does not explain the variation in data localisation policies across different EU member states. This variation suggests there is no single, unified European approach to data localisation. As I will show in the case study section, some member states, such as Germany and France, have adopted more restrictive data localisation policies, whilst others, such as Ireland and the Netherlands, have adopted more liberal policies.[55]

3.3. Theory and Methods: Data Localisation as Soft Balancing

In this section, I develop the theoretical framework for understanding data localisation policies as a form of soft balancing against the US. I argue that data localisation policies are strategic responses by US allies to counterbalance US hegemony in the digital realm. First, I define the concept of soft balancing and contextualise its relevance to the US European allies. Second, I develop the theoretical framework for this article. Finally, I delineate methods.

3.3.1. Soft Balancing

Soft balancing, as defined by T.V. Paul, refers to the conscious strategy adopted by weaker states to limit the power and influence of a stronger state through tacit balancing short of formal alliances, often through ententes or limited security understandings.[56] This strategy involves using non-military tools to delay, frustrate, and undermine the aggressive unilateral policies of

[55] Laura Kabelka, "Sovereignty requirements remain in cloud certification scheme despite backlash" *EURACTIV* (16 June 2022) <https://www.euractiv.com/section/cybersecurity/news/sovereignty-requirements-remain-in-cloud-certification-scheme-despite-backlash/> (accessed 12/04/23)
[56] Thazha V. Paul, "Soft balancing in the age of US primacy." *International security* 30, no. 1 (2005): 46-71. p.47

a more powerful state.[57] Furthermore, Paul highlights that second-tier major powers and emerging powers refrain from traditional hard balancing through alliances or arms build-ups, opting for soft balancing instead.[58] Soft balancing is connected to balance-of-power theory, as it involves conscious coordination of diplomatic friction to achieve outcomes contrary to the preferences of the stronger state.[59]

Overall, soft balancing is a conscious strategy that involves non-military tools such as diplomatic and economic initiatives to limit the power and influence of stronger state. This concept is distinct from traditional hard balancing and is deeply rooted in the dynamics of international relations. Data localisation policies can be considered a soft balancing tool as they are indirect and non-confrontational. They aim to limit the power and influence of the stronger state without directly challenging it. Hard balancing, on the other hand, involves direct and confrontational measures, such as military alliances or arms build-ups.

Another concept which can be considered relevant to data localisation policies is hedging, which focuses on states' strategic flexibility in uncertain environments.[60] Unlike soft balancing which targets specific actors, hedging involves states pursuing a mix of cooperative and competitive actions to navigate power dynamics.[61] It is primarily opportunistic, driven by risk management, and does not require states to necessarily commit to a specific stance. In this paper, I argue that data localisation policies represent soft balancing rather than hedging, as these policies enact regulations to safeguard states' interests from perceived dominance in the digital sphere, specifically against powerful actors. This targeted approach aims to reshape digital power dynamics, aligning with the strategic and conscious nature of soft balancing.

---

[57] Robert A. Pape, "Soft balancing against the United States." *International security* 30, no. 1 (2005): 7-45. P.7
[58] Paul, "Soft balancing in the age of US primacy." p.47
[59] Laura Levick and Carsten-Andreas Schulz, "Soft balancing, binding or bandwagoning? Understanding institutional responses to power disparities in the Americas." *Canadian Journal of Political Science/Revue canadienne de science politique* 53, no. 3 (2020): 521-539. p.524
[60] Nicholas Ross Smith, "When hedging goes wrong: Lessons from Ukraine's failed hedge of the EU and Russia." *Global policy* 11, no. 5 (2020): 588-597. p.589
[61] *ibid.*

Indeed, the EU historically serves as a case study of soft balancing. Franz Oswald identifies the EU as 'the most successful soft balancer of US supremacy.'[62] This point is exemplified by what Anu Bradford calls the 'Brussels Effect,'[63] whereby the EU sets global standards via its laws and regulations, including data protection norms through the General Data Protection Regulation (GDPR). This positions the EU as a dominant force in global digital regulation, reducing the influence of other actors, even if such balancing is not the explicit intention. However, data localisation policies cannot be simply classified under the Brussels Effect. Whilst both involve asserting regulatory control, data localisation policies present unique challenges and implications. They carry substantial economic costs and are far more contentious, as evidenced by the different approaches to implementation among EU member states. In this paper, I suggest that the motivation behind these policies goes beyond norm-setting behaviour, arguing that they are strategic moves aimed at reshaping the power dynamics in the digital realm. This reframed understanding of data localisation not as a side-effect, but as a purposeful and conscious strategy of soft balancing, forms the premise for my paper's investigation into the rise of these policies within the European Union.

3.3.2. Theory

Data localisation policies, despite their negative economic effects and security inefficiencies, have gained traction among the US European allies. Understanding their rise in popularity requires an examination of the motivations behind their adoption. The philosophical premise for localising data 'varies and depends greatly on cultural and political contexts.'[64] However, regardless of the differences in stated reasons, the effect of data localisation policies

[62] Oswald, "Soft balancing between friends," p.146
[63] Anu Bradford, *The Brussels effect: How the European Union rules the world*. Oxford University Press, USA, 2020.
[64] Komaitis, "The 'wicked problem' of data localisation," p.357

is consistent – it offers states increased control over data that extends across their borders and reduces their dependence on the US.

I hypothesise that data localisation policies adopted by US allies in Europe are not mere regulatory adjustments or solely aimed at enhancing cybersecurity. Instead, they are strategic responses reflecting political resolve to soft balance against the US, which involves employing non-military strategies to counterbalance a dominant power. I hypothesise that three state motivations link data localisation policies as tools for soft balancing as a conscious strategy: (1) reducing dependence on US tech companies for critical digital infrastructure, (2) limiting the US ability to use data as a means of exerting influence over its allies, and (3) promoting domestic industry and economic growth, therefore enhancing the relative power of US allies vis-à-vis the US. If these three motivations can be found to explain a policy's implementation, I identify the policy as consistent with soft balancing behaviour. It is crucial to clarify here that these motivations do not imply outright hostility or opposition towards US tech companies. Rather, they represent a strategic endeavour to balance the power dynamics in the digital realm.

The first question that naturally emerges is whether policymakers adopt data localisation policies with the explicit goal of soft balancing, or whether the effect of soft balancing is an incidental outcome. Whilst some might argue that soft balancing could be an unintended effect, the alignment of the motivations behind data localisation policies with the principles of soft balancing provides evidence towards an intentional strategy. Policymakers would not explicitly label their efforts as 'soft balancing,' but the strategic choices and objectives indicate a calculated approach to counterbalance the hegemony of US tech firms. Therefore, the central aim of this paper is to argue that data localisation policies, such as the EUCS, are deliberate attempts at soft balancing, regardless of whether policymakers are explicitly aware of this effect. This forms the premise for the case study that follows, which will further delve into the

motivations behind these policies and analyse whether they align with the principles of soft balancing.

Whilst this paper argues that EU member states' adoption of data localisation policies is a form of soft balancing against US technological dominance, it is crucial to consider an alternative explanation for these policies' adoption: that policymakers fail to fully grasp the technical complexities of data localisation policies, leading to potential oversights in policy design. If European policymakers did not understand the magnitude of the economic costs and security risks, it is possible that they would believe that these policies served their interests sufficiently for there to be no puzzle – data localisation measures would serve the interests of their states without the need for soft balancing to be a motivation. However, evidence suggests otherwise. The stark division in opinions among European member states on data localisation suggests that policymakers are having comprehensive, informed discussions about the pros and cons of the policy. Informed debates make misunderstandings unlikely to be a driving cause for adoption of any policy in the EU and suggests instead that European states are deliberately using data localisation as a costly tool for soft balancing; the perceived gains in sovereignty outweigh the costs. Essentially, policymakers understand the costs and risks, and deem them a necessary sacrifice in pursuit of their soft-balancing objectives.

3.3.3. Methods

To test my soft balancing hypothesis, I draw on the case of the European Cybersecurity Certification Scheme for Cloud Services (EUCS). The European Commission released the first draft of the EUCS in June 2019, followed by a second draft in February 2020, and the final version in January 2021. Although it is not fully operational at the time of writing this paper, it offers valuable insights into the motivations behind data localisation policies. By scrutinising the EUCS, I aim to identify evidence linking its justifications to the three hypothesised soft

balancing aims: (1) reducing dependence on US tech companies for critical digital infrastructure, (2) limiting the US ability to use data as a means of exerting influence over its allies, and (3) promoting domestic industry and economic growth, therefore enhancing the relative power of US allies vis-à-vis the US.

In the case study, I employ within-case process tracing,[65] gathering Causal Process Observations (CPOs) and applying process tracing tests to evaluate the strength of the evidence. Data sources included primary data from semi-structured elite interviews and secondary sources encompassing newspaper articles, policy documents, company documents, policymakers' and company representatives' statements and speeches, open-source intelligence reports and other forms of institutional documents. I faced challenges in data collection due to the topic's contemporary nature and accessing key interviewees, political elite and tech industry representatives. I addressed this limitation by focusing on in-depth interviews with high-level tech industry representatives to obtain unique insights into their experiences with policymakers on the topic of data localisation policies, rather than gathering broad opinions, which are readily available from public sources. For this paper, I conducted two in-depth anonymous background interviews with senior US tech industry representatives.[66] These interviews were strictly anonymous and used to provide context; no direct information or quotes are attributed in the case study. The interviews were nonetheless crucial for this paper and supplemented by a thorough analysis of secondary sources, which I carefully analysed as public sources, acknowledging that they may be biased and not necessarily revelatory of decision-makers' personal thoughts.

The investigation into the EUCS will proceed in five sections. First, I provide a brief overview of data localisation policies in the EU. Second, I explain what the EUCS is and how

[65] Andrew Bennett and Jeffrey T. Checkel, eds. *Process tracing*. Cambridge University Press, 2015. p.5
[66] Ethical approval of research involving human participants was granted (Central University Research Ethics Committee Approval Reference: SSH_DPIR_C1A_21_053)

it constitutes a form of data localisation. In the third section I analyse the official justifications for the EUCS, identifying evidence of the soft balancing aims outlined above. In the fourth section, I delve into the criticisms and divisions that the EUCS has sparked among experts, industry associations, and EU member states, seeking to uncover potential hidden motivations. Lastly, I present the evidence supporting the alternative explanation mentioned above, allowing for a balanced and thorough assessment of the theory of data localisation as a form of soft balancing.

3.4. Case Study: The European Cybersecurity Certification Scheme for Cloud Services (EUCS)

3.4.1. Overview of Data Localisation Policies in the EU

In this section, I summarise the key developments of the EU's data localisation policies at the supranational level. The first is the General Data Protection Regulation (GDPR), which governs the processing and transfer of personal data within the EU.[67] It requires that personal data be stored and processed within the EU, unless the data subject has explicitly consented to the transfer, or the transfer is necessary for a specific purpose. The second is the Cloud Security Certification (EUCS), a certification programme for cloud service providers that are based in the EU or offer services within the EU to assess their protection measures, which I elaborate on in the next section. The third is E-Privacy Regulation, which encompasses a proposal that imposes additional data localisation requirements on providers of electronic communication services, such as messaging apps and email providers. Under this regulation, providers would

[67] European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)." *Official Journal of the European Union*, vol. 59, no. 1, 4 May 2016, pp.1-88.

be required to store metadata, such as information about the origin and destination of messages, within the EU.

Although policies apply uniformly across all member states, member states are responsible for enforcing the EU's data protection regulations within their own territories. Nevertheless, the EU has a number of mechanisms in place to ensure such enforcement, such as the European Data Protection Board (EDPB) which provides guidance and promotes the consistent application of data protection rules across the EU. The next sections focus specifically on the EUCS.

3.4.2. EUCS: Overview

Cloud infrastructure encompasses the underlying physical and virtual resources that support the delivery of cloud computing services, including data centres, servers, storage devices, networking equipment and software. Cloud infrastructure is a salient topic for European policymakers as with technological development, especially in the realm of Artificial Intelligence, 'you need large quantities of harmonised data and computing power to process these data.'[68] To foster innovation, the data of companies in a specific sector will have to be increasingly combined, but 'this is currently difficult as companies' data are stored in silos in the clouds of foreign tech providers.'[69] The EU is mainly dependent on digital infrastructures owned by a number of major foreign market players, as '92% of European data resides in the clouds of US technology companies, of which 80% are with only five suppliers.'[70]

The EUCS is a proposal for a new certification framework for cloud service providers (CSPs) operating in the EU. It was created under the Cybersecurity Act, whose aim was 'to improve cybersecurity across a wide range of digital products, services and processes,' and

[68] Moerel, "The Ebb and Flow of Trans-Atlantic Data Transfers"
[69] *ibid.*
[70] *ibid.*

establish 'a unified approach to cybersecurity certification in the European internal market.'[71] The proposed framework is known as the European Cybersecurity Certification Scheme for Cloud Services (EUCS),[72] and it aims to establish a common set of cybersecurity standards and procedures that CSPs must meet in order to receive certification. The EUCS was developed by the European Union Agency for Cybersecurity (ENISA) in collaboration with other EU institutions, and it is part of a broader effort by the EU to increase cybersecurity and data protection for businesses and consumers. Under the EUCS, CSPs would be subject to a series of rigorous cybersecurity requirements, including regular security assessments and audits, incident reporting procedures, and data protection measures. CSPs that meet these requirements would be awarded a certification that would be recognised across the EU, providing a clear indication of their cybersecurity capabilities and enhancing consumer trust. The certification has three assurance levels, corresponding to levels 'basic', 'substantial' and 'high.'[73] The EUCS is currently in the draft stage, and it is subject to review and feedback from stakeholders before it is finalised and implemented.

Although some argue that EUCS does not qualify as data localisation, under the EUCS proposal being developed, 'cloud service providers would be compelled to localise their operations and infrastructure within the EU and to demonstrate their "immunity" from foreign law.'[74] In other words, it includes sovereignty requirements that would make it 'impossible for non-European companies to be awarded the certificate. The cloud service provider would have to be headquartered in Europe, not be controlled by any non-EU entity and completely

[71] Dutch Authority for Digital Infrastructure, "Cloud Certification" <https://www.dutchncca.nl/certification-schemes/cloud-certification> (accessed 14/03/23)
[72] European Union Agency for Cybersecurity (ENISA), "EUCS – Cloud Services Scheme" (December 2020) <https://ec.europa.eu/newsroom/cipr/items/713799/en> (accessed 25/02/23)
[73] *ibid.*
[74] Kenneth Propp, "European Cybersecurity Regulation Takes a Sovereign Turn" *European Law Blog* (12 September 2022) <https://europeanlawblog.eu/2022/09/12/european-cybersecurity-regulation-takes-a-sovereign-turn/> (accessed 11/04/23)

independent from non-EU laws.'[75] It may not be considered data localisation as the scheme and certification per se is not mandatory for CSPs, however, 'its level of assurance "high" might become mandatory for sectors like energy operators and banks, deemed highly critical under the recently revised Networks and Information System Directive (NIS2).'[76] Therefore, I believe that EUCS provides sufficient data localisation measures to be relevant for analysis.

The implementation of EUCS could bring several economic downsides. First, EUCS could reduce competition among CSPs, potentially leading to higher prices and reduced innovation. Second, EUCS could be perceived as protectionist and exclusionary, discouraging foreign investment in the EU's cloud computing sector. Third, the cost of developing a European cloud infrastructure could be substantial, possibly making EUCS less competitive with other CSPs. Lastly, there is a concern that EUCS might struggle to keep pace with technological advances and changing market conditions, potentially reducing its competitiveness and attractiveness to users.

In the following sections, I present the official justifications for EUCS, the criticisms and divisions it has sparked, and the potential evidence supporting alternative explanations for its development. By examining these factors, we gain a more nuanced understanding of whether the implementation of data localisation policies like EUCS represents an intentional strategy of soft balancing against US tech dominance.

3.4.3. EUCS: Official Motivations

The three motivations that I hypothesised link data localisation policies to soft balancing behaviour are: (1) reducing dependence on US tech companies for critical digital infrastructure,

[75] Luca Bertuzzi, "Is data localisation coming to Europe?" *International Association of Privacy Professionals* (23 August 2022) <https://iapp.org/news/a/is-data-localization-coming-to-europe/> (accessed 11/03/23)
[76] Luca Bertuzzi, "EU countries seek way out of impasse on sovereignty requirements for cloud services" *EURACTIV* (30 January 2023) <https://www.euractiv.com/section/cybersecurity/news/eu-countries-seek-way-out-of-impasse-on-sovereignty-requirements-for-cloud-services/> (accessed 08/03/23)

(2) limiting the US ability to use data as a means of exerting influence over its allies, and (3) promoting domestic industry and economic growth, therefore enhancing the relative power of US allies vis-à-vis the US. In this section, I provide evidence that European policymakers have referenced all three motivations when justifying the need for EUCS.

In reference to the specific sovereignty requirements in the EUCS, the draft document reads: 'the objective of these specific requirements is to adequately prevent and limit possible interference from states outside of the EU with the operation of certified cloud services.'[77] This provides evidence for (1) the aim to reduce dependence on foreign, rather than specifically US, tech companies, and (2) the aim of undermining the ability of the foreign states to use data as a means of exerting influence over its allies. Indeed, EUCS is seen as 'another way to safeguard Europe's "sovereign" interest in protecting data from foreign government access.'[78] Official justifications and motivations for EUCS are unlikely to single out the US as a target, therefore more evidence is required.

Moreover, EUCS aims to 'reinforce separate European efforts to bolster smaller, home-grown cloud service providers.'[79] Stemming from EUCS, EU Member States have launched projects directly aimed at (3) promoting domestic industry and economic growth. The most significant of these initiatives is Gaia-X, a European project that aims to create a secure and federated data infrastructure for Europe to enable secure, decentralised, and interoperable data sharing across different sectors and industries. Gaia-X was initiated by Germany and France and is explicitly based on 'principles of *sovereignty-by-design.*'[80] When German Economy Minister Peter Altmaier and French Economy Minister Bruno Le Maire championed the project, Le Maire stated: 'We are not China, we are not the United States – we are European countries with our own values and our own European interests that we want to defend. The

[77] Kabelka, "Sovereignty requirements remain in cloud certification scheme despite backlash"
[78] Propp, "European Cybersecurity Regulation Takes a Sovereign Turn"
[79] *ibid.*
[80] Moerel, "The Ebb and Flow of Trans-Atlantic Data Transfers"

COVID crisis has shown that giant tech companies are winners of the crisis.'[81] Although both China and the US are both mentioned, Gaia-X is a clear attempt to undermine the supremacy of US dominant players like Amazon and Google, rather than Chinese companies. This can be understood from the fact that Amazon, Microsoft and Google's cloud services account for 69 percent of the market in Europe.[82] As a response to the slow development of Gaia-X, a group of European software and hardware firms launched an association called Euclidia, 'for Europe to become a global leader without following the American or Asian models in cutting edge cloud technology.'[83] This once again provides evidence towards the motivations behind all these projects, which is to target tech giants. In addition, the European Commission has steadily been developing legislative initiatives such as the Digital Markets Act and the Data Act, aimed at giving European challengers a 'fighting chance to regain market share' and 'set new rules to better protect European data from foreign governments' reach.'[84]

France launched the line of thinking which led to the drafting of the EUCS. In order to discern the motivations behind EUCS, it is useful to understand the initial French approach. In 2016, France's Information Security Systems Agency (ANSSI) launched a certification and labelling programme known as SecNumCloud to 'establish minimum levels of security for French public entities procuring cloud services to host data and information systems.'[85] Essentially, it is a label to show public agencies and firms in critical sectors which cloud services can be trusted. At the time, it was criticised as 'explicit protectionism against non-French cloud service providers.'[86] In 2021, the French government issued the 'Trusted Cloud

[81] Janosch Delcker and Melissa Heikkila, "Germany, France launch Gaia-X platform in bid for 'tech sovereignty.'" *Politico* (4 June 2020) <https://www.politico.eu/article/germany-france-gaia-x-cloud-platform-eu-tech-sovereignty/> (accessed 09/03/23)
[82] Clothilde Goujard and Laurens Cerulus, "Inside GAIA-X: How chaos and infighting are killing Europe's grand cloud project" *Politico* (26 October 2021) <https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/> (accessed 01/04/23)
[83] *ibid.*
[84] *ibid.*
[85] Kenneth Propp, "European Cybersecurity Regulation Takes a Sovereign Turn"
[86] Nigel Cory, "Sovereignty Requirements in French – and potentially EU-Cybersecurity regulations: The latest barrier to data flows, digital trade, and digital cooperation among likeminded partners" *Information Technology*

Doctrine' making SecNumCloud certification mandatory whenever a French government agency procures cloud services that would handle sensitive data and for private operators of essential services. The latest SecNumCloud revisions, enacted in March 2022, retain broad data localisation requirements for all data (both personal and non-personal) and foreign ownership and board limits, which 'effectively force foreign firms to set up a local joint venture to be certified under SecNumCloud as "trusted" and thus able to manage European data and digital services.'[87] In other words, foreign cloud companies are forced to 'enter into joint ventures with French providers in which the foreign participant owns a minority or non-controlling interest, or else to license their technologies to a certified local vendor.'[88] Given that France is leading efforts to embed SecNumCloud's sovereignty requirements in EUCS, it is clear that a fundamental aim of EUCS is to undermine the influence of existing tech giants.

3.4.4. EUCS: Criticisms and Divisions

Experts have heavily criticised the EU's Draft Cloud Security Scheme. The criticisms began with France's SecNumCloud certification programme from which the Cloud Security Scheme stemmed from. Experts argued that SecNumCloud's sovereignty requirements 'breach both France and the EU's commitments under the World Trade Organisations General Agreement on Trade in Services (GATS).'[89] As the latest version of SecNumCloud explicitly requires suppliers of cloud computing services to store and process their customers' data within the EU, it 'effectively constitutes a ban on the cross-border supply of these services.'[90] The US

and Innovation Foundation (10 December 2021) <https://itif.org/publications/2021/12/10/sovereignty-requirements-france-and-potentially-eu-cybersecurity/> (accessed 11/04/23)

[87] Nigel Cory, "France's "Sovereignty Requirements" for Cybersecurity Services Violate WTO Trade Law and Undermine Transatlantic Digital Trade and Cybersecurity Cooperation" (10 May 2022) <https://itif.org/publications/2022/05/10/france-sovereignty-requirements-cybersecurity-services-violate-wto-trade/#> (accessed 20/04/23)

[88] Propp, "European Cybersecurity Regulation Takes a Sovereign Turn"

[89] Cory, "France's "Sovereignty Requirements" for Cybersecurity Services Violate WTO Trade Law and Undermine Transatlantic Digital Trade and Cybersecurity Cooperation"

[90] *ibid.*

'raised concerns directly with the French government, which seems unperturbed.'[91] Evidence of tension specifically with the US supports my theorisation of soft balancing.

Moving onto EUCS specifically, experts have argued that 'ENISA is running an opaque process without broad and open stakeholder engagement.'[92] The ITIF claimed that EUCS 'follows China's approach in making local firm ownership and control – rather than the use of best-in-class cybersecurity practices – the defining factors in ascertaining whether a cloud service provider can be deemed "trusted" and allowed to operate in the local market.'[93] The comparison to China's approach emphasises the divide that EUCS is creating between the US and its allies. In the same report, ITIF accused France of not wanting American cloud firms yet of expecting 'all the cybersecurity assistance it can get from the US government and those same US cloud firms.'[94] They frame the EUCS as an explicit 'attack' on US tech firms.[95] Moreover, ITIF researchers explain that the specific form of data localisation suggested in the EUCS prevents the sharing of cybersecurity-related information, prevents local organisations from accessing cybersecurity services, and 'undermines 13 of the 14 controls in one of the main international standards for information and cybersecurity.'[96] Sovereignty requirements would 'make it harder, if not impossible, for US firms to take preventative action to protect European customers and cybersecurity agencies in the run-up to a cyberattack,' as well as precluding 'transatlantic and global cybersecurity cooperation before it even starts.'[97] This evidence points towards the lack of benefits that EUCS may provide to EU member states, rendering clear the political nature of the document. The report ends with the question, 'if Europe does not trust

[91] Cory, "France's "Sovereignty Requirements" for Cybersecurity Services Violate WTO Trade Law and Undermine Transatlantic Digital Trade and Cybersecurity Cooperation"
[92] *ibid.*
[93] Nigel Cory, "Europe's Cloud Security Regime Should Focus on Technology, Not Nationality" *Information Technology and Innovation Foundation* (27 March 2023) <https://itif.org/publications/2023/03/27/europes-cloud-security-regime-should-focus-on-technology-not-nationality/> (accessed 12/04/23)
[94] *ibid.*
[95] *ibid.*
[96] *ibid.*
[97] *ibid.*

US cloud firms at home, how can they make the case to governments in third-country markets to trust them?'[98] Once again, the direct targeting of US tech firms is emphasised.

Moreover, ENISA has been criticised by US and European firms and industry associations, as well as some EU Member States, for lacking transparency and stakeholder engagement: 'while there are several bodies, such as the European Cybersecurity Certification Group, the Stakeholder Cybersecurity Certification Group, and various ad hoc groups of experts that are supposed to advise ENISA on the framework and its technical standards, in practice, these outside stakeholders are relegated, never really consulted, and largely ignored.'[99] A statement signed by the tech industry representatives of four organisations[100] released in June 2022, explicitly states: 'the proposed digital sovereignty requirements, regardless of the assurance level for which they are aimed at, are purely politically motivated, will create complex legal compliance and will not add to increased levels of cybersecurity,' adding that the EUCS 'should not be compromised by considerations that are political in nature.'[101] A spokesperson for Digital Europe argued that EUCS 'will hurt cloud service providers directly and will mean, more broadly, that the European economy will lose choice and quality in cloud offerings.'[102] He elaborated that 'we have been particularly puzzled by how proposals for these requirements have been introduced. The process has been driven by individual players and member states, with industry stakeholders and other member states left in the dark and now being asked to accept a new version of the scheme as *fait accompli.*'[103] This provides strong evidence towards the political nature of EUCS in its intent to target US tech firms without any real, concrete benefits for EU member states.

---

[98] Cory, "Europe's Cloud Security Regime Should Focus on Technology, Not Nationality"
[99] *ibid.*
[100] American Chamber of Commerce to the European Union (AmCham EU), BSA Software Alliance, Computer and Communications Industry Association (CCIA Europe) and Information Technology Industry Council (ITI)
[101] AmCham EU, BSA, CCIA Europe, ITI. "European Cybersecurity Certification Scheme for Cloud Services" (14 June 2022) <https://www.itic.org/documents/europe/Final_EUCS_statement_1406.pdf> (accessed 11/04/23)
[102] Kabelka, "Sovereignty requirements remain in cloud certification scheme despite backlash"
[103] *ibid.*

The European Centre for International Political Economy (ECIPE) further 'underscores growing private concerns about the draft label plan among US tech giants, which have so far not made any public comment on it.'[104] ECIPE elaborated that the proposed EUCS 'could set a dangerous precedent for any data-intensive sector, that could see the cybersecurity label become mandatory for new technologies.'[105] The ECIPE Director Matthias Bauer stated 'I think the political intention is to squeeze out foreign suppliers but it will of course have also ramifications for EU businesses that are more or less relying on cloud computing services.'[106] Although this does not specifically reference the US as a foreign supplier, it can be deduced by the aforementioned market share that US tech giants hold in the EU. He added that 'member states should now call on the cybersecurity agency and also the European Commission to abandon politically motivated EUCS immunity requirements.'[107] Moreover, Alexandre Roure, Europe's Director of Public Policy for the trade association CCIA, claimed that 'these requirements have nothing to do with cybersecurity concerns, some may even argue this is a protectionist approach pushed by certain national governments.'[108]

ENISA's EUCS also caused numerous divisions among member states. A specific group of member states, referred to as the D9+ and which include Belgium, Denmark, Estonia, Finland, Ireland, Luxembourg, Netherlands, Poland, Portugal, Spain, the Czech Republic and Sweden raised specific concerns. The Netherlands, Sweden and Ireland released a non-paper in April 2022, arguing that 'the proposed requirements on sovereignty in the cloud scheme could have wide-ranging effects for companies (sub-contractors) involved in cloud service deliveries and their ability to develop their services and compete on the global market.'[109] They

[104] Foo Yun Chee, "Tech-sponsored study criticises plan to exclude non-EU cloud vendors" *Reuters* (6 March 2023) <https://www.reuters.com/technology/tech-sponsored-study-criticises-plan-exclude-non-eu-cloud-vendors-2023-03-06/> (accessed 12/04/23)
[105] *ibid.*
[106] *ibid.*
[107] *ibid.*
[108] Kabelka, "Sovereignty requirements remain in cloud certification scheme despite backlash"
[109] *ibid.*

recommend to develop 'more generic legislation at the EU level such as the Data Act, rather than imposing technical security requirements in a cloud scheme.'[110] They specifically refer to the potential economic downsides, stating that 'the consequences of proposed sovereignty requirements should be studied carefully by relevant experts.'[111] Moreover, they urged that 'fragmentation of the European market must be prevented,'[112] and finally that although 'in specific circumstances (e.g., in the area of national security) localisation requirements can be justified, such requirements should be supported by solid safeguards.'[113] The divisions among member states show that the costs of data localisation policies are being considered by policymakers, and that there are genuine concerns about EUCS' nature, intent and consequences.

3.4.5. Alternative Explanation: Misunderstandings

There is some evidence that European policymakers genuinely believe in the benefits of EUCS without the intent of targeting US tech companies, due to the lack of technical understanding. The ITIF reported that 'some European officials have justified EUCS sovereignty requirements, in part because they mistakenly think they are like provisions in FedRAMP – which is false.'[114] FedRAMP refers to the US Federal Risk and Authorisation Management Programme, and the report explains that FedRAMP in the US differs from SecNumCloud and EUCS sovereignty requirements in three key ways: it does not discriminate according to foreign ownership of firms, it only applies to cloud services used by US federal government agencies rather than the broader market, and finally it adheres to technical

[110] Cory, "France's "Sovereignty Requirements" for Cybersecurity Services Violate WTO Trade Law and Undermine Transatlantic Digital Trade and Cybersecurity Cooperation"
[111] *ibid.*
[112] *ibid.*
[113] *ibid.*
[114] Cory, "Europe's Cloud Security Regime Should Focus on Technology, Not Nationality"

cybersecurity standards in an open and transparent manner.[115] This is evidence which points towards policymakers misunderstanding the nature of EUCS and the consequences it may have. However, it is not sufficient evidence to invalidate my primary hypothesis. In addition, despite the foundation's claims, it continues to hold European policymakers accountable by recommending that 'if Europe fails to remove these restrictions, the US should re-evaluate cybersecurity cooperation and information sharing with the EU and its member states and develop and initiate retaliatory measures.'[116]

3.4.6. Discussion

In my analysis, I presented substantial evidence that the EUCS represents a strategic effort to soft balance against the US. First, the EUCS's sovereignty requirements are clearly aimed at reducing the EU's dependence on non-European CSPs, which are predominantly US-based. The EUCS' clauses on 'digital sovereignty' are aimed at protecting the EU from being subject to foreign laws, especially the US CLOUD Act. This aligns with the first hypothesised motivation for soft balancing: reducing dependence on US tech companies for critical digital infrastructure.

Second, the EUCS's emphasis on European cybersecurity and data protection can be understood as an EU measure designed to undermine the extensive data surveillance capabilities of US intelligence agencies. By requiring CSPs to comply with EU data protection laws and not be subject to foreign jurisdictions, the EUCS challenges US influence in data governance. This is further substantiated by concerns raised by groups such as the European Centre for International Political Economy (ECIPE), who warn that the EUCS could set a 'dangerous precedent'[117] and could be perceived as politically motivated to 'squeeze out

[115] Cory, "Europe's Cloud Security Regime Should Focus on Technology, Not Nationality"
[116] *ibid.*
[117] Chee, "Tech-sponsored study criticises plan to exclude non-EU cloud vendors"

foreign suppliers,'[118] which are primarily US-based ones. This aligns with the second hypothesised motivation for soft balancing: limiting the US' ability to use data as a means of exerting influence over its allies.

Finally, the EUCS seeks to promote domestic cloud industry capabilities to directly compete with the US tech sector, as further reinforced by initiatives such as Gaia-X. By establishing a certification scheme that advantages European CSPs, the EUCS could help EU businesses compete with non-European tech giants and foster innovation within the EU. Criticisms from organisations such as Digital Europe, which claim that the EUCS could hurt CSPs and limit choice, corroborate the idea that this approach might be tailored against dominant US firms. This aligns with the third hypothesised motivation for soft balancing: promoting domestic industry and economic growth, therefore enhancing the relative power of US allies vis-à-vis the US.

Whilst the EUCS does not explicitly enforce data localisation, its sovereignty clauses could lead to a de facto form of localisation by making European CSPs more appealing, to say the least, for local businesses. A group of member states known as the D9+ has already expressed concerns over this, specifically mentioning the potential economic downsides and market fragmentation that could undermine the EU companies' competitiveness globally.

3.5. Conclusion

Throughout this paper, I answered the question of why US allies are choosing to adopt data localisation policies despite their evident economic drawbacks and security inefficiencies. I argued that data localisation policies are strategic responses reflecting political resolve to soft balance against the US, which involves employing non-military tools to counterbalance a

[118] Chee, "Tech-sponsored study criticises plan to exclude non-EU cloud vendors"

dominant power. Through the case study of the EUCS, I presented substantial evidence of the presence of the three motivations that I hypothesised link data localisation policies to soft balancing behaviour: (1) reducing dependence on US tech companies for critical digital infrastructure, (2) limiting the US ability to use data as a means of exerting influence over its allies, and (3) promoting domestic industry and economic growth, therefore enhancing the relative power of US allies vis-à-vis the US. My findings indicate that policymakers understand the costs and risks of data localisation policies and deem them a necessary sacrifice in pursuit of their soft-balancing objectives.

The implications of my findings are three-fold. For the US, my findings on the reasons for the European shift towards data localisation underscores the necessity of reassessing its alliance management strategies. I provided evidence of a strong resolve by European policymakers to soft balance against US technological dominance. Therefore, rather than forcing allies into a 'with us or against us'[119] choice, the US seeking collaborative paths may prove more beneficial to maintain the Western edge in technology whilst respecting the sovereign interests of its European allies. Losing allies' support can have significant consequences on the US standing in the tech war, potentially leading to disruptions in supply chains, reduced market access for US tech companies, weakened cybersecurity cooperation and negative economic repercussions for the US economy.

For European policymakers, my findings call for an approach to data localisation with more technical understanding. The findings highlight that the costs, both economic and political, of certain data localisation measures may significantly outweigh the perceived benefits. European policymakers may perceive the benefits of balancing against US tech dominance as outweighing the costs. Such a perspective considers the protection of privacy through data

[119] Tim Stevens, "Huawei and UK foreign policy" *UK in a Changing Europe* (21 July 2020) <https://ukandeu.ac.uk/huawei-and-uk-foreign-policy/> (accessed 01/09/20)

localisation a worthy trade-off despite its economic implications. However, this approach is not without its own set of costs and risks, which become clear through the stark division in opinions among EU member states. European policymakers need to weigh domestic interests and alliance dynamics against the broader impacts of their decisions on the global digital economy, ensuring a balanced approach that respects both sovereignty and economic considerations.

For IR literature, this paper introduced the idea of data localisation policies as a form of soft balancing, challenging traditional understandings of alliance dynamics in the US-China competition context. Understanding data localisation policies as soft balancing provides a number of analytical gains. First, it allows us to see the broader geopolitical context in which these policies are adopted. Data localisation policies are not simply about protecting data sovereignty or cybersecurity. They are also about states seeking to position themselves in a changing global order, in which the US and China are competing for dominance in technology. Second, understanding data localisation as soft balancing helps us understand the motivations of states that adopt them. These states are not simply trying to maximise data sovereignty, therefore other political motivations must be considered. Third, understanding data localisation as soft balancing allows us to identify the potential consequences of these policies for IR, as they can cause shifts in alliance dynamics and a departure from the traditional belief that data localisation policies would primarily be adopted by authoritarian states.[120]

In conclusion, in this paper, I argued that data localisation policies adopted by US allies in Europe are strategic responses reflecting political resolve to soft balance against the US. This reframed understanding of data localisation as a form of soft balancing provides new insights for understanding the evolving motivations of states in the context of US-China tech war.

[120] Polatin-Reuben and Wright. "An Internet with BRICS Characteristics" p.1

4. My Way or the Huawei: US Influence on China's Involvement in the UK's Critical National Infrastructure

Thesis Paper 2

Abstract

This article investigates the extent to which the United States can influence the United Kingdom's decision-making about Chinese technology companies' involvement in its domestic critical national infrastructures (CNI). The UK's policy reversal from accepting Huawei's involvement in its 5G networks in January 2020 to banning it in July provides a deviant case study, representing a case that goes against the UK's previous policy of warmly accepting Chinese investments across different sectors of its CNI. Using within-case process tracing, I argue that US influence was a necessary but not sufficient condition for the UK's policy reversal. The effectiveness of US influence was contingent on three jointly sufficient favourable background conditions: the behaviour of other Five Eyes intelligence-sharing allies, geopolitical developments such as China's 2020 security law for Hong Kong, and domestic actors' positions. The findings suggest that US influence on its allies in the context of technological competition with China is limited. Even though US influence can be effective under specific geopolitical and domestic conditions, the US needs to develop a more nuanced and cooperative strategy if it seeks to leverage alliances in its competition with China.

4.1. Introduction

In recent years, states in all regions of the world have responded in various ways to Chinese overtures to invest in their critical national infrastructures (CNI), as part of initiatives such as the Chinese Belt and Road Initiative (BRI) and the Digital Silk Road (DSR). Political decision-making on whether to accept Chinese investments and involvement has sparked fervent debates in public and policymaking realms, given the rapid development of non-Western states becoming global leaders in key technologies, as China has become in the realm of 5G. As pointed out by Andrea Gilli, historically speaking, 'this is the first time since the end of WWII that a leader of a key technology is neither an (American) ally nor a NATO country.'[1] Given reports that China has officially launched research and development for its 6G mobile networks,[2] the question of whether to accept Chinese investments is likely to become even more salient in the future.

We urgently need to understand how 'middle power' states, thrown into the midst of the competition for technological primacy between the United States and China – commonly referred to as a 'Tech War' – will make decisions relating to their CNI.[3] The US has attempted to employ both persuasive and coercive tactics to sway its allies to reject Chinese investments in CNI. Members of the Five Eyes alliance (FVEY) have been particularly targeted by US influence, as their ties in intelligence gathering have rendered Chinese presence in their domestic telecommunications networks subject to strategic and security concerns. This tension can be observed most recently by the United Kingdom's quick policy reversal from accepting

[1] Andrea Gilli, "NATO and 5G: What Strategic Lesson?" *NDC Policy Brief, No.13* (2020) p.3
[2] Arjun Kharpal, "China starts development of 6G having just turned on its 5G mobile network" *CNBC* (7 November 2019) <https://www.cnbc.com/2019/11/07/china-starts-6g-development-having-just-turned-on-its-5g-mobile-network.html> (accessed 02/01/20)
[3] In this article, I adopt the definition of CNI as infrastructure 'that provides an essential support for economic and social wellbeing, for public safety and for the functioning of key government responsibilities.' (Organisation for Economic Cooperation and Development (OECD), "Protection of critical infrastructure and the role of investment policies relating to national security." *Paris: Organisation for Economic Co-operation and Development*, 2008. p.3)

Huawei's involvement in building its national 5G telecommunications networks in January 2020 to banning the company in July. These developments raise the question of the extent to which the US can effectively influence the UK's decision-making regarding Chinese investment in domestic CNI.

There are good reasons for which UK policymakers would welcome Chinese investment in their CNI, and these are predominantly economic. It is economically lucrative to authorise such investments and accept foreign direct investment (FDI), as it contributes to the increase of the gross domestic product (GDP) of the state. The economic benefits of Chinese investment in the UK's CNI include increased tax revenue, job creation, and increased investment in research and development.[4] On the other hand, the reasons for which the UK would ban such investments are security concerns related to foreign ownership of CNI. This includes the multiplication of 'opportunities for espionage', the reduction of 'law enforcement communications interception capabilities,'[5] and the overall potential for disruption, through both physical- and cyber-attacks of CNI and the services it provides.[6]

The UK's policy reversal on Huawei is a good example of US influence over its allies' domestic politics. In the past, the UK warmly welcomed Chinese investments across sectors of its CNI, making the Huawei policy reversal a deviant case. By employing within-case process tracing of a single case study, I argue that US influence was necessary for the UK's policy reversal, but it was not sufficient alone. US influence interacted with three favourable background conditions: the behaviour of the other FVEY members, geopolitical developments at the time, and the interests and divisions of domestic actors. None of these conditions would

[4] Sourafel Girma, David Greenaway, and Katharine Wakelin. "Who benefits from foreign direct investment in the UK?." *Scottish journal of political economy* 48, no. 2 (2001): 119-133. p.131
[5] James Lewis, "New Objectives for CFIUS: Foreign Ownership, Critical Infrastructure, and Communications Interception." *Fed. Comm. LJ* 57 (2004) p.475
[6] Dan Assaf, "Foreign Direct Investment in an Era of Increased Threats to Critical Infrastructures." In *Critical Infrastructure Protection IV: Fourth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, ICCIP 2010, Washington, DC, USA, March 15-17, 2010, Revised Selected Papers 4*, pp. 17-27. Springer Berlin Heidelberg, 2010. p.17

have caused the policy reversal on their own. Instead, US influence amplified their individual effects, making them jointly sufficient.

Are these findings generalisable across sectors of CNI and US allies? First, US influence varies across CNI sectors in the UK. Whilst successful in telecommunications, it may be less so in others, such as the civil nuclear sector, in which Chinese investments continue to be accepted.[7] This could indicate that the US is willing to exert more pressure in sectors relevant to its competition on technological superiority with China, and that allies are more likely to be influenced in such sectors. Second, the generalisability of these findings to digital CNI sectors in other US allies depends on specific background conditions. These conditions may enable or disable US influence, presenting an area for further research. As the necessary conditions I identify in this paper are not universally present, I argue that US influence can be effective but is not consistently so. It represents a gamble, dependent on the interplay of international and domestic factors.

The question of how states make decisions on foreign involvement in their CNI is also linked to much larger conceptual questions, not only on great power rivalry between the US and China and its effect on international relations (IR), but also on alliance cohesion between the US and the UK, as well as the FVEY alliance more broadly. The Huawei debate seems to be providing a test of strength in the post-Cold War era for alliance persistence in the Western world.[8] Moreover, how states make such decisions can be tied to their different conceptualisations of sovereignty and the weight to which they ascribe self-sufficiency and independence from external forces. The issue of foreign involvement in CNI is particularly important in an era of digitalisation, where cyberspace is borderless. How states make decisions regarding foreign involvement in their CNI will provide insights into how they are dealing with

[7] Andrew Ward and Jim Pickard, "Hinkley go-ahead after 'national security' safeguards" *Financial Times* (15 September 2016) <https://www.ft.com/content/0cde26b6-7b66-11e6-b837-eb4b4333ee43> (accessed 21/01/20)
[8] Ruike Xu, *Alliance persistence within the Anglo-American special relationship: The post-Cold War era*. Springer, 2017.

globalisation and security in a world where economic benefits and security risks are potentially at odds. Given that the article's question implicates a broad range of fundamental IR concepts and themes, we would expect a thriving debate; however, the literature review in the next section shows that this area of research remains unexplored and underdeveloped.

The paper proceeds with the literature review, expounding first the empirical puzzle followed by the literature relevant to explaining the importance of US influence, the hypothesised necessary condition of the policy outcome. Second, I provide an overview of the theoretical approach, followed by a delineation of the research design and the causal chain. Finally, the last section presents the case study and carries out process tracing.

4.2. Literature Review

4.2.1. The Puzzle

In the past few decades, the UK has warmly welcomed Chinese investments in its CNI. During President Xi Jinping's state visit to the UK in 2015, then-chancellor George Osborne claimed it would be a 'golden decade' for Sino-British relations.[9] The Department for International Trade actively encouraged British businesses to invest in the BRI, and after Theresa May's trade delegator visit to Beijing in 2019 Sino-British deals worth £9.3 billion were signed.[10] British finance minister Philip Hammond stated that the 'UK is committed to helping realise the potential of the BRI.'[11] In 2016, then-Prime Minister Theresa May approved a project to construct a nuclear power station in Somerset, Hinkley Point C, led by state-owned

[9] Jonathan Ford and Laura Hughes, "UK-China relations: from 'golden era' to the deep freeze." *Financial Times.* (14 July 2020). <https://www.ft.com/content/804175d0-8b47-4427-9853-2aded76f48e4> (accessed 15/07/20)
[10] British Foreign Policy Group, "China's Belt and Road Initiative: *Towards a British Response Strategy – Student Ambassador Series* (10 April 2019). <https://bfpg.co.uk/2019/04/chinas-belt-and-road-initiative-towards-a-british-response-strategy/> (accessed 01/02/20)
[11] Chris Devonshire-Ellis, "China's Belt and Road Initiative and the United Kingdom" *Silk and Road Briefing* (13 June 2018). <https://www.silkroadbriefing.com/news/2019/06/05/chinas-belt-road-initiative-united-kingdom/> (accessed 12/04/20)

Électricité de France S.A. (EDF) of France and state-owned China General Nuclear Power Group (CGN) of China. CGN's involvement in Hinkley Point C led to a quid pro quo agreement which could oblige the UK government to approve CGN's plan to build another nuclear reactor, Bradwell B, the first majority Chinese-owned nuclear plant.[12]

On the other hand, in relation to Chinese investment in telecommunications, the UK broke its previous policy pattern. In July 2020, the UK government decided to ban Huawei from its national fifth generation (5G) networks. Given previous enthusiasm on Chinese involvement in CNI, this response to Huawei's involvement in 5G networks was puzzling. 5G is expected to enable the advance of robotics, automation, virtual and augmented reality, the Internet of Things, artificial intelligence, and machine learning.[13] Whilst innovations on 4G networks were largely dominated by states in the global West, since 2012 China has led in building networks and setting operating standards around the world, ensuring an omnipresence in 5G infrastructure rollout through its largest telecommunications equipment company, Huawei.[14]

In recent years fear and suspicion have characterised states' *modus operandi* with Chinese telecommunications companies, due to the belief that Beijing, which has a record of practicing 'little restraint when it comes to penetrating foreign networks',[15] pulls the strings of companies such as Huawei and ZTE. This is evidenced by Article 7 of China's 2017 National Intelligence Law which requires organisations and citizens to 'support, assist and cooperate with state intelligence work.'[16] Huawei has also problematically faced allegations of corporate espionage

[12] Jonathan Ford, "UK's reliance on China's nuclear tech poses test for policymakers" *Financial Times* (14 February 2019). <https://www.ft.com/content/7734e3be-2f6f-11e9-8744-e7016697f225> (accessed 15/03/20)
[13] Kadri Kaska, Henrik Beckvard and Tomas Minarik, "Huawei, 5G and China as a security threat." *NATO Cooperative Cyber Defence Center for Excellence* 28 (2019). p.6
[14] Foreign Policy, "5G Explained: Part One—Technology and Infrastructure." (2020) <https://foreignpolicy.com/2020/01/22/5g-cellular-huawei-china-networks-technology-infrastructure-power-map/> (accessed 25/02/20)
[15] Ivo Daalder, "Commentary: Britain sticks with Huawei for 5G – and jeopardises the Five Eyes alliance." *Chicago Tribune*. (30 January 2020) <https://www.chicagotribune.com/opinion/commentary/ct-opinion-5g-huawei-britain-ivo-daalder-20200130-xympy43dovds7m3gs4fvn5xapq-story.html> (accessed 31/01/20)
[16] Arjun Kharpal, "Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice." *CNBC* (4 March 2019) <https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html> (accessed 05/05/20)

and intellectual property theft.[17] The fear of Chinese control of basic 5G infrastructure is linked to espionage and sabotage, specifically the risks posed by backdoors in hardware or programming of software to allow access to spies and saboteurs. In addition, over-dependence and lack of alternatives could allow China to cut off access to technology as a way of punishment. Even without installing backdoors, Huawei could provide the Chinese government with technical specs, first notice of zero-day flaws, or overall information on network structure that could be used to detrimental effect.

Nevertheless, the revolutionary significance of acquiring 5G quickly has created a dilemma for many states. Europe especially 'finds itself in a difficult situation, positioned between the US and China, facing pressure from both sides.'[18] The advantages of maintaining Huawei in 5G networks are largely economic, as its equipment is currently embedded in European networks. Apart from the economic cost of removing it from the networks, delaying the rollout of 5G has been predicted to cause the UK to miss the opportunity 'to add around $224 billion to its GDP between 2020 and 2030.'[19] Moreover, banning Huawei is not understood as an effective solution to the security challenges. If China were interested in accessing a network for whatever reason, it would be able to with or without the help of Huawei equipment.[20] Even in the absence of Huawei hardware, systems can still rely on software developed in China and software can be reprogrammed remotely, potentially allowing access to the network.[21] On the

[17] Amanda Connolly, "Huawei, Meng Wanzhou hit with new racketeering, corporate espionage charges in US" *Global News* (13 February 2020) <https://globalnews.ca/news/6547303/doj-adds-huawei-charges/> (accessed 05/05/20)
[18] Tim Rühlig and Maja Björk, "What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe." *The Swedish Institute of International Affairs* (2020) p.5
[19] Thomas Wintle, "Huawei ban from UK's 5G network risks $23.6bn economic hit – report" *CGTN* (10 September 2020) <https://newseu.cgtn.com/news/2020-09-09/Huawei-ban-from-UK-s-5G-network-risks-23-6bn-economic-hit-report--TE41jbvIoE/index.html> (accessed 17/11/20)
[20] Rühlig and Björk, "What to Make of the Huawei Debate?" pp.7-13
[21] Sue Halpern, "The Terrifying Potential of the 5G Network" *The New Yorker* (26 April 2019) <https://www.newyorker.com/news/annals-of-communications/the-terrifying-potential-of-the-5g-network> (accessed 07/08/20)

other hand, the security risks of retaining Huawei equipment the potential for the company to engage in espionage or disrupt communications during future disputes.[22]

The US, like all other states, faces the dilemma described. However, it also plays a role in the decision matrix of other states as an important alliance partner and the Western hegemon, who has decided to agitate against Huawei. The Trump administration launched an aggressive campaign to prevent Chinese firms from participating in the global 5G rollout. Throughout 2019 and 2020, American officials tried to 'pressure, scold, and, increasingly, threaten' other states considering using Huawei in building 5G networks, pledging to withhold intelligence from them.[23] This has been perceived not only by China but also by some Western states as a 'protectionist move' targeted at undermining China's high-tech aspirations.[24]

Despite the Trump administration's warnings of the erosion of their so-called special relationship, British policymakers decided in January 2020 not to ban 'high-risk vendors' but only exclude them from 'security critical network functions' and cap their presence in other network functions to up to 35%.[25] In contrast, other US intelligence-sharing allies such as Australia placed full bans on Huawei participation in 5G networks with little hesitation. Just a few months later, on 14 July, the government announced that Huawei will be completely removed from the UK's 5G networks by the end of 2027, with a total ban on the purchase of any new 5G kit after 31 December 2020.[26] Following the UK's decision, other states which had initially welcomed Huawei equipment also decided to cut the Chinese company out of their

[22] Tim Bowler, "Huawei: Why is it being banned from the UK's 5G network?" *BBC News* (14 July 2020) <https://www.bbc.com/news/newsbeat-47041341> (accessed 17/11/20)
[23] Julian Barnes and Adam Satariano. "US Campaign to Ban Huawei Overseas Stumbles as Allies Resist." *The New York Times* (17 March 2019) <https://www.nytimes.com/2019/03/17/us/politics/huawei-ban.html> (accessed 17/03/20)
[24] E. K. Jaisal, "The US, China and Huawei Debate on 5G Telecom Technology: Global Apprehensions and the Indian Scenario." *Open Political Science* 3, no.1 (2020) p.69
[25] Dominic Raab, "Oral Statement to Parliament: Foreign Secretary's Statement on Huawei". *GOV.UK.* (28 January 2020) <https://www.gov.uk/government/speeches/foreign-secretary-statement-on-huawei> (accessed 12/02/20)
[26] Department for Digital, Culture, Media and Sport, "Huawei to be removed from UK 5G networks by 2027." *GOV.UK.* (14 July 2020) <https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027> (accessed 15/07/20)

telecommunications networks, thus delaying the rollout of their 5G and incurring massive economic losses.[27]

Given the factors outlined above, the UK's change in attitude and policy towards Chinese involvement in CNI is puzzling. Numerous reasons for which Huawei was banned in the UK apply to all other Chinese companies – for example, similarly to Huawei, CGN, the company involved in Hinkley Point C, is on the US' Commerce Department's entity list which bans American companies from supplying the Chinese group without obtaining rarely-granted licenses.[28] In this paper, I identify the causes of this policy change and measure the effect of US influence to explain the change in policy outcome.

4.2.2. US Strategies to Achieve Technological Superiority

Now that I have established that the UK's change in decision-making vis-à-vis Chinese investments in its CNI is puzzling, I turn to the literature which provides potential explanations on why the US seeks to exert influence in the UK's and its allies' domestic decision-making on Chinese investments. These explanations are found predominantly in literature which addresses US-China Tech War dynamics.

A relevant body of literature is that which deals with US-China relations as they relate to involvement in CNI, most commonly pointing to the US' attempts to securitise Chinese companies. Jonna Nyman used the example of US elite actors' securitisation of the bid by China National Offshore Oil Corporation (CNOOC) for US energy company Unocal to argue that such securitisation is problematic, as it 'encourages strategic and/or economic competition

[27] Matthew Field, "Cutting out Huawei from 5G network would cost Britain £7bn" *The Telegraph* (5 April 2019) <https://www.telegraph.co.uk/technology/2019/04/04/cutting-huawei-5g-network-would-cost-britain-7bn/> (accessed 12/11/20)
[28] Christian Shepherd, "US blacklists Chinese nuclear company over theft of military tech" *Financial Times* (15 August 2019) <https://www.ft.com/content/9601ebda-bf24-11e9-b350-db00d509634e> (accessed 26/08/20)

between states over energy supplies.'[29] Andrew Stephen Campion used critical discourse analysis to examine how China has been constructed as an existential threat, drawing on US reactions to CNOOC in 2005 and to Huawei more recently.[30] Campion argues that a coherent 'China Threat Discourse', which portrays the state 'as a belligerent and capable actor with interests running counter to the interests of the Self,' [31] has been employed in the US to protect its interests, increasingly in the context of CNI. Although this article is elucidating, it does not contribute to understanding the differences in the backlash against Huawei as compared to the reaction against CNOOC.

The tensions between the US and China over 5G are representative of a much more expansive landscape that will underpin the future of the world's CNI. Intensifying strategic competition between the US and China has 'lent new momentum to a US whole-of-government effort to curb the use of technology built or maintained by leading Chinese tech firms.'[32] Yan Xuetong argues that 'digital mentality', defined as 'the way of perceiving and responding to international strategic issues from the perspective of cybersecurity and digital economy'[33] influences foreign policy decision-making. This implies that the mentality leads to policymakers' consideration of cyberspace as more strategically important to national survival than the geophysical world. This characterises the struggle between the US and China, just as Cold War mentality, which rested on ideological biases and beliefs, defined US-Soviet competition. Digital mentality is a particularly helpful concept to understand why the US has focused on applying pressure on its allies vis-à-vis foreign involvement in critical digital

[29] Jonna Nyman, "'Red Storm Ahead': Securitisation of Energy in US–China Relations." *Millennium* 43, no. 1 (2014): 43-65. p.43
[30] Andrew Stephen Campion, "From CNOOC to Huawei: securitization, the China threat, and critical infrastructure." *Asian Journal of Political Science*28, no.1 (2020) p.52
[31] *ibid.* p.32
[32] Robert Greene and Paul Triolo, "Will China Control the Global Internet Via its Digital Silk Road?" *Carnegie Endowment for International Peace*. (8 May 2020) <https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857> (accessed 22/09/20)
[33] Yan Xuetong, "Bipolar Rivalry in the Early Digital Age." *The Chinese Journal of International Politics* (2020). P.5

infrastructures in comparison to other CNI sectors. However, this is only rendered implicit within this literature and there is a lack of empirical testing of Xuetong's concept of digital mentality.

A final concept which is central to the article for the purpose of understanding *why* the US and China seek to achieve global technological primacy over the other is that of weaponised interdependence, which Henry Farrell and Abraham L. Newman coin to explain that 'states with political authority over the central nodes in the international networked structures through which money, goods and information travel are uniquely positioned to impose costs on others.'[34] Importantly, they point out that if US allies decide that the US has been 'abusing' weaponised interdependence in ways that conflict their core interests, they will defect and set up their own alternatives. The concept not only provides insights on the motivations behind the US' pressure to ban Huawei, but also delivers a stark warning that this pressure may be counterproductive to the US' larger strategic aims.

Overall, current IR literature provides several reasons why the US would seek to influence its allies, specifically the UK's, decision-making on whether to accept Chinese companies' involvement in its domestic telecommunications networks. However, it falls short of understanding and explaining how, when and to what extent the US attempts to influence could be effective. In this article, I seek to shed light on this empirical puzzle and evaluate US influence as a variable in third states' decision-making matrix on Chinese companies' involvement in their CNI.

[34] Henry Farrell and Abraham L. Newman, "Weaponized interdependence: How global economic networks shape state coercion." *International Security*44, no.1 (2019) p.45

4.3. Theory

I posit that US influence was a necessary but not sufficient factor behind the UK's policy reversal on Huawei's involvement in its 5G network from January to July 2020. Rather, US influence interacted with a series of favourable background conditions, which, when combined, had a cumulative effect leading to the policy shift. The role of US influence as a driving factor indicates that the UK's policy reversal was highly dependent on alliance pressure. However, it is important to note that whilst these factors were necessary as a combined set of causes, the effectiveness of US influence under different conditions cannot be assessed without identifying these alternative combinations. In the next sections, I explore the background conditions followed by the necessary variable (US influence) in further depth.

4.3.1. Background Conditions

In this section, I identify three favourable background conditions that enabled US influence to be effective in the UK case. It is important to note that none of the following background conditions alone would have cause the policy reversal. US influence was necessary to amplify their individual effects and make them jointly sufficient.

The first of the favourable background conditions (A) is the behaviour of the other Five Eyes (FVEY) members. This condition reminds us that the UK decision was taken within a broader international environment. Whilst the US was active in pushing against Huawei, it was not alone. Australia, in particular, also banned Huawei, and may also have been speaking with the UK. The FVEY is an anglophone intelligence alliance based on signals intelligence (SIGINT) founded in 1941. It is the world's most enduring multilateral arrangement of its type and 'has always been the most dominant actor in cyberspace.'[35] FVEY partners have often felt

[35] Max Smeets, "US cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection." *Intelligence and National Security* 35, no. 3 (2020): 444-453. p.4

'psychological pressure to avoid social sanctions' in not adopting US intelligence methodologies.[36] FVEY members, the US, UK, Canada, Australia and New Zealand, interact with an affinity strengthened by their common Anglo-Saxon culture, accepted liberal-democratic values and complementary national interests, 'all seasoned with profound sense of confidence in each other and a degree of trust so strong as to be unique in the world.'[37] However, importantly for this article, a number of scholars have pointed to the asymmetric nature of the alliance and British resentment towards having been assigned a secondary role.[38]

The second of the favourable background conditions (B) is the geopolitical developments at the time. Anti-China rhetoric was on the rise as a result of China's role in the promulgation of COVID-19, causing a global pandemic and bringing the world economy to a halt. Most importantly, there was an increasing aggressiveness of Chinese foreign policy on the world stage as indicated by China's new security law for Hong Kong, which 'makes it easier to punish protesters and reduces the city's autonomy'[39] and human rights violations such as China's repression of Uighurs in Xinjiang.[40] The new security law in Hong Kong, a former British colony, resulted in the UK offering up to three million Hong Kong residents the chance to settle in the UK and apply for citizenship,[41] thus escalating political tensions with China.

The final background condition (C) is the role of domestic actors. Domestic actors also played a role in the policy reversal by challenging the wisdom of letting China invest in 5G. Whilst their singular motivations are difficult to pinpoint, it is clear that they helped to create

[36] Richard Morgan, "Oversight through Five Eyes: Institutional Convergence and the Structure and Oversight of Intelligence Activities." *Global Intelligence Oversight* (2016) p.58
[37] James Samuel Cox, *Canada and the five eyes intelligence community*. Canadian Defence & Foreign Affairs Institute, 2013. p.2
[38] Andrew O'Neil, "Australia and the 'Five Eyes' intelligence network: the perils of an asymmetric alliance." *Australian Journal of International Affairs* 71, no. 5 (2017): 529-543. p.533
[39] BBC, "Hong Kong security law: What is it and why is it worrying?" *BBC News* (30 June 2020) <https://www.bbc.co.uk/news/world-asia-china-52765838> (accessed 03/11/20)
[40] Lindsay Maizland, "China's Repression of Uighurs in Xinjiang" *Council on Foreign Affairs* (30 June 2020) <https://www.cfr.org/backgrounder/chinas-repression-uighurs-xinjiang> (accessed 03/11/20)
[41] BBC, "Hong Kong: UK makes citizenship offer to residents" *BBC News* (1 July 2020) <https://www.bbc.com/news/uk-politics-53246899> (accessed 30/03/22)

a climate of domestic division in the lead-up to the decision. This division made the decision-making process more difficult and less clear-cut. However, the extent to which this division was correlated, or caused, by US influence is difficult to determine.

4.3.2. Necessary Condition: US Influence

In this section, I explain US influence as a necessary condition for the UK's policy reversal, which rendered the favourable background conditions outlined above jointly sufficient by amplifying their individual effects. US influence manifests itself in a number of ways and varies in intensity, ranging from persuasion to coercion. The first way is through the discursive framing of what is appropriate for US allies to do, which resembles norm framing, a 'persuasive device used to fix meanings, organise experience and alert others that their interests and identities are at stake.'[42] In the case of Huawei, the framing of the company as an international security threat without substantive evidence began in 2013, when the US President at the time, Barack Obama, banned Huawei from working with the US government. The second way in which US influence manifests is through coercive threats. The Trump administration played the card of threatening to halt intelligence sharing with key allies which use Huawei equipment in their 5G networks numerous times. Essentially, the US used statements on values they share with the UK and other allies to coerce them. Robert Ayson explains that 'expectations that allies should act according to common values can be used to discipline a close partner.'[43] Finally, in another form of coercion, a more intense pressure is felt once actions are taken by actors towards making the threats a reality, if intimidation does not work. In the Huawei case, then the UK approved the company's involvement in its 5G national networks, despite previous

[42] Michael Barnett, "Culture, strategy and foreign policy change: Israel's road to Oslo." *European Journal of International Relations* 5, no.1 (1999) p.25
[43] Robert Ayson, "The coercive power of shared values." *Political Science* 70, no.3 (2018). p.199

levels of US influence, the US took steps to actualise the threat of dissolving their special relationship by initiating a review of their intelligence-sharing conditions.

The presence of US influence in the UK's telecommunications sector, unlike other Chinese investments in the UK's CNI, aligns with the US strategy to counter China's technological rise. As I highlighted in the literature review, the US perceives a significant threat from China achieving global technological dominance, particularly in technology sectors. Investments in telecommunications is critical, as it sets precedents for future technological developments like 6G, making Chinese systems more economically attractive. This differs from sectors like civil nuclear, which do not easily replicate this trend due to the established presence of Chinese companies. Indeed, a senior UK intelligence official recalled that British policymakers had asked their US counterparts during a meeting at the White House why they had made 'the position of Huawei hardware in the UK the centre piece of a global campaign against Chinese technology.' A US policymaker responded with a shrug, stating 'you've got to pick something.' This indicates that concerns on Huawei were not founded on security concerns – which this source called 'nonsense' as 5G was completely 'sensationalised into a big bubble of risk' – but were part of a larger strategy to undermine Chinese technological superiority.

4.4. Research Design

The universe of cases relevant to this paper are the instances of the UK's acceptance or ban of Chinese investments in different sections of its CNI. The Huawei case yields a different outcome from the others, which prompts an investigation into the cause of this divergence. I hypothesise that US influence, in conjunction with favourable background conditions, was a necessary factor. To test this hypothesis, I employ the deviant case method, which involves selecting a case that demonstrates a surprising value in relation to a general cross-case

relationship.[44] Despite prior expectations and a cost-benefit analysis from economic and political perspectives, the UK's decision regarding Huawei in its 5G networks deviates from the anticipated outcome. To analyse this, I employ within-case process tracing, employing techniques to examine the intermediate steps in cognitive mental processes.[45] I collect Causal Process Observations (CPOs) and subject them to process tracing tests to determine the strength of the evidence.

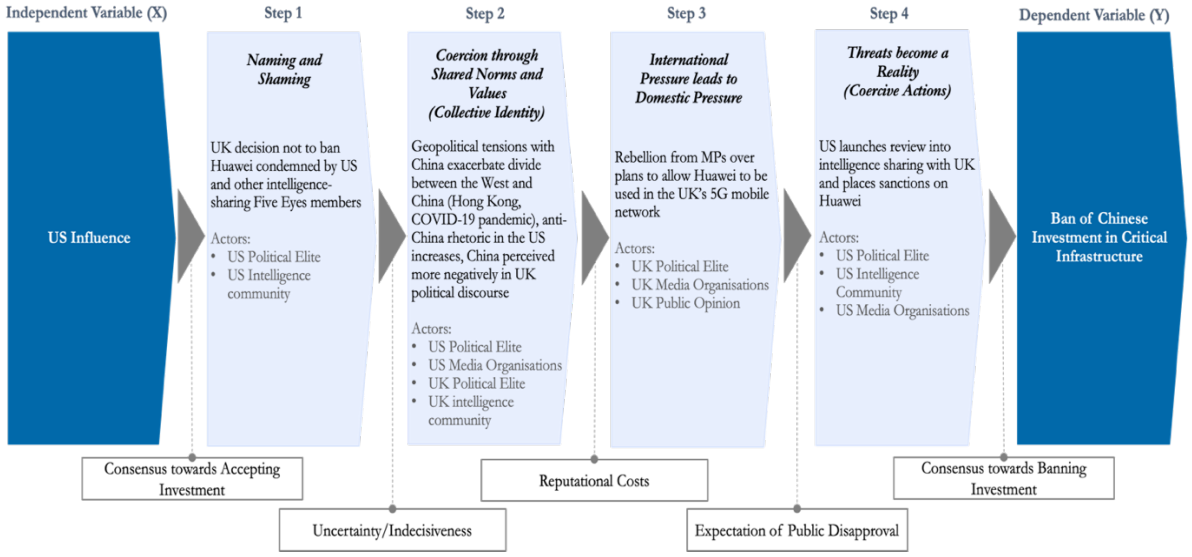
The timeframe of the case study starts from November 2010, when the UK set up the Huawei Cyber Security Evaluation Centre (HCSEC). In March 2013, US President Obama banned Huawei from working with the US government, and in December 2018 Canada arrested Huawei CFO Meng Wanzhou at the request of the US. On 15 May 2019, the US banned Huawei by executive decree, and in June, Huawei filed a lawsuit against the US Department of Commerce. On 28 January 2020, the UK announced it would not ban Huawei equipment from being used in its national 5G networks. On 15 May, the US announced new export controls aimed at limiting Huawei's access to semiconductor technology. Finally, on 14 July 2020, the UK performed a U-turn on its policy and the National Security Council decided that Huawei would be removed from the UK's 5G networks by 2027.

Figure 1 displays the causal chain, depicting the independent variable as US influence and the dependent variable as the ban on Chinese investment in CNI. Step 1, 'naming and shaming,' involves US political elite and intelligence officials making statements to influence UK policymakers, leading to uncertainty and indecisiveness. Step 2, 'coercion through shared norms and values,' sees US political elite and media organisations emphasising the divide between the West and China, creating risks of reputation costs. Step 3, 'international pressure leads to domestic pressure,' involves UK political elite and media organisations forming

[44] Jason Seawright and John Gerring, "Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options." *Political Research Quarterly* 61.2 (2008): 294-308 p.302
[45] Andrew Bennett and Jeffrey T. Checkel, eds. *Process tracing*. Cambridge University Press, 2015. p.5

resistance groups against Chinese involvement, driven by fear of public disapproval. The final step, 'threats become a reality,' entails coercive actions by the US, such as imposing sanctions and launching reviews, with US political elite, media organisations, and the intelligence community as relevant actors. Favourable conditions allow US influence to operate in each step, with the behaviour of other FVEY members, geopolitical developments, and disagreements between domestic actors contributing to the overall influence. Throughout the case study section, for each step I discuss the background conditions within the individual steps. I show how US influence amplified their individual effects, and why they would not have led to a policy reversal on their own.

Figure 1: Causal Graph illustrating the effect of US Influence on UK Policy vis-à-vis Chinese Investment in CNI



4.5. Case Study

4.5.1. Consensus on Accepting Huawei Before Onset of US Influence

Extensive evidence suggests a prevailing consensus among British policymakers regarding the acceptance of Chinese investments in the UK's CNI prior to 2019. In January 2018, then-prime minister Theresa May declared 'China is a country that we want to do a trade deal with.'[46] Further back in 2015, then-chancellor George Osborne stated that 'no economy in the West is as open to Chinese investment as the UK.'[47] These are narratives indicate the importance of national economic prosperity related to accepting Chinese investments.

In relation to telecommunications specifically, then-Prime Minister Boris Johnson stated that the decision to retain Huawei was based on a blunt assessment of Britain's economic interests.[48] Johnson's adviser, Dominic Cummings, emphasised the aim to make Britain 'the best place in the world to be for those who can invent the future.'[49] UK officials argued that building a Huawei-free network would add 'delays of years' and 'very considerable costs.'[50] Industry actors agreed: in January 2020, the CEOs of BT and Vodafone wrote a letter to the Prime Minister arguing they had 'not seen evidence that Huawei equipment poses a security risk that warrants a total ban' and reiterated that if Huawei is banned there would be 'significant ramifications for the rollout of 5G.'[51]

---

[46] Charlie Cooper, "Britain toughens stance on China as it eyes US" *Politico* (13 July 2020) <https://www.politico.com/news/2020/07/13/boris-johnson-china-huawei-359741> (accessed 14/07/20)
[47] Ford and Hughes, "UK-China relations"
[48] Mark Landler and Stephen Castle, "Johnson Risks a Rift with Trump by Granting New Access to Huawei" *The New York Times* (28 January 2020) <https://www.nytimes.com/2020/01/28/world/europe/johnson-trump-hwawei-rift.html?searchResultPosition=7> (accessed 21/02/20)
[49] *ibid.*
[50] Robbie Gramer and Lara Seligman, "Can the US-UK Special Relationship Weather the Huawei Storm?" *Foreign policy* (30 January 2020) <https://foreignpolicy.com/2020/01/30/huawei-intelligence-united-states-britain-trump-5g-infrastructure-concerns-digital-espionage-special-relationship-five-eyes/> (accessed 04/02/20)
[51] Dan Sabbagh and Mark Sweney, "BT and Vodafone to lobby PM to allow use of Huawei equipment" *The Guardian* (17 January 2020) <https://www.theguardian.com/technology/2020/jan/17/uk-officials-frustrated-us-huawei-plan-b> (accessed 17/01/20)

Whilst maintaining a positive approach towards Chinese investments in the UK's CNI, policymakers also proposed safeguards to mitigate risks. In 2013, the Intelligence and Security Committee released a report on foreign involvement in CNI, proposing an effective process by which Government is alerted and updated on Chinese investments in CNI. The report concludes that 'any policy which seeks to block all Chinese companies from any future contracts relating to CNI projects is not only impractical but, crucially, (…) it is unlikely to result in the national security protection envisaged.'[52] Moreover, in January 2020, Foreign Secretary Dominic Raab confirmed that Huawei would be subject to 'one of the strongest regimes for telecoms security in the world,'[53] insisting that 'we know more about Huawei and the risks it poses than any other country in the world.'[54] This can also be understood by the UK's creation of the Huawei Cyber Security Evaluation Centre (HCSEC) in 2010. As written by Dr Ian Levy, the technical director of NCSC, 'we've never "trusted" Huawei and the artefacts you can see (like the Huawei Cyber Security Evaluation Centre (HCSEC) and the oversight board reports) exist because we treat them differently to other vendors.'[55] A senior intelligence official during an interview agreed with this, specifying that the 'UK's approach since 2003 has always been technical risk management.'

Overall, before the onset of US influence in numerous forms in 2019, the evidence collected points to UK policymakers acknowledging the strategic concerns especially as they relate to national security and aiming to address them whilst maintaining a consensus about accepting Chinese investments in CNI.

[52] Sir Malcom Rifkind MP, "Foreign Involvement in the Critical National Infrastructure" Cm (Series) (Great Britain. Parliament); 8629 2013-14. Norwich (2013). p.18
[53] Heather Stewart and Dan Sabbagh, "UK Huawei decision appears to avert row with US" *The Guardian* (28 January 2020) <https://www.theguardian.com/technology/2020/jan/28/boris-johnson-gives-green-light-for-huawei-5g-infrastructure-role> (accessed 17/02/20)
[54] *ibid.*
[55] Ian Levy, "The future of telecoms in the UK" *National Cyber Security Centre* (28 January 2020) <https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk> (accessed 01/02/20)

4.5.2. Step 1: Naming and Shaming

US Influence

British officials sought smoking gun evidence proving Huawei constituted a security threat, whilst 'the Trump administration polluted the debate in Europe'[56] despite the lack of such evidence. Robert Strayer, US Deputy Assistant Secretary of State for Cyber Policy, confirmed 'we really pivoted that discussion over time.'[57] Ahead of the January decision to keep Huawei equipment in 5G networks, the Trump administration delivered sharp warnings about China. Secretary of State Mike Pompeo, during a visit to London in mid-January, stated: 'we were trying to make the case (…) that we think putting Huawei technology anywhere in your system is very, very difficult to mitigate and therefore not worth the gamble.'[58] Following the UK's decision to maintain Huawei in 5G networks in January 2020, a Trump administration official stated that the US was 'disappointed', adding that 'we look forward to working with the UK on a way forward that results in the exclusion of untrusted vendor components from 5G networks.'[59] This confirms the hypothesis that the US sought to alter the decision-making vis-à-vis Huawei within the UK, as it is a political source publicly stating that US policymakers would step in to ensure the exclusion of Huawei.

Following the January 2020 decision to retain Huawei, several Democratic and Republican Senators and House Candidates expressed their disappointment on social media, calling for the UK-US 'special relationship' to be 'reconsidered' due to Boris Johnson's 'wrong, dangerous

[56] Ellen Nakashima and William Booth, "Britain bars huawei from its 5G wireless networks, part of a growing shift away from the Chinese tech giant" *The Washington Post,* (15 July 2020) <https://www.washingtonpost.com/national-security/britain-to-bar-huawei-from-its-5g-wireless-networks-part-of-a-growing-shift-away-from-the-chinese-tech-giant/2020/07/13/44f6afee-c448-11ea-b037-f9711f89ee46_story.html> (accessed 01/08/20)
[57] *ibid.*
[58] Gramer and Seligman, "Can the US-UK Special Relationship Weather the Huawei Storm?"
[59] Adam Satariano, "Britain Defies Trump Plea to Ban Huawei from 5G Network" *The New York Times* (28 January 2020) <https://www.nytimes.com/2020/01/28/technology/britain-huawei-5G.html?searchResultPosition=8> (accessed 09/02/20)

and grave short-sighted mistake.'[60] There were calls for Congress to 'work on a bipartisan basis to push back on this decision by the UK.'[61] US senator Tom Cotton explained that 'allowing Huawei to build the UK's 5G networks today is like allowing the KGB to build its telephone network during the Cold War' and US Senator Lindsey Graham clearly wrote 'this decision has the potential to jeopardise US-UK intelligence sharing agreements and could greatly complicate a US-UK free trade agreement. I hope the British government will reconsider its decision.'[62] Moreover, Senator Ben Sasse, who is a member of the Senate Select Committee on Intelligence, stated: 'here's the sad truth: our special relationship is less special now that the UK has embraced the surveillance state commies at Huawei. The Chinese Communist Party has infected Five Eyes with Huawei, right at a time when the US and UK must be unified in order to meet the global security challenges of China's resurgence.'[63]

In addition, the US threatened to cut off intelligence-sharing ties with the UK. Defence Secretary Mark T. Esper stated that 'if countries choose to go to the Huawei route, it could well jeopardise all information sharing and intelligence sharing we have been talking about, and that could undermine the alliance, or at least our relationship with that country.'[64] In February, Acting Chief of Staff to President Trump Mick Mulvaney warned British officials of a 'direct and dramatic impact' on intelligence sharing with the US.[65] This evidence reveals US efforts to influence the UK through naming an shaming, as there appears to be no other plausible

[60] Joe Tidy, "Huawei: How the UK's decision affects the rest of the world" *BBC News* (28 January 2020) <https://www.bbc.co.uk/news/technology-51284393> (accessed 15/02/20)
[61] Tidy, "Huawei: How the UK's decision affects the rest of the world"
[62] *ibid.*
[63] Arjun Kharpal, "Our special relationship is less special: UK-US bond tested by Britain's Huawei 5G decision" *CNBC* (29 January 2020) <https://www.cnbc.com/2020/01/29/uk-us-relationship-tested-with-britain-huawei-5g-decision.html> (accessed 03/02/20)
[64] David Sanger and David McCabe, "Huawei Is Winning the Argument in Europe, as the US Fumbles to Develop Alternatives" *The New York Times* (17 February 2020) <https://www.nytimes.com/2020/02/17/us/politics/us-huawei-5g.html?searchResultPosition=1> (accessed 29/03/20)
[65] John Hemmings, "The UK risks plunging the Five Eyes alliance into crisis" *The Telegraph* (4 March 2020) <https://www.telegraph.co.uk/politics/2020/03/04/uk-risks-plunging-five-eyes-alliance-crisis/> (accessed 20/06/20)

explanation for such statements beyond an attempt to impact the UK debate regarding Huawei's inclusion in 5G networks.

Effect of US Influence on the UK

In the UK, there is compelling evidence of discussions regarding the impact of US influence on the January 2020 decision. A former British National Security Adviser stated: 'you've had this crescendo of voices from Washington, trying with increasing stridency to put us off this decision. It put the Boris Johnson government into a difficult position: Did they defer to Trump's view or did they defy it? Anything other than approving it would have looked like caving into pressure.'[66] Liam Fox, former UK Defence Secretary, said there were fears in Washington that the UK's decision not to ban Huawei would 'give a green light' to other Western allies to follow suit.[67]

Stronger evidence was collected in the context of a discussion in the Commons Chamber on 27 January 2020. Crispin Blunt, a Conservative MP, argued that 'the strategic goal of our policy towards China must be interdependence, not isolation' and most importantly, 'unless the Americans can make a legitimate security case, we should quietly ignore their current public position that thinly disguises a protectionist trade position built on supposition, and proceed on the evidence. We should also gently let our American friends know that we are not leaving one dependent economic relationship on Friday to immediately enter another.'[68] In the same debate, MP Henry Smith stated, 'robust exchanges have obviously taken place with the

[66] Landler and Castle, "Johnson Risks a Rift with Trump"
[67] Helen Warrell and George Parker, "US attacks UK's decision on Huawei" *Financial Times* (28 January 2020) <https://www.ft.com/content/e3d38d0e-41c5-11ea-a047-eae9bd51ceba> (accessed 01/02/20)
[68] Parliamentary Proceeding, "5G Network and Huawei" *House of Commons* 670 cc533-536 (27 January 2020) <https://hansard.parliament.uk/Commons/2020-01-27/debates/038EF380-E4D6-4A6D-A0D8-0FAEB1D0A9B0/5GNetworkAndHuawei> (accessed 28/10/20)

United States and we know its opinions.'[69] This is strong evidence as it directly refers to the naming and shaming patterns of the US in potentially altering the course of UK policy.

Background Condition A: Behaviour of FVEY Members

In Step 1, evidence points to the background condition of the behaviour and potential pressure of other FVEY members. In February 2020 senior Australian MPs cancelled a planned trip to the UK due to tensions over the role of Huawei in the UK's 5G networks, as evidenced by leaked details of a high-level meeting during UK Foreign Secretary Dominic Raab's visit of Australia.[70] According to the leaked details, Australian Labour MP Anthony Byrne strongly criticised Mr Raab over British claims that they could safely allow Huawei to build the UK networks, stating: 'how would you feel if the Russians laid down infrastructure in your own networks? That's how we feel about Huawei.'[71] This evidence points to the presence of the variable of pressure from other FVEY members. However, the behaviour of the other FVEY members alone, without the presence of US influence, could not have led to the policy reversal. New Zealand remained ambiguous about its own stance on Huawei,[72] and Canada remained undecided about Huawei's involvement until 2022.[73] Additionally, UK intelligence officials directly addressed the lack of relevance of the FVEY alliance in their decision-making on Huawei. John Sawers, former chief of the UK Secret Intelligence Service, stated, 'we have much better coverage than any other western country, including, I might say, the United States,

[69] Parliamentary Proceeding, "5G Network and Huawei"
[70] BBC, "Huawei row: Australian MPs cancel UK trip amid tensions over leak" *BBC News* (15 February 2020) <https://www.bbc.com/news/world-australia-51513886> (accessed 31/03/22)
[71] Latika Bourke, "Australian MPs delivers stunning rebuke to UK's Dominic Raab on Huawei" *The Sydney Morning Herald* (7 February 2020) <https://www.smh.com.au/world/europe/australian-mp-delivers-stunning-rebuke-to-uk-s-dominic-raab-on-huawei-20200206-p53yjg.html> (accessed 31/03/22)
[72] Robert Ayson, "NZ's useful Huawei ambiguity" *Newsroom* (16 January 2020) <https://www.newsroom.co.nz/ideasroom/the-ban-that-isnt-new-zealand-and-huawei> (accessed 31/03/22)
[73] Amanda Connolly and Alex Boutilier, "Canada's Huawei decision was picking up momentum 2 years ago. So what is happening?" *Global News* (1 December 2021) <https://globalnews.ca/news/8414227/canada-huawei-ban-timeline/> (accessed 31/03/22)

for protecting ourselves against the threat of espionage from Chinese-made equipment.'[74] This indicates a lack of genuine security concerns. Overall, the behaviour and influence of other FVEY members, in conjunction with other background conditions interacting with US influence, were necessary for the outcome of the UK's policy reversal and ultimate ban of Huawei.

4.5.3. Step 2: Coercion Through Shared Norms and Values

US Influence

One of the first references to the West versus China discourse was made in the days after the UK's decision in 2020 January to retain Huawei by acting US Assistant Secretary of Defense David Helvey. He emphasised that the US and the UK should 'develop a common strategic understanding of the challenge and opportunity of China's rise' and warned of China's strategic advantage in key technologies, telecommunications, transportation and energy.[75] Helvey used terms such as the importance of staying 'unified' and thinking 'strategically' in order to avoid driving 'Beijing and Moscow closer' – clear referrals to a Western approach which had to counter hostile states. He ended with a stark warning: 'the transatlantic community must stand together to hold China accountable and refrain from transactional approaches that prioritise short-term economic gain over security and our open way of life', and 'the US and Europe must remain the guardians and sentinels of a stable, inclusive, rules-based order and draw upon shared strengths and principles to meet China's challenge to it.'[76]

More widely across the US, narratives on the importance of unity were present. A Republican congressional advisor stated: 'Britain is forcing us into a corner (…). We would

[74] Helen Warrell, Sebastian Payne and Nic Fildes, "UK ministers seek to placate Tory rebels over Huawei deal" *Financial Times* (13 March 2020).<https://www.ft.com/content/c8144666-6516-11ea-b3f3-fe4680ea68b5> (accessed 02/11/20)
[75] David Helvey, "Europe and the US must stand together on China" *Financial Times* (3 February 2020) <https://www.ft.com/content/a47faf4a-42b3-11ea-9a2a-98980971c1ff?shareType=nongift> (accessed 04/03/20)
[76] *ibid.*

rather the special relationship be renewed and revitalised in this new era of great power competition, but it is difficult to do when genuine security concerns were discarded.'[77] The term 'great power competition' is key in signalling the importance of choosing which side the UK will take. Moreover, US Senator Tom Cotton told UK lawmakers that China was using Huawei 'to drive a hi-tech wedge' between Britain and the US,[78] again pointing to the collective unit of Western states against China. This is strong evidence that at the highest levels of government, the US was attempting to influence the UK into banning Huawei by using language on their shared norms and values.

Effect of US Influence on the UK

In the UK, evidence of narratives on Western unity were identified. Conservative MP Tobias Ellwood stated 'I don't think there's any harm in pursuing trade with China – but it must be on equal terms. We still remain in a strong position, but only if we operate collectively, internationally, in unison.'[79] Robert Hannigan, former head of British GCHQ, argued 'the democratic West has woken up late to its overdependence on a country whose values are diametrically opposed to it.'[80] Conservative MP Bob Seely argued that 'the relationship between the UK and China, and the world and China, and the United States and China, is fundamentally changing.'[81] Former officials warned that the maintenance of a FVEY standard of cyber-security in telecommunications 'is a vital strategic and security interest, the loss of which (…) might lead the UK being excluded from work on developing future technologies

[77] Ben Riley-Smith, "US spy planes could be pulled from Britain as White House conducts major Huawei review" *The Telegraph* (4 May 2020) <https://www.telegraph.co.uk/news/2020/05/04/us-spy-planes-could-pulled-britain-white-house-conducts-major/> (05/05/20)
[78] Reuters, "UK in 5G talks with suppliers from Japan, South Korea: source" *Reuters* (3 June 2020) <https://www.reuters.com/article/us-britain-huawei-tech/uk-in-5g-talks-with-suppliers-from-japan-south-korea-source-idUSKBN23A3CY> (accessed 03/06/20)
[79] Cooper, "Britain toughens stance on China"
[80] Adam Satariano, Stephen Castle and David E. Sanger, "UK Bars Huawei for 5G as Tech Battle Between China and the West Escalates" *The New York Times* (14 July 2020) <https://www.nytimes.com/2020/07/14/business/huawei-uk-5g.html> (accessed 18/07/20)
[81] Nakashima and Booth, "Britain bars huawei"

for intelligence collection.'[82] Iain Duncan Smith, leading the Tory rebellion, argued 'China is itself becoming a very unreliable and rather dangerous actor. This is not a country that is in any way managing itself to be a good and decent partner.'[83] This evidence however is not particularly strong, as there is no indication that these narratives were adopted as a result of US influence.

On the other hand, stronger evidence derives directly from Downing Street, which confirmed that during a call between Prime Minister Johnson and President Trump, Johnson had 'underlined the importance of like-minded countries working together to diversify the market and break the dominance of a small number of companies.'[84] This more powerfully points towards the effect of US influence on UK decision-making, due to the quote taken from direct communication between leaders of the two states. This evidence suggests that coercion through shared norms and values affected UK policymakers' discourse. In addition, Conservative MP Stuart Anderson, during a Defence Committee meeting in June 2020, asked a US congressman 'do you believe that we're heading for a clash of global ideology between China and the West?'[85] Turner's response was that 'China is on the move',[86] alluding to an affirmative response. Tory MP Sarah Atherton also asked a question which points towards anti-China rhetoric; 'what course is China plotting? What's it trying to achieve?'[87]

Industry actors, the media and academia also provide evidence of US influence in the UK's decision to ban Huawei, using language that emphasises norms and values. This evidence, whilst considered secondary as it does not directly derive from policymakers, may impact how

[82] Gordon Corera, "Huawei: UK prepares to change course on 5G kit supplier" *BBC News* (20 February 2019) <https://www.bbc.co.uk/news/technology-47305420> (accessed 03/03/20)
[83] Sylvia Hui, "UK-China ties freeze with debate over Huawei, Hong Kong" *AP News* (13 July 2020) <https://apnews.com/article/ab544e59150aa75dce22a4aff9c79d78> (accessed 15/07/20)
[84] Warrell and Parker, "US attacks UK's decision on Huawei"
[85] Laurie Clarke, "UK MP to US congressman: Huawei is already out of the 5G network" *New Statesman* (16 June 2020) <https://tech.newstatesman.com/security/uk-mp-us-congressman-huawei-5g-network> (accessed 21/06/20)
[86] *ibid.*
[87] *ibid.*

issues are framed domestic and globally. For example, Dr. Bragagni, CEO of a major UK cable manufacturer, acknowledged the influence of the US on the UK's decision-making process, despite emphasising the autonomy of the UK's decision-making. Newspapers and media outlets also emphasised the divide between the West and China on technology, with headlines and articles reading 'UK Bars Huawei for 5G as Tech Battle Between China and the West Escalates' (*New York Times)*,[88] 'Geopolitical tension between the US and China is the reason behind the review into the use of Huawei's technology' (*BBC News*),[89] and 'United States has pushed Johnson to reverse his January decision to grant Huawei a limited role in 5G.' (*Reuters*).[90] Academics in the UK also highlighted impact of the West versus China discourse, with Tim Stevens, a senior lecturer in Global Security at King's College London describing US actions as 'straight-forward bullying,' arguing that 'the transatlantic spat over Chinese tech giant Huawei continues to demonstrate why no country – even a swashbuckling entrepot like Britain – can ever act in its own interests without meeting resistance.'[91] These sources collectively reveal the influence of the US in the UK's decision-making process.

Background Condition B: Geopolitical Developments

The geopolitical developments at the time were a significant contributing factor to the effect of US influence on the UK. However, evidence shows that geopolitical developments alone were insufficient to influence the UK's policy outcome. For example, the deputy political editor of *Sky News* argued that the UK's policy U-turn 'is not a consequence, for instance, of the new security law governing Hong Kong; China's behaviour over the coronavirus outbreak; the

[88] Satariano, et. al., "UK Bars Huawei for 5G"
[89] Leo Kelion, "Huawei: Why the UK might hang up on 5G and broadband kit supplier" *BBC News* (10 July 2020) <https://www.bbc.co.uk/news/technology-53341080> (accessed 14/07/20)
[90] Paul Sandle and Guy Faulconbridge, "Britain set to ban Huawei from 5G, though timescale unclear" *Reuters* 13 July 2020.<https://www.reuters.com/article/us-britain-huawei/britain-set-to-ban-huawei-from-5g-though-timescale-unclear-idUSKCN24E0K3> (accessed 15/07/20)
[91] Tim Stevens, "Huawei and UK foreign policy" *UK in a Changing Europe* (21 July 2020) <https://ukandeu.ac.uk/huawei-and-uk-foreign-policy/> (accessed 01/09/20)

treatment of the Uighur Muslim minority in Western China or years of trade infractions.'[92] Some policymakers did point to the importance of geopolitical developments in determining the policy outcome of banning Huawei. Tom Tugendhat, chair of the House of Commons Foreign Affairs Select Committee, stated: 'the virus has clarified the choice. The cost of doing business with autocratic regimes is that you don't just import their technology, you also import their values and make yourself dependent on their politics.'[93] However, this statement was made in the context of discussions on the impact of US sanctions on the company, thus pointing again towards the relevance US influence as a necessary variable. Moreover, Tobias Ellwood, Conservative MP, argued that the persecution of the Uighurs, draconian laws in Hong Kong and obfuscation over the Covid-19 outbreak in Wuhan show 'the real face of China being exposed.'[94] Sir Iain Duncan Smith led the rebellion by the Tory MPs and argued that he was 'genuinely concerned that this country has got itself far too bound into a process in which we are reliant on untrusted vendors.'[95] Penny Mordaunt, another Conservative MP, said that the UK's decision to maintain Huawei in its networks was 'regrettable', adding that she thought 'the size and complexity of the problem we're trying to protect ourselves against is enormous.'[96] Tugendhat further wrote on Twitter at the time of the UK's January decision that the plan to maintain Huawei 'leaves many concerns and does not close the UK's networks to a frequently malign international actor.'[97]

This evidence points towards the importance of geopolitical developments as a favourable background condition for the UK's policy reversal on Huawei, but I maintain that it was jointly

[92] Sky News, "Huawei U-turn: Cyber attacks, levies and other possible repercussions of the UK's 5G move" *Sky News* (15 July 2020) <https://news.sky.com/story/huawei-u-turn-cyber-attacks-levies-and-other-possible-implications-of-the-uks-5g-move-12028238> (accessed 16/07/20)
[93] Helen Warrell and Nic Fildes, "UK review of Huawei eyes impact of US sanctions" *Financial Times* (1 June 2020) <https://www.ft.com/content/9e581ace-69ec-4a42-81c3-c28d2bb40aa1> (accessed 01/06/20)
[94] Laura Miller, "Inside Huawei's 5G implosion" *Wired* (21 July 2020) <https://www.wired.co.uk/article/huawei-uk-ban-5g> (accessed 08/08/20)
[95] BBC, "Huawei: Government wins vote after backbench rebellion" *BBC News* (10 March 2020) <https://www.bbc.co.uk/news/uk-politics-51806704> (accessed 08/05/20)
[96] Stewart and Sabbagh, "UK Huawei decision appears to avert row with US"
[97] Landler and Castle, "Johnson Risks a Rift with Trump"

sufficient with other background conditions and with the interaction with US influence as the necessary variable for the outcome. This is because the one may argue that the statements above were rhetorical instruments to justify the stance to remove Huawei from 5G networks. Whilst pointing to the aggressiveness of China on the world stage is an acceptable justification for a U-turn on the existing pro-Huawei policy, ceding to US pressure is not. Moreover, it is puzzling to think that Chinese authoritarianism only became a problem after the January decision to ban Huawei. In the years leading up to the decision to keep Huawei within the networks, China mishandled numerous other geopolitical developments. The diplomatic rift over Hong Kong did not emerge between January and July, but was rather a long-term issue, even during the 'golden decade' between the UK and China. UK policymakers would have been fully aware back in January that they were dealing with an authoritarian state whose response to global events would not match their own. Indeed, a senior UK intelligence official admitted that 'China's political behaviour just created a terrible climate, with Hong Kong, with the detention, mass incarceration and surveillance of the Uighurs in Western China, the pandemic, with all sorts of things, China's activities did not help' but, ultimately the ban of Huawei was a 'political choice between East and West.' Most importantly, this source stated that 'I urge you to see this in the context of, despite all the political noise, it was actually an inexplicable and unexplained decision by the Americans to put Huawei in the UK front and centre.' This evidence points towards US influence as a necessary variable for the UK's policy reversal, interacting with the favourable background condition of geopolitical developments.

4.5.4. Step 3: International Pressure leads to Domestic Pressure

US Influence

This step, which centres on the UK's domestic debate, also provides evidence of US influence through the need for UK policymakers to justify their actions to US policymakers.

Conservative MP Mark Francois, in June 2020, assured US congressman Mike Turner that Huawei was 'already out of the 5G network,' adding 'we just haven't ripped them out yet' and that the NCSC review was simply 'effectively a fig leaf.'[98] Moreover, MP Dominic Grieve stated during a parliamentary hearing: 'in light of the United States' position and the lack of clarity on entity classification, I entirely understand why the Secretary of State finds it difficult to make a decision at the moment.'[99] This is strong evidence of the existence of US influence a few days before the ban of Huawei, particularly as it would be in the interest of the UK policymakers not to emphasis the US' effect on internal decision-making.

The evidence of US attempts to influence UK policymakers was further revealed during an interview with a senior UK intelligence official, who recounted two specific anecdotes. First, the official described a situation where a US delegation 'shouted at us (the UK' regarding Huawei and conducted a briefing at the US embassy to vet telecommunications companies without informing the UK government. When confronted, the US delegation expressed surprise, asking 'how did you know we were doing this?' The second anecdote highlighted the US's active briefings with Members of Parliament, with one instance involving an MP reading from a briefing note bearing the US State Department logo. This evidence, obtained during an anonymised interview with an individual possessing extensive knowledge of the policymaking process, provides strong indications of US attempts to influence UK policymakers.

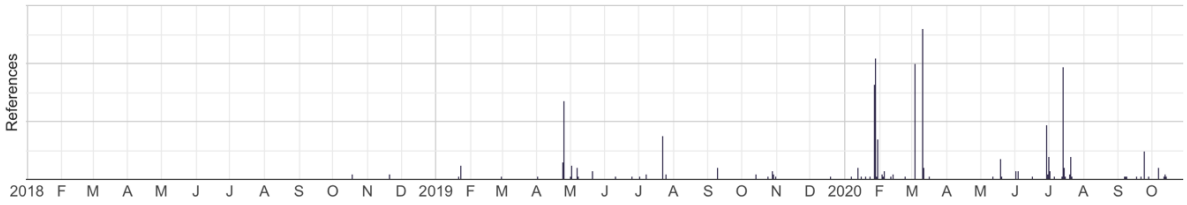
Effect of US Influence on the UK

Figure 7 shows the results of the number of references made to Huawei during parliamentary hearings between 1 January 2018 and 28 October 2020. There were 429

[98] Clarke, "UK MP to US congressman"
[99] Parliamentary Proceeding, "Telecoms Supply Chain" *House of Commons* Volume 663 (22 July 2019) <https://hansard.parliament.uk/Commons/2019-07-22/debates/7C7CE899-13EB-4C18-8678-44CB6CAA14F5/TelecomsSupplyChainReview?highlight=huawei%20american#contribution-4F9DB400-A3C6-4054-BA08-A1F588B19A9F> (accessed 28/10/20)

references in total and five debate titles. There is a notable peak of references towards the end of January, when Huawei involvement in 5G networks was approved, in March and in July, when the government performed a U-turn on its policy.

***Figure 2: References to Huawei in Parliamentary Hearings*[100]**



In March 2020, thirty-eight Conservative rebels backed an amendment to end Huawei's involvement in building 5G networks by the start of 2023; the government defeated this amendment.[101] Evidence indicating the relevance of international pressure leading to domestic pressure includes Tom Tugendhat's statement, the Tory chair of the Commons Foreign Affairs Committee: 'I think the mood in the parliamentary part has hardened and I think it's a shared realisation of what it means for dependence on a business that is part of a state that does not share our values.'[102] Sir Iain Duncan Smith, leading the Tory rebellion, argued that 'given that so many nations are saying no to Huawei, this should be an opportunity for us to prioritise national security over the breakneck speed with which the deployment of 5G is being pressed on us.'[103] By referring to the many nations which banned Huawei, he is clearly referring to the US and other intelligence-sharing allies, namely Australia and New Zealand, as at the time, no other European state had yet to fully ban the company. An academic with insight in the

[100] Retrieved from "Find references – Hansard" *UK Parliament*
[101] BBC, "Huawei: Government wins vote after backbench rebellion"
[102] E&T, "Tory rebellion threatens Huawei's future in 5G rollout" *Engineering & Technology Magazine.* (17 April 2020) <https://eandt.theiet.org/content/articles/2020/04/tory-rebellion-threatens-huawei-s-future-in-5g-rollout/> (accessed 17/04/20)
[103] Lizzy Buchan, "Boris Johnson facing Tory revolt over Huawei 5G decision" *The Independent* (6 March 2020) <https://www.independent.co.uk/news/uk/politics/boris-johnson-huawei-5g-decision-trump-tories-a9380561.html> (accessed 10/03/20)

policymaking process to ban Huawei also provided evidence of US influence, stating that 'with Donald Trump making lots of noises, given our special relationship with America, our government probably made a decision at that point to take two or three steps backwards.'

The following evidence strongly indicates the role of US influence in causing the rebellion in the UK. First, one leading rebel Tory, following the UK's decision to keep Huawei in its telecoms structure, stated: 'I think we're going to hear more pressure, not less, from the Americans – both in the Trump administration and Capitol Hill.'[104] Second, Sir Iain Duncan Smith, when addressing parliament in March 2020, remarked 'the government's decision to go ahead with Huawei in the 5G network in the UK – it is clear from the evidence – has angered our allies.'[105] Mr Owen Paterson, former Secretary of State for Environment, Food and Rural Affairs, agreed: 'we have infuriated the Americans and our other allies in the Five Eyes.'[106] Lord Ricketts, a member of the House of Lords, also argued that 'many American commentators seem to see the slightest role of Huawei in our system as an existential threat.'[107] The evidence is particularly strong as it would be in every interest of the policymakers to avoid referring to US influence, due to the perception that an external government influencing an internal decision.

Finally, a senior UK intelligence official claimed that 'the Conservative back-benching was basically about US pressure' and that the decision to ban Huawei 'was a political choice' as the MPs made it very clear that they trusted the NCSC and GCHQ to mitigate the risks, however that this was a 'just a straight-forward political choice between East and West and we're with America.' He added that no MP had ever taken interest in Huawei prior to 2019, despite its

[104] Warrell, et. al., "UK ministers seek to placate Tory rebels over Huawei deal"
[105] Parliamentary Proceeding, "Huawei and 5G", *House of Commons* 672 cc273-805WH (4 March 2020) <https://hansard.parliament.uk/Commons/2020-03-04/debates/9023564F-30E1-40C4-A9DE-E19DB8139E02/HuaweiAnd5G> (accessed 28/10/20)
[106] *ibid.*
[107] Parliamentary Proceeding, "UK Telecommunications" *House of Commons,* Volume 678(14 July 2020) <https://hansard.parliament.uk/Commons/2020-07-14/debates/9467A1F1-B87B-4E16-AD0C-DFF02A51981A/UKTelecommunications?highlight=huawei%20american%20united%20states#contribution-8548AC01-3C2B-454A-86EC-9BF841EFDB57> (accessed 28/10/20)

role in 4G and 3G systems. He claimed that 'a good chunk of the rebels were just there because they didn't want to be on the other side of the White House.' He also labelled US actions as 'bullying.' Finally, when asked whether the Tory rebellion would not have taken place if another US government administration had taken a favourable position to Huawei, he agreed it would not have and that there were a couple dozen rebel MPs which 'started shouting Huawei (and who previously) had never expressed the slightest interest in the subject.' This source would not have any other reason to be deceptive about this, given his anonymised status.

Background Condition C: The Interests of Domestic Actors

Evidence of US influence on domestic debate in the UK is clear. US influence in this step interacted with the favourable background condition of UK domestic actors' positions and interests. In January 2020, a number of MPs 'attacked the government's decision' to allow Huawei equipment in national 5G networks.[108] Former Conservative cabinet minister David Davis stated, 'the only way to protect our safety is to ban it,' and his backbench colleague Julian Lewis added that Huawei was 'intimately linked with the Chinese communist state and its deeply hostile intelligence agency.'[109] John Nicholson, member of the Scottish National Party, argued that the government had 'chosen low cost over security,' and his colleague, Carol Monaghan, argued that she did not know if this was 'naivety or arrogance preventing the UK government from seeing the high risk being presented to security.'[110] Labour's shadow culture secretary Tracy Brabin criticised the government for putting policymakers in 'the ludicrous position of having to choose between the UK's security concerns and our infrastructure needs.'[111] Sammy Wilson, member of the Democratic Unionist Party, asked for assurances

[108] BBC, "Huawei: MPs attack government over decision for 5G networks" *BBC News* (28 January 2020). <https://www.bbc.co.uk/news/uk-politics-51278305> (accessed 28/01/20)
[109] *ibid.*
[110] *ibid.*
[111] *ibid.*

from Foreign Secretary Raab that 'in the future (the UK will) not be as dependent on foreign technology.'[112] Moreover, Iain Duncan Smith, former leader of the Conservative Party, said it 'beggars belief' that the firm was given the green light 'when the UK had a cyber war going on with China.'[113]

However, domestic divisions could not have caused UK's policy reversal on Huawei on its own. This is supported by a senior intelligence official in the UK who claimed that one of the lessons of the technical briefings was that 'most of the MPs weren't interested in the technical reassurances' and said that 'if the Americans say you're wrong, you must be wrong.' He argued that 'putting Huawei into 5G didn't make (American) secrets any less safe, that's nonsense, you know all this "clean networks" stuff is just absolute nonsense, and no serious national security communications expert gives it the light of day.' This evidence strengthens the hypothesis of the necessity of US influence for the policy outcome.

4.5.5. Step 4: Threats Become a Reality (Coercive Threats)

US Influence

Initially, US threats to halt intelligence-sharing with the UK were not necessarily credible; US President Trump dismissed the threats during his visit to London in June 2019, assuring then-Prime Minister May of an agreement on Huawei.[114] In January 2020, a UK government official confirmed the security of intelligence sharing.[115] Secretary of State Mike Pompeo downplayed concerns about the Huawei decision harming bilateral ties, expressing confidence in working together to implement the decision.[116] The *New York Times* reported in February 17, 2020, that Britain had 'already called the Trump administration's bluff' and that it appeared

[112] BBC, "Huawei: MPs attack government over decision for 5G networks"
[113] *ibid.*
[114] Landler and Castle, "Johnson Risks a Rift with Trump"
[115] Gramer and Seligman, "Can the US-UK Special Relationship Weather the Huawei Storm?"
[116] *ibid.*

'to be paying no price for its decision to let Huawei into limited parts of its network.'[117] Foreign Secretary Dominic Raab stated that 'intelligence-sharing will not be put at risk and would not ever be put at risk by this government.'[118] A UK official emphasised that there was no reason for the US to lessen intelligence-sharing, as the decision to retain Huawei upholds the security of our 5G network.'[119] A senior UK intelligence official also claimed in an interview that 'there was never any serious threat to withhold intelligence-sharing,' adding that 'the Americans confirmed to us that there was no risk to classified communications sharing (…). That was all nonsense, there was no crisis in the Five Eyes.'

However, in May, the US imposed an export control[120] that cut Huawei off from a key source of semiconductors made with US technology, 'leading British officials to doubt they could count on the security of Huawei's equipment.'[121] Commerce tightened the export ban by amending the Foreign-Produced Direct Product Rule (FDPR)[122] and blocked overseas shipments to Huawei of foreign-made semiconductors made with US technology, meaning that, as explained by Dr Ian Levy, technical director of the NCSC, 'no-one, anywhere in the world, can send Huawei-designed chips to Huawei if US technology was used in the design tools or manufacture processes.'[123] Ciaran Martin, the former head of the NCSC, argued this

[117] Sanger and McCabe, "Huawei Is Winning the Argument in Europe"
[118] Stewart and Sabbagh, "UK Huawei decision appears to avert row with US"
[119] William Booth, Jeanne Whalen and Ellen Nakashima, "Britain, resisting US pressure, to allow some Huawei equipment in 5G networks" *The Washington Post* (28 January 2020) <https://www.washingtonpost.com/world/europe/britain-resisting-us-pressure-to-allow-some-huawei-equipment-in-5g-networks/2020/01/28/52e708b4-4145-11ea-99c7-1dfd4241a2fe_story.html>(accessed 31/01/20)
[120] Office of Public Affairs, "Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with US Technologies" *US Department of Commerce* (15 May 2020) <https://www.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts> (accessed 15/05/20)
[121] Nakashima and Booth, "Britain bars huawei"
[122] Bureau of Industry and Security, "Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List" *Department of Commerce,* Docket No. 200514-0100, RIN 0694-AH99 (15 May 2020) pp.29849-29863.
[123] Ian Levy, "A different future for telecoms in the UK" *National Cyber Security Centre* (14 July 2020) <https://www.ncsc.gov.uk/blog-post/a-different-future-for-telecoms-in-the-uk> (accessed 15/07/20)

measure was 'deliberately more targeted at Huawei's future ability to source hardware.'[124] This evidence affirms that the sanctions were a deliberate move to pressure the UK to ban Huawei.

According to reports in *The Telegraph*, the White House launched a review in May 2020 to determine whether spy planes, intelligence officials and other US assets were at risk due to Huawei involvement in the UK's networks.[125] This also shows the US' intentions to target the UK through coercive actions. Half a dozen sources 'including current US and UK officials' told *the Telegraph* that the review, which was not yet announced to the public, was 'underway, carrying potential ramifications for the special relationship' and that 'every military and intelligence asset the Americans have in Britain' was being re-assessed.[126] One former official stated: 'this was not a bluff. You cannot mitigate the danger Boris Johnson is exposing to the UK by letting Huawei into the network. This review is not a punishment. This is the White House saying, "okay, if they're going to go down this path and put themselves at risk then how do we protect ourselves."'[127] Senator Ben Sasse argued that the UK made the 'the right call' to remove the 'Chinese Communist spy ring out of their network,' strengthening the US-UK special relationship and joint efforts to expose threats.[128] However, his statement does not clearly indicate US intentions through coercive actions to change the UK's policy, making it less compelling evidence.

Effect of US Influence on the UK

The Observer published a report revealing that the British government 'privately told the Chinese technology giant Huawei that it was being banned from Britain's 5G telecoms network

[124] Nakashima and Booth, "Britain bars huawei"
[125] Justin Vallejo, "White House could pull US military and intelligence operations out of UK as part of Huawei review, reports say" *The Independent* (5 May 2020) <https://www.independent.co.uk/news/world/americas/huawei-review-white-house-uk-trump-boris-johnson-5g-network-a9498821.html> (accessed 05/06/20)
[126] Riley-Smith, "US spy planes could be pulled from Britain"
[127] *ibid.*
[128] Billy Perrigio, "Bowing to US Pressure, UK Bans 5G Equipment from China's Huawei over Security Concerns" *Time* (14 July 2020) <https://time.com/5866643/uk-huawei-5g-ban/> (accessed 15/07/20)

partly for geopolitical reasons following huge pressure from President Donald Trump.'[129] This strong evidence, derived from an investigative report, points to undisclosed developments, indicating the UK government's interest in concealing the information. The private nature of the reported internal conversations on the importance of US influence suggests a strategic approach, potentially aimed at avoiding angering the Chinese government.

Culture Secretary Oliver Dowden stated that 'the new US measures restrict Huawei's ability to produce important products using US technology or software' and that the NCSC concluded that 'the UK can no longer be confident it will be able to guarantee the security of future Huawei 5G equipment affected by the change in the US foreign direct product rules.'[130] The emphasis on the US forcing the UK's hand in this statement should be noted. Moreover, a source with insight into the Conservative party claimed that US influence drove the U-turn in the Huawei policy. The source also argued that the U-turn would probably not have occurred if not for the US sanctions, but added that in his opinion, it was highly likely that any other US administration would have taken a similar stance to the Trump administration. A senior UK intelligence advisor also claimed that 'the 2020 (US) sanctions were forensically brilliantly done and just left us with no choice,' adding that 'the Americans basically took out Huawei.' This confirms that US influence through coercive actions affected UK policymaking vis-à-vis Huawei.

Following the UK's policy reversal in July, US President Trump claimed credit, stating, 'I did this myself, for the most part.'[131] Senior Commerce Department official Robert B. Blair echoed Trump's sentiment, asserting they had 'scored a major victory' with Britain's decision.[132] However, President Trump's eagerness to claim victory may have been an attempt

[129] Toby Helm, "Pressure from Trump led to 5G ban, Britain tells Huawei" *The Guardian* (18 July 2020) <https://www.theguardian.com/technology/2020/jul/18/pressure-from-trump-led-to-5g-ban-britain-tells-huawei> (accessed 18/08/20)
[130] *ibid.*
[131] *ibid.*
[132] Satariano, et. al., "UK Bars Huawei for 5G"

to showcase his power over foreign affairs. In response, UK Health Secretary Matt Hancock dismissed Trump's claims, stating 'all sorts of people can try to claim credit for the decision, but this was based on a technical assessment by the (NCSC).'[133] Nevertheless, the NCSC's review of this decision was a consequence of the US's legal changes, once again pointing to the necessary condition of US influence.

Lord O'Neill, former Commercial Secretary to the Treasury, emphasised the lack of economic logic in the decision and compared it to the dilemmas that drove Brexit.[134] He added, 'if we are too influenced by the US – especially given American competition with China – it doesn't make sense.'[135] Labour MP Kevan Jones, former Defence Minister, also indicated that the decision was taken for 'geopolitical reasons' rather than considering the economic costs to the UK.'[136] Additionally, Priya Guha, a former British diplomat, stated that 'American sanctions left the UK with little choice,' describing it as 'checkmate by the US.'[137] Tobias Ellwood, Conservative MP, admitted that US sanctions that cut Huawei off from its American semiconductor suppliers were the 'game changer.'[138] Another UK official argued that the UK revisited its decision due to a campaign of 'unrelenting pressure' by the Trump administration.[139] Nick Macpherson, formerly the top official in the UK Treasury, suggested that the Huawei decision 'has little to do with national security and everything to do with the forthcoming lopsided US-UK trade deal.'[140] Dr. Ian Levy indicated that the US action led to a reassessment of the decision,[141] confirming the influence of US coercion on the UK's policy reversal. A senior UK intelligence official also confirmed that the US legal changes delivered the conclusive blow to Huawei's 5G involvement.

---

[133] Helm, "Pressure from Trump led to 5G ban"
[134] *ibid.*
[135] Ford and Hughes, "UK-China relations"
[136] Helm, "Pressure from Trump led to 5G ban"
[137] Satariano et. al., "UK Bars Huawei for 5G"
[138] Miller, "Inside Huawei's 5G implosion"
[139] Corera, "Huawei: UK prepares to change course"
[140] Cooper, "Britain toughens stance on China"
[141] Levy, "A different future for telecoms in the UK"

This evidence points to the effect of US influence through coercion on the UK's policy reversal. Additionally, media sources reported the UK was 'bowing to US pressure'[142] and that the 'US move gave UK convenient excuse for U-turn,'[143] indicating the impact of US influence on the UK's decision-making process. China's ambassador to the UK, Liu Xiamoing, and Chinese Foreign Ministry spokeswoman Hua Chunying expressed concerns about the UK's decision.[144] Their statements, whilst reflecting their roles, reveal the perception of the UK moving away from its pro-Chinese investments policy. This evidence, derived from Chinese officials, highlights the lack of market-driven logic in the UK's decision and the perception of the UK's shift in foreign policy.

4.5.6. Discussion

Prior to the onset of US influence in 2019, the first section indicates that UK policymakers acknowledged strategic concerns about retaining Huawei in 5G networks but generally maintained a consensus on approving Chinese involvement in CNI primarily for economic reasons. The process tracing sections presented strong evidence of US influence as the necessary variable in causing the policy outcome of the ban of Huawei in the UK's 5G networks. Importantly, US influence interacted with favourable background conditions in each step, rendering these a package of jointly sufficient causes.

In Step 1, the US engaged in naming and shaming, stirring uncertainty and indecisiveness among UK policymakers. US influence interacted with the behaviour of other FVEY members, evidenced by pressure on UK policymakers from Australian politicians. However, the behaviour of other FVEY members alone could not have caused the policy shift, as shown by

[142] Perrigio, "Bowing to US Pressure"
[143] Sky, "Huawei U-turn"
[144] James Landale, "UK Huawei decision part of wider strategic tensions with China" *BBC News* (12 July 2020) <https://www.bbc.co.uk/news/world-asia-china-53366301> (accessed 12/07/20); BBC, "Huawei: China attacks UK's 'groundless' ban of 5G kit" *BBC News* (15 July 2020) <https://www.bbc.co.uk/news/technology-53412678> (accessed 15/07/20)

the lack of evidence of pressure from other members aside from the US and Australia, and the UK's confidence in its ability to mitigate risks on its own. In Step 2, the US successfully engaged in coercion through shared norms and values, raising the risk of reputational costs for the UK. US influence interacted with the background condition of geopolitical developments at the time, including the COVID-19 pandemic and the increasing aggressiveness of Chinese foreign policy on the world stage as evidence by China's new security law for Hong Kong. US influence amplified the effect of geopolitical developments, but these developments could not have caused the policy reversal on their own.

In Step 3, there was substantial evidence pointed to the success of US influence leading to domestic pressure in the UK. The interaction with the final background condition, that of the interests of domestic actors, was evidenced through the large number of MPs attacking the government's decision to allow Huawei equipment in national 5G networks. At that time, without US influence, this rebellion was unsuccessful. Importantly, evidence was presented that MPs were uninterested in technical reassurances by the UK's own intelligence apparatus specifically due to US involvement. Finally, in Step 4, the US engaged in coercive actions and made its threats more credible, leading to a consensus among UK policymakers towards banning Huawei in its national 5G networks.

Overall, the process tracing sections show how US influence, intertwined with specific background conditions, formed a package of jointly sufficient causes leading to the UK's decision. Within this package, US influence emerged as causally more significant than the background conditions. However, it is important to recognise the limitation of this study: the absence of an alternative set of jointly sufficient conditions means I cannot rule out that US influence could have been sufficient without these specific conditions.

4.6. Broader Implications

In this article, I analysed the complex relationship between the US and the UK over the issue of Huawei and 5G technology. The effectiveness of US pressure on the UK was contingent on a unique set of background conditions, raising critical questions about the broader US approach to its allies in the context of US-China great power competition. Despite intense pressure from the Trump and Biden administrations,[145] Huawei still supplies over 50% of 5G equipment in 31 European countries,[146] including major players like Germany, Italy, and Spain. Even within the FVEY alliance, the US has faced challenges, as seen in Canada's delayed decision to ban Huawei.[147]

These varied responses across different allies reveal that the success of US influence is not a given but highly dependent on geopolitical and domestic circumstances. Furthermore, a glaring gap in the US strategy is the absence of coherent solutions to its allies' technological needs. This lack of alternatives and a tangible plan resonated with the sentiments of other European leaders,[148] reflecting a fragmented, or 'non-cooperative,' US approach. The 'non-cooperative' term here refers to an approach where the US prioritises pressuring its allies to align with its policies without offering adequate support or alternatives, undermining the potential for collaborative success in technological and security endeavours.

In conclusion, whilst the US has experienced limited success in influencing its allies' decisions regarding Huawei, this influence is highly conditional and not universally applicable. This inconsistency reveals a need for the US to rethink its strategy, not only in the context of Huawei but in its broader approach to technological competition and alliance management.

---

[145] John Strand, "Ban Huawei? Not Europe" *Center for European Policy Analysis (CEPA)* (12 January 2023) <https://cepa.org/article/ban-huawei-not-europe/> (accessed 11/04/23)
[146] *ibid.*
[147] Andy Blatchford, "Canada joins Five Eyes in ban on Huawei and ZTE" *Politico* (19 May 2022) <https://www.politico.com/news/2022/05/19/canada-five-eyes-ban-huawei-zte-00033920> (accessed 20/05/2022)
[148] Sanger and McCabe, "Huawei Is Winning the Argument in Europe"

Counterfactually, we could imagine a scenario where the US pursued a cooperative strategy that incentivises, rather than threatens, its allies. Instead of pressuring allies to reject Chinese tech, the US could have worked collaboratively to develop technological alternatives. This might have involved greater investments in joint technological research and development initiatives with key allies, focusing on fostering innovation in 5G and other critical technologies. Additionally, providing financial incentives for adopting alternative technology to Huawei could have aligned allies' interests more effectively with US objectives. The US could have offered favourable trade terms or subsidies to encourage the adoption of alternative technologies aligned with shared security interests. This collaborative approach could have signalled a commitment to strengthen alliances and provide attractive alternatives to Chinese offerings.

The varied reactions of US allies to the Huawei issue reveal that reliance on influence alone is often precarious and dependent on many specific and unpredictable factors. Therefore, a more effective strategy would emphasise collaboration and shared incentives. It is important to explicitly acknowledge that this discussion pertains to the strategies employed by the US to achieve its objectives, and that the pursuit of unilateral dominance does not necessarily align with normative principles. Whether allowing China to invest in CNI is "right" in any broader sense is a central question that underpins strategic studies on US-China great power competition but lie beyond the scope of this specific paper's analysis.

4.7. Conclusion

In conclusion, this paper demonstrated that US influence was a necessary but not sufficient condition in the UK's policy reversal on Huawei's involvement in its domestic 5G networks. The interaction of US influence with favourable background conditions, including the

behaviour of other FVEY members, geopolitical developments, and the position of domestic actors, played a crucial role in shaping the policy outcome.

The findings have important implications for the limits of US influence and its alliance management in the tech sector. Whilst I illustrate that US influence can significantly impact an ally's policy decisions under specific conditions, the effectiveness of this influence is not guaranteed and varies depending on the context and background conditions. This provides an avenue for further research into the configurations of favourable conditions for other allied states.

The UK's policy reversal on Huawei further brings to light critical questions about the broader US approach to its allies. The current non-cooperative approach, characterised by a reliance on influence without providing coherent technological alternatives, appears precarious and fragmented. This could indicate an ineffectiveness in alliance management in other technology-related developments, such as developing international norms and standards. European allies are essential to US tech leadership,[149] which could be severely undermined if the US maintains a coercive approach to alliance management.

Moreover, my findings reveal that in comparison to other sectors of CNI, the telecommunications sector is relatively novel, suggesting that the US has greater scope to diminish Chinese influence. This focus on digital infrastructure is consistent with the US strategic agenda to undermine China's technological superiority, and we can expect continued efforts to curtail Chinese presence in allied digital infrastructures. Overall, this paper contributes to understanding the role of allied influence in states' decision-making processes, elucidating how the US-China competition for technological primacy affects policy outcomes related to FDI in digital CNI sectors.

[149] Franz Oswald, "Soft balancing between friends: transforming transatlantic relations." *Debatte: journal of contemporary central and Eastern Europe* 14, no. 2 (2006): 145-160.

Appendix

The following table contains the positions of my interviewees and time of interview.

Table 1: List of interviews

Interviewee and Position	Time of Interview
Dr Maurizio Bragagni *CEO of Tratos UK* *Telecoms Industry Actor in the UK*	28 October 2020 (remote interview)
Background Source *UK Conservative Party Official*	31 October 2020 (remote interview)
Pseudonymised Source *Senior UK Intelligence Official*	6 November 2020 (remote interview)
Pseudonymised Source *Academic*	20 November 2020 (remote interview)
Background Source *Senior UK Intelligence Official*	9 December 2020 (remote interview)
Background Source *Senior UK Intelligence Official*	9 December 2020 (remote interview)
Background Source *Official in the UK Department for Business, Energy and Industrial Strategy*	26 January 2021 (remote interview)

5. Do Big Tech Companies' Geopolitical Postures Matter? Microsoft and Google's Conduct in China

Thesis Paper 3

Abstract

What explains the behaviour of Microsoft and Google in China? This article challenges the argument that these companies have geopolitical postures that drive their business interactions in third countries and that these postures are an independent factor in US-China strategic competition over technological superiority. Using a small-N case study comparison and process tracing through semi-structured interviews and secondary sources, I show that Microsoft and Google's decisions are primarily guided by rational profit maximisation under specific constraints: the individual company's business model, relevant Chinese legislation, and internal company structure. I argue that a company's geopolitical posture, as reflected in official policies and public statements, has no identifiable effect on decision-making in the Chinese market. This 'posture' may, in fact, be an outcome of addressing reputational concerns whilst maintaining flexibility in business interactions. The findings offer valuable insights into the complex dynamics between corporate strategy and international politics in the context of US-China relations.

5.1. Introduction

'Does Google have a corporate foreign policy and, if so, what does it look like?'[1] This question, posed to a Google executive during a United Kingdom Foreign Affairs Committee enquiry, encapsulates the central question of this paper: do private sector agents, such as tech companies, have meaningful geopolitical postures? If the answer was "yes," we would expect these postures to explain crucial company decisions, such as whether a United States' company operates in China. This query is crucial in an era where Big Tech companies wield considerable influence and power.

Indeed, in recent years there has been an exponential increase in scholars', policymakers' and pundits' ascribing foreign policies, or geopolitical postures more broadly, to actors in the technology private sector. This argument has emerged predominantly due to growing public perceptions of the influence and power that Big Tech companies have garnered, with claims being made that the companies like Facebook and Google have 'powers approaching or surpassing those of many countries.'[2] Policymakers in various states are calling for tech embassies to be established in Silicon Valley,[3] as well as expressing concerns on companies' growing influence.

In this paper, I investigate what explains variation in US Big Tech companies' behaviour in China, focusing on Microsoft and Google as case studies. I define geopolitical posture as a set of purposely crafted and defined *a priori* policies, or code of conduct, intended to inform and influence a company's decisions, constraining its behaviour vis-à-vis its business interactions in third countries. I assess the postures using the benchmark of whether the

[1] Foreign Affairs Committee, "Oral Evidence: Tech and the future of UK foreign policy, HC 201" *House of Commons* (2 November 2021) <https://committees.parliament.uk/oralevidence/2955/pdf/> (accessed 10/11/21)
[2] The Economist, "Democracies must team up to take on China in the technosphere" (19 November 2020) <https://www.economist.com/briefing/2020/11/19/democracies-must-team-up-to-take-on-china-in-the-technosphere> (accessed 30/10/21)
[3] Foreign Affairs Committee, "Oral Evidence: Tech and the future of UK foreign policy, HC 201" *House of Commons* (7 September 2021) <https://committees.parliament.uk/oralevidence/2662/pdf/> (accessed 09/11/21)

company explicitly refers to the US government as a partner and source of its outlook. Consequently, I class them as either aligned, apolitical, or non-aligned.

This study's universe of cases comprises the US 'Big Five' tech companies: Microsoft, Amazon, Google (Alphabet), Facebook (Meta), and Apple. Of these, I identify Microsoft and Amazon as aligned with the US government, Google and Facebook as non-aligned, and Apple as apolitical. Despite their varying stances, in this paper I narrow my scope to Microsoft and Google, categorised as aligned and non-aligned respectively based on their public affiliation with the US government. Through a small-N case study comparison, using semi-structured interviews and secondary sources to carry out within-case process tracing, I find that their geopolitical postures have no influence on their business decisions in China. Instead, I show that each company's decision-making in China was led by rational profit maximisation under constraints, which include the companies' business models, relevant Chinese legislation, and the company's internal structure.

I focus on US-based Big Tech companies due to the lack of scholarly analysis of Western companies' role in US-China strategic competition as opposed to Chinese companies, for which much more literature is available.[4] I narrow my empirical focus to Microsoft and Google for multiple reasons. First, both companies significantly contribute to the S&P 500 by market capitalisation,[5] and are instrumental in sociocultural evolution, fulfilling the criteria of market power and influence.[6] Second, the contrasting geopolitical postures of these companies – Microsoft as aligned and Google as non-aligned – present a juxtaposition for investigating the influence of such postures in their China strategies. Third, the diversified product offerings and

[4] See William J. Norris, *Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control*. Ithaca, NY, 2016 and James Reilly, *Orchestration: China's Economic Statecraft Across Asia and Europe*. Oxford University Press, 2021.
[5] Andrew Bary, "Big 5 Tech Stocks Now Account for 23% of the S&P 500" *Barrons* (26 July 2021) <https://www.barrons.com/articles/big-tech-stocks-sp-500-51627312933?tesla=y> (accessed 03/01/22)
[6] Nicolas Lekkas, "GAFAM: The Big Five Tech Companies Facts (FAAMG)" *GrowthRocks* (18 August 2021) <https://growthrocks.com/blog/big-five-tech-companies-acquisitions/> (accessed 03/01/22)

business models between Microsoft's software and cloud services and Google's search and advertisement operations offer an opportunity for understanding how these variables interact with their decision-making vis-à-vis China. Fourth, their varying degrees of dependence on the Chinese market and supply chain allow a thorough comparative analysis. Finally, both companies are subject to high levels of public and internal scrutiny. This enables an in-depth analysis of whether those external pressures reflect the company's own projected code of conduct.

My findings reveal that the behaviour of US Big Tech companies in China is not guided by geopolitical postures but by rational profit maximisation within specific constraints. This insight has several implications. Normatively, whilst these findings do not necessarily suggest a misalignment with US government preferences, they do suggest that the absence of geopolitical postures could lead to engagement in non-liberal practices, including potential complicity in authoritarianism and human rights abuses. As Jacob Helberg, a former policy adviser at Google, observed, 'a company's policies, like a society's laws, reflect its most basic values.'[7] Consequently, complying with the dictates of the Chinese Communist Party may position these policies in conflict with American values.[8] Ethically, this dilemma challenges Silicon Valley idealists to reconcile their companies' proclaimed values with their value-neutral products.[9] Strategically, the findings suggest that alignment between a tech company and the United States government is contingent on the company's ability to be profitable in China. The different geopolitical postures of tech companies pose a unique challenge for the US compared to China with its own tech champions. If the US seeks to engage these companies in its competition with China, it might consider employing policy tools such as tariffs, export

[7] Jacob Helberg, "Silicon Valley Can't Be Neutral in the US-China Cold War" *Foreign Policy* (June 22, 2020) <https://foreignpolicy.com/2020/06/22/zoom-china-us-cold-war-unsafe/> (accessed 04/12/21)
[8] Ian Bremmer, "The Technopolar Moment: How Digital Powers Will Reshape the Global Order." *Foreign Affairs* (New York, N.Y.) 100.6 (2021): 112-28.
[9] *ibid.*

controls, and investment restrictions.[10] However, these measures come with their own set of complications and costs.

The paper is organised as follows: first, I review existing literature on the geopolitical postures of tech companies, and then outline theory and methods. Subsequently, I present an overview of the study's universe of cases, followed by in-depth case studies of Microsoft and Google. In the case study sections I employ process tracing, drawing on elite interviews as well as secondary sources including official documents, public hearings, and media reports.

5.2. Literature Review

Scholars, pundits, and policymakers have increasingly equated tech companies to political actors. Tobias Feakin, Ambassador for Cyber Affairs and Critical Technology at the Australian Department of Foreign Affairs and Trade, argued that tech companies are 'growing to extraordinary levels and sizes, and having the kind of influences on our societies that I imagine many governments could only dream of.'[11] This perception derives from the idea that Big Tech exercises a form of sovereignty over digital space, and thus governments eye global tech companies as 'proxies – and potential targets – of their respective national power.'[12] Indeed, a British Member of Parliament admitted that his constituents were frightened by such companies due to their ability to make 'decisions that take on democratic governments.'[13] Consequently, companies within the tech industry are said to be 'new superpowers.'[14]

[10] Jon Bateman, "Biden is Now All-In on Taking Out China" *Foreign Policy* (12 October 2022) <https://foreignpolicy.com/2022/10/12/biden-china-semiconductor-chips-exports-decouple/> (accessed 12/10/22)
[11] Foreign Affairs Committee, "Oral Evidence" (7 September 2021)
[12] Helberg, "Silicon Valley Can't Be Neutral in the US-China Cold War"
[13] Foreign Affairs Committee, "Oral Evidence" (2 November 2021)
[14] Klon Kitchen, "The New Superpowers: How and Why the Tech Industry is Shaping the International System" *National Affairs,* Number 29 (Fall 2021) <https://nationalaffairs.com/the-new-superpowers-how-and-why-the-tech-industry-is-shaping-the-international-system> (accessed 29/11/21)

As new political actors, tech companies have been ascribed geopolitical postures by policymakers. For example, Anne Marie Engtoft Larsen, Tech Ambassador at the Ministry of Foreign Affairs in Denmark, argued that tech companies are 'as different from each other as countries' as they have 'different business models, different corporate cultures and different levels of maturity.'[15] The political differences between companies is often mentioned: 'while Microsoft has a mentality in which national sovereignty still trumps ethical arguments (…) Google is trying to balance the rights of sovereignty against its own evolving set of values.'[16] Variation in US tech companies' approaches towards foreign states have been linked to the companies' origins: 'it's no accident that Microsoft was founded during the cold war while Google was founded after the cold war.'[17] Tech companies are also pointing fingers among themselves for value-driven explanations of their business interactions, with Palantir CEO Alex Karp stating, in November 2021, that companies should work where they can 'ethically justify' and if they 'want to work in China or in any other country that is adversarial (to the US)' they should 'disclose it and defend it.'[18] In the US, the view that tech companies are 'eroding the line between political and commercial'[19] has become widespread. Simultaneously, the political agency of tech industry practitioners can be discerned by the circulation in the Biden administration of a report published by the China Strategy Group, a bipartisan group which includes academics, former policymakers, engineers, venture capital investors and technology executives. The report advances policies that position the United States to 'out-compete China'

[15] Foreign Affairs Committee, "Oral Evidence" (7 September 2021)
[16] Mark Landler, "Google Searches for a Foreign Policy" *New York Times* (27 March 2010) <https://www.nytimes.com/2010/03/28/weekinreview/28landler.html> (accessed 04/11/21)
[17] *ibid.*
[18] Samantha Subin, "Palantir CEO says companies working with US adversaries should justify their position" *CNBC News* (23 November 2021) <https://www.cnbc.com/2021/11/23/palantir-ceo-companies-working-with-us-adversaries-should-justify-their-position-.html> (accessed 02/12/21)
[19] Gregory F. Treverton and Pari Esfandiari, "Viewing tech giants as a geopolitical force" *The Hill* (31 January 2020) <https://thehill.com/opinion/technology/480823-viewing-tech-giants-as-a-geopolitical-force> (accessed 15/11/21)

and proposes the creation of a new multilateral forum, named the T-12, 'to strengthen cooperation among like-minded countries.'[20]

Despite the increased interest in the topic, theorisation on companies' geopolitical postures has hitherto been informal, with a clear lack of understanding and empirical testing of what it means to have such a posture. Ian Bremmer introduced a broad theorisation and categorisation of geopolitical postures by classifying tech companies into different worldviews: globalism, nationalism and techno-utopianism.[21] Bremmer's argument was criticised by Stephen M. Walt who countered that such distinctions were futile, as Big Tech will always be 'backstopped' by rules enacted and enforced by governments.[22] On a broader level, Stephanie Hare has explained that after former US National Security Agency contractor Edward J. Snowden revealed US intelligence agencies' mass surveillance of Americans and non-Americans, companies 'have tried to convince their customers within and outside the United States of their independence from the US government, to varying degrees of success.'[23] Other scholars have focused on single case studies to identify geopolitical positioning. Nancy Ayer Fairbank argued that Microsoft seems to be seeking an 'expansion and consolidation of its role as a quasi-public actor.'[24] ShinJoung Yeo instead analysed the 'geopolitics of search' through the case of Google's struggles in China, arguing that the 'structure of political economy that animates relations between Google, the US, the transnational Internet industry, and China is, in fact, suggestively ambiguous by illuminating the changing dynamics of the US-led trans-

[20] China Strategy Group, "Asymmetric Competition: A Strategy for China and Technology: Actionable Insights for American Leadership" (Fall 2020) <http://industrialpolicy.us/resources/SpecificIndustries/IT/final-memo-china-strategy-group-axios-1.pdf> (accessed 12/10/21)
[21] Bremmer, "The Technopolar Moment"
[22] Stephen M. Walt, "Big Tech Won't Remake the Global World Order" *Foreign Policy* (8 November 2021) <https://foreignpolicy.com/2021/11/08/big-tech-wont-remake-the-global-order/> (accessed 27/12/21)
[23] Stephanie Hare, "For Your Eyes Only: U.S. Technology Companies, Sovereign States, and the Battle over Data Protection." Business Horizons 59.5 (2016): 549-61. p.551
[24] Nancy Ayer Fairbank, "The State of Microsoft?: The Role of Corporations in International Norm Creation." *Journal of Cyber Policy* 4.3 (2019) p.397

nationalising capitalism.'[25] In other words, Yeo explains that Google's case reveals the fragility and volatility of the US-dominant information and communication, to which the US is responding by 'retooling and readjusting to accommodate China.'[26] Although this perspective maintains the view of companies as tools or victims of geopolitical dynamics, it moves away from a state paradigm and introduces the importance of the 'trans-nationalised global economy' as shaping the political dynamics between the US and China rather than the other way around. This provides an insight on the companies' motivations to retain independence, at least in public framing, from the US government.

The existing theorisations of geopolitical postures of tech companies are insufficient in providing a benchmark towards which one can analyse their behaviour in third countries. If companies have geopolitical postures, there must be indications of the ways in which such postures constrain their behaviour. In this paper, I will address the existing literature gap by identifying the indicators of a geopolitical posture and test its effect on corporate decision-making in the tech industry.

5.3. Theory and Methods

5.3.1. Geopolitical Postures

Despite the increase in discourses on Big Tech geopolitical postures, there is very little theorisation of what it means. In this paper, I define geopolitical posture as a set of purposely crafted and defined *a priori* policies, or code of conduct, intended to inform and influence a company's decisions, constraining its behaviour vis-à-vis its business interactions in third countries. Given that my universe of cases encompasses US-based technology companies, a

[25] Yeo ShinJoung, "Geopolitics of search: Google versus China?." *Media, Culture & Society* 38, no. 4 (2016): 591-605. p.592
[26] *ibid.* p.601

useful benchmark to identify their geopolitical postures is the extent to which they clearly espouse and claim to act in accordance with their host government's foreign policy. US foreign policy towards China is not static and varies according to numerous variables such as the specific issue being tackled, the administration currently in power, and volatile geopolitical conditions. Therefore, rather than theorising the extent to which the companies' outwardly stated principles are aligned with broad conceptions of democracy and liberal ideals, or of the balance between competition and cooperation in different areas of US foreign policy vis-à-vis China, the most useful analytical benchmark is whether the company explicitly refers to the US government as a partner and source of its outlook.

I rely on three sources to identify whether a company has a defined geopolitical posture, and how closely it refers to the US government as its authority. The first is official company policy, often referred to by a firm as its 'core values' or as 'corporate social responsibility', for which I carry out content analysis of specific references to the firm's conduct in foreign states. The second is public statements, predominantly by CEOs or employees in leadership roles which speak on behalf of the company rather than expressing personal inclinations and opinions. I carry out content analysis to identify clear references to policies and principles guiding company behaviour in China and as well as cooperation with the US government in this realm. Finally, the third source I selected to assess geopolitical postures is the quantity and nature of the company's partnerships with different branches of the US government. An identification of the empirical public-private partnerships allows for the analysis of proximity to the US government to be less skewed by unfounded public rhetoric based on reputational concerns – the so-called smoke and mirrors. However, this third source is only useful in the context of the other two indicators of geopolitical postures, as it cannot in itself reveal whether a company has purposely crafted and defined policies which affect its decisions vis-à-vis business interactions in China. All the five Big Tech companies have profited in the past decade

from contracts and subcontracts with the Department of Homeland Security, especially during the war on terror between 2007 and 2019. However, interesting patterns emerge: 'Amazon and Microsoft have benefitted the most from this increase: from 2015 to 2019, Amazon saw a 400 percent increase in all federal contracts, while Microsoft enjoyed an 800 percent increase.'[27]

Based on these sources, I examine whether a company's geopolitical posture can be identified, what it consists of, and how closely aligned to the US government it is. The next step is to assess the extent to which this geopolitical posture influences the company's decision-making and business interactions in China. The first factor that should be considered is a temporal one; that is, whether the identified policies were devised and expressed prior to the relevant decision-making analysed in China, such as an exit from the market or attempts to re-enter. Secondly, the effect of a geopolitical posture can be identified by analysing whether decisions were taken that do not reflect profit maximisation but rather are in line with its geopolitical posture. In other words, in the presence of a devised geopolitical posture, the company took a decision on its operations in China which it would not have done if it had followed a purely rational, profit maximising under constraints path. Finally, if the company does operate in China, we can observe whether its geopolitical posture affects its relationship to the Chinese Communist Party (CCP). Most importantly, the quantity and form of concessions made to the CCP in order to retain access to the Chinese market provide a good indication of the trade-off between value-driven considerations and profit maximisation.

Given the analytical benchmark of referring to the US as a partner and source of outlook, I theorise that geopolitical postures between the five Big Tech companies range between: (1) aligned, which means that the company has a clear code of conduct in foreign states and these are explicitly linked to the US government in both rhetoric and practice; (2) non-aligned, which

[27] Edward Ongweso Jr., "Big Tech Has Made Billions Off the 20-Year War on Terror" *Vice* (9 September 2021) <https://www.vice.com/en/article/4aveeq/big-tech-has-made-billions-off-the-20-year-war-on-terror> (accessed 18/01/22)

means that companies specify their own code of conduct in foreign states, but do not explicitly identify themselves as being tied to the US government in rhetoric and practice; and finally, (3) apolitical, with no clear references to any code of conduct in foreign states in the company's business interactions with third states.

5.3.2. Rational Profit Maximisation Under Constraints

The alternative explanation to geopolitical postures as explanations for private sector behaviour in China is that of profit maximisation under constraints, which can be modelled using rational choice theory. Rational choice theory is a methodological approach which explains individual and collective outcomes as 'individual goal-seeking under constraints.'[28] The aim of the theory is to identify, given one's preferences (considered fixed and exogenous), existing payoffs and constraints, what they *should* do, what the choice should be for the purpose of profit maximisation. Employing rational choice theory as devised by IR scholars as opposed to other disciplines such as economics is relevant in the context of treating firms as a form of actor engaging in geopolitical dynamics, along with other non-state and state actors. Rational choice models are particularly useful in this context as they contain no *a priori* prescription of goals or motivations, and therefore provide flexibility in the identification of the actor's goals.

The hypothesis that behaviour in China is driven by rational profit maximisation under constraints assumes that companies have inherently distinct incentives compared to states, which are broadly security or power seeking. Some scholars who have analysed the role of non-state actors as norm entrepreneurs point out that their analyses clash with conceptions of corporations as profit driven.[29] It is argued that 'private companies are becoming increasingly

[28] Duncan Snidal, "Rational Choice in International Relations", in Walter Carlsnaes, Thomas Risse and Beth A. Simmons, eds. *Handbook of International Relations,* 2nd ed. London: Sage, 2013, pp.85-111. p.87
[29] Fairbank, "The State of Microsoft?"

involved in international norm emergence'[30] possibly to retain legitimacy and public support. However, profit and growth are the existential priority for a company and thus can be assumed to be the object of maximisation.

The constraints that firms face as they operate in a third country are numerous, but I identify three as the most relevant for my chosen case studies. Geopolitical postures themselves are not considered one of the constraints as there is no evidence to indicate that any of these firms have been targeted by the CCP due to any kind of political standing on their part. In other words, the political alignment or stance of these companies in the global context has not translated into barriers or limitations within the Chinese market, making them irrelevant to the specific constraints they face in this environment.

The first constraint is a firm's business model, which is relevant in shaping the way that it can operate in the Chinese market. For example, if there is sufficient appeal within the Chinese market for its products and services, or if there is a competitive environment with debilitating effects for the firm. The second constraint is Chinese legislation or policies directly affecting the firm's ability to operate within the market. There may be an outright ban of the firm or of the firm's specific activities, which render it impossible for the firm to stay within the market. These two constraints are highly interrelated; indeed, retaining access to the Chinese market is contingent upon the interaction of the business model of the individual firm and the subsequently relevant Chinese legislation. The laws and regulations that both domestic and foreign tech companies face in China are wide-reaching and constantly being bolstered. Some foreign competitors are outright blocked in China, through strict regulations on which websites and social media platforms are accessible in the country, 'blocked behind China's so-called "Great Firewall" of internet censorship.'[31] Notable examples are Facebook, blocked in China

[30] Fairbank, "The State of Microsoft?"
[31] Paige Leskin, "Here are all the major US tech companies blocked behind China's Great Firewall" *Business Insider* (10 October 2019) <https://www.businessinsider.com/major-us-tech-companies-blocked-from-operating-in-china-2019-5?r=US&IR=T> (accessed 03/01/22)

since 2009, and Google, as YouTube was blocked permanently in 2009 and its China-based search engine was shut down in 2010.[32] However, this does not mean that these companies do not operate in China at all – Facebook had an estimated $5 billion in ad revenue from Chinese-based companies in 2018 and as will be further analysed in the case studies, Google has engaged in projects to develop a censored search engine for Chinese users and other services remain in the market.[33]

Other companies face swathes of different legislation. China's first privacy law, the Personal Information Protection Law (PIPL) came into effect on November 1st 2021, allowing the government to enforce 'vague rules as it sees fit' and broadly requires 'tech firms to write code for their platforms so that they promote content that the government likes, and inhibit what it does not.'[34] Throughout 2021, we have seen efforts from China's central bank to 'mitigate systemic risks posed by the rise of fintech; the cyberspace regulator to rein in data privacy abuses; and a push by the market regulator to end anti-competitive practices by platform companies.'[35] There is relevant legislation to each individual company which will be laid out in the case studies.

The third constraint is the company's internal structure, focusing on adherence to ethical standards and corporate culture. Whilst these constraints may appear similar to geopolitical posture, they differ in their emphasis on ethical considerations and organisational values rather than political factors. Adherence to ethical standards, rooted in a long history of business ethics,[36] and corporate culture can indirectly impact a company's financial success by

[32] Leskin, "Here are all the major US tech companies blocked behind China's Great Firewall"
[33] *ibid.*
[34] The Economist, "China has become a laboratory for the regulation of digital technology" (11 September 2021) <https://www.economist.com/china/2021/09/11/china-has-become-a-laboratory-for-the-regulation-of-digital-technology> (accessed 03/01/22)
[35] Vincent Ni, "TechScape: Xi Jinping's 'Little Red Book' of tech regulation could lead the way" *The Guardian* (3 November 2021) <https://www.theguardian.com/technology/2021/nov/03/techscape-china-jack-ma-regulation> (accessed 03/01/22)
[36] Betsy Stevens, "Corporate ethical codes: Effective instruments for influencing behavior." *Journal of Business ethics* 78 (2008): 601-609.

enhancing its reputation, fostering customer loyalty, and promoting employee satisfaction. However, when these standards conflict with profit-driven activities, they impose limitations on the company's ability to maximise profit. Additionally, a company's culture can significantly influence its actions. If the majority of employees oppose a particular business move, it can effectively constrain the company's profit-making activities. Employee activism, defined as coordinated action by employees to address societal problems connected to the company they work for,[37] can exert substantial influence. For example, Google's Project Dragonfly, involving the development of a censored search engine for Chinese users, faced significant internal opposition.[38] Employee activism has also targeted domestic partnerships, such as protests against the company's involvement in a Pentagon programme aimed at using AI to improve drone strikes.[39] Whilst the long-term impact of employee activism on business decisions is debatable, it remains an external constraint on companies' profit-making activities, particularly in the context of ethical concerns surrounding Chinese government's censorship and surveillance practices. Therefore, adherence to ethical standards and employee activism are crucial factors constraining companies' profit maximisation strategy in China, distinct from the company's geopolitical posture. In the case of US tech companies operating in China, employee activism is a particularly important constraint due to the ethical concerns surrounding the Chinese government's censorship and surveillance practices.

[37] Forrest Briscoe and Abhinav Gupta, "Business Disruption From the Inside Out" *Stanford Social Innovation Review* 19, no. 1 (2020): 48-54. p.48
[38] Reuters, "Google employees push to stop Project Dragonfly" *Reuters* (27 November 2018) <https://www.reuters.com/article/google-workers-idINL4N1Y23E8> (accessed 04/02/22)
[39] Scott Shane and Saisuke Wakabayashi, "The Business of War: Google Employees Protest Work for the Pentagon" *The New York Times* (4 April 2018) <https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html> (accessed 03/01/22)

5.3.3. Methods

The timeframe of this research must reflect the period in which the companies in the universe of cases were considered influential. At the same time, the scope of the investigation must be flexible enough to allow for a comprehensive analysis of patterns of behaviour within China. The focus is therefore on the period between 2010 and 2021, which encompasses the decade which was claimed to have marked the 'development of capitalism' with Apple, Amazon and Microsoft emerging as the world's first trillion-dollar companies.[40]

To test the hypothesis that geopolitical postures affected Big Tech firms' behaviour in China, in terms of whether the company operates in China and under what conditions, I employ process tracing. This method is defined as 'techniques for examining the intermediate steps in cognitive mental processes to understand better the heuristics through which humans make decisions.'[41] I collect Causal Process Observations (CPOs) and subject them to process tracing tests to assess the relevance of the hypotheses.

First, I provide a brief overview of the Big Five tech companies, Google (Alphabet), Apple, Facebook (Meta), Microsoft, and Amazon, covering the period from 2010 to 2021. This introductory analysis serves as a contextual foundation for the subsequent, more detailed examination. Subsequently, I present two case studies, first Microsoft then Google. For each case study, my first task is to identify the geopolitical postures through official company policy, public statements, and partnerships with the US. My second task is to identify and analyse significant decisions on business interactions in China in accordance with whether they follow a pattern of rational profit maximisation under the three constraints identified (business model, Chinese legislation, and company internal structure) or whether they can be explained by the identified postures. I chose to structure the analysis around individual business decisions rather

[40] Jay Owens, "The tech giants dominated the decade. But there's still time to rein them in." *The Guardian* (25 December 2019) <https://www.theguardian.com/commentisfree/2019/dec/25/2010s-tech-giants-google-amazon-facebook-regulators> (accessed 05/02/22)
[41] Andrew Bennett and Jeffrey T. Checkel, eds. *Process tracing*. Cambridge University Press, 2015. p.5

than individual constraints because each decision reflects a multifaceted interplay among various constraints. Simplifying this relationship would not accurately represent the complex dynamics at play.

The sources for this data are both primary data collected in semi-structured elite interviews,[42] and secondary sources including official company documents, public hearings, local media reporting and social media posts. The obstacles to data collection, particularly the elite interviewing process, required a heavy reliance on secondary sources. This was mainly due to difficulties accessing current employees and leading figures in the Big Tech industry and the risks associated with obtaining information that could jeopardise their careers. Fortunately, the nature of a geopolitical posture often requires public communication, making secondary sources a valuable resource.

5.4. Overview of Universe of Cases

In this section, I outline the universe of cases that constitute the Big Five tech companies: Microsoft, Amazon, Google (Alphabet), Facebook (Meta), and Apple. *Table 1* shows the geopolitical posture of each company and whether they operate in the Chinese market. For the sake of conciseness, *Table 1* only captures the presence or absence of each company in the Chinese market as the dependent variable (DV). This serves the purpose of showing the overarching pattern between geopolitical postures and presence in the Chinese market among the Big Five and justifying the case selection. The DV is further elaborated on for each company in the text of this section. Moreover, the subsequent in-depth case studies offer a more nuanced analysis by exploring specific decisions regarding the companies' presence or absence in the market.

[42] Ethical approval of research involving human participants was granted (Central University Research Ethics Committee Approval Reference: SSH_DPIR_C1A_21_053)

Microsoft and Amazon, categorised as *aligned*, demonstrate a history of collaboration with the US government through various partnerships and contracts. Microsoft's detailed geopolitical posture is further explored in the following section. Amazon's alignment is evidenced in its public statements,[43] and government contracts.[44] Google and Facebook, classified as *non-aligned*, developed their codes of conduct in foreign states independently of explicit alignment with the US government. The subsequent section delves deeper into Google's geopolitical posture. Facebook has a flexible operational code of conduct in third countries,[45] avoids public alignment with the US,[46] and shows little evidence of formal contracts with the US government.[47] Apple, categorised as *apolitical,* strategically avoids explicit alignment with any government. This is reflected in its limited public commentary on its conduct in foreign states,[48] and minimal evidence of high-profile partnerships with the US government.[49] The company's legal disputes with the US government over encryption policies reveal a restrained level of cooperation.[50]

---

[43] Richard Waters, "Jeff Bezos warns US military it risks losing tech supremacy" *Financial Times* <https://www.ft.com/content/b38c5cf6-198a-11ea-97df-cc63de1d73f4> (accessed 08/02/22)
[44] Sharon Weinberger, "Meet America's newest military giant: Amazon" *MIT Technology Review* (8 October 2019) <https://www.technologyreview.com/2019/10/08/75349/meet-americas-newest-military-giant-amazon/> (accessed 18/01/22); Allan Smith, "Impressive and a little scary: How Amazon and Jeff Bezos made Washington a second home" *NBC News* (6 September 2019) <https://www.nbcnews.com/politics/politics-news/king-hill-how-amazon-jeff-bezos-made-washington-second-home-n1033296> (accessed 18/01/22); Naomi Nix, "Amazon is Flooding D.C. with Money and Muscle: The Influence Game" *Bloomberg* (7 March 2019) <https://www.bloomberg.com/graphics/2019-amazon-lobbying/> (accessed 18/01/22)
[45] Facebook, "The Facebook Code of Conduct" <https://s21.q4cdn.com/399680738/files/doc_downloads/governance_documents/2021/06/FB-Code-of-Conduct.pdf> p.56 (accessed 07/02/22)
[46] Foreign Affairs Committee, "Oral Evidence: Tech and the future of UK foreign policy, HC 201" *House of Commons* (11 January 2022) <https://committees.parliament.uk/oralevidence/3247/pdf/> (accessed 11/01/22)
[47] *ibid.*
[48] The most recent mention of an explicit business strategy in the form of an official company policy was in Apple's 2018 annual report, which did not mention conduct in foreign states, but rather emphasised the aim of 'building and expanding its own retail and online stores and its third-party distribution network to effectively reach more customers.' Refer to: Apple Inc., *Annual Report Pursuant to Section 13 or 15(D) of the Securities Exchange Act of 1934,* United States Securities and Exchange Commission, Washington D.C. (2018)
[49] Danny Yadron, Spencer Ackerman and Sam Thielman, "Inside the FBI's encryption battle with Apple" *The Guardian* (18 February 2016) <https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple> (accessed 18/01/22)
[50] *ibid.*

In China, *aligned* companies like Microsoft and Amazon have shown adaptability, with practices such as source code sharing and technology licensing.[51] This conduct does not reflect their geopolitical postures. *Non-aligned* company Facebook made numerous attempts to re-enter the Chinese market,[52] whilst Google's stance has been fluctuating since 2010. Whilst this is in line with their geopolitical postures at a broad level, the in-depth case study in the next section shows that geopolitical posturing does not explain specific decisions. Apple, with its *apolitical* posture, has made significant concessions to the Chinese government,[53] likely influenced by its dependence on China for manufacturing and revenue. It is noteworthy that some companies perceived to be aligned with the US government, such as Microsoft and Amazon, have active operations in China. This observation counters intuitive expectations and strengthens my argument that a company's geopolitical posture does not necessarily prescribe its presence or behaviour in the Chinese market.

[51] Bethany Dawson, "Amazon booster its business in China by blocking reviews on books by leader Xi Jinping and following Communist Party 'edicts' says Reuters investigation" *Business Insider* (18 December 2021) <https://www.businessinsider.fr/us/amazon-collaborated-with-chinas-propaganda-arm-to-boost-sales-reuters-2021-12> (accessed 21/12/21)

[52] Paul Mozur, Mark Scott and Mike Isaac, "Facebook faces a new world as officials rein in a Wild Web" *The New York Times* (17 September 2017) <https://www.nytimes.com/2017/09/17/technology/facebook-government-regulations.html> (accessed 06/02/22); Lin Yang, "How Facebook's Zuckerberg Went from Courting to Criticising Beijing" *VOA News* (5 September 2020) <https://www.voanews.com/a/silicon-valley-technology_how-facebooks-zuckerberg-went-courting-criticizing-beijing/6195455.html> (accessed 21/12/21)

[53] Jack Nicas, Raymond Zhong and Daisuke Wakabayashi, "Censorship, Surveillance and Profits: A Hard Bargain for Apple in China" *The New York Times* (May 17, 2021) <https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html> (accessed 20/12/21); Reuters, "Tim Cook reportedly signed five-year $275bn deal with Chinese officials" *The Guardian* (7 December 2021) <https://www.theguardian.com/technology/2021/dec/07/apple-china-deal-tim-cook> (accessed 18/01/22); Mikey Campbell, "Peter Thiel calls Apple's relationship with China a real problem" *Apple Insider* (7 April 2021) <https://appleinsider.com/articles/21/04/07/peter-thiel-calls-apples-relationship-with-china-a-real-problem> (accessed 20/12/21); Wesley Hilliard, "Congress members demand Apple exit China in letter to Tim Cook" *Apple Insider* (21 May, 2021) <https://appleinsider.com/articles/21/05/21/congress-members-demand-apple-exit-china-in-letter-to-tim-cook> (accessed 18/01/22)

Table 1: US Tech Companies' Geopolitical Postures and Presence in Chinese Market

	IV: Geopolitical posture	DV: Operates in Chinese Market
Microsoft	Aligned	Yes
Amazon	Aligned	Yes
Google (Alphabet)	Non-aligned	No
Facebook (Meta)	Non-aligned	No
Apple	Apolitical	Yes

Overall, the relationship between a company's geopolitical posture and its operations in China is more complex than expected. Whilst *aligned* companies might be expected to have a more limited presence in China, the fact that Microsoft and Amazon have active operations in China suggests that other factors, such as rational profit maximisation, may play a more important role in shaping companies' decisions about whether or not to operate in China. *Non-aligned* companies would be expected to operate in the Chinese market, but their geopolitical postures should also explain their behaviour and individual decisions in the Chinese market. Therefore, further research into companies' behaviour in China is required to better understand the explanatory power of geopolitical postures. In the next two sections, I expound the in-depth case studies of Microsoft and Google to shed light on the mechanisms shaping their decision-making in the Chinese market. As I explained in more detail in the introduction, the reason for this focus includes their significant market power, contrasting geopolitical postures, diversified product offerings, different Chinese market dependencies, and the levels of public and internal scrutiny they undergo. In the case studies, I explore their strategies in China aiming to shed light on the mechanisms shaping their decision-making.

5.5. Case Study 1: Microsoft

5.5.1. Geopolitical Posture: Aligned

Microsoft broadly outlines its corporate 'values' as respect, integrity and accountability.[54] On its website, it displays its compliance offerings, law enforcement data requests, US national security orders report and international export controls.[55] On involvement in foreign states, it lays out its commitments to corporate social responsibility, stating 'we believe that companies that can do more, should' and explicitly state that 'we unequivocally support the fundamental rights of people, from defending democracy, to addressing systemic racial injustice and inequity, to protecting human rights.'[56] In terms of work with governments, it states that the company strives to 'earn the trust of our customers, employees, the communities we serve, and the governments that represent them through a commitment to privacy, security, the responsible use of AI, and transparency.'[57] The company also frames itself as an early supporter of the European Union's General Data Protection Regulation (GDPR).[58]

In terms of public statements, Microsoft has attempted to maintain good relations with Washington whilst encouraging the US government to maintain to improve their relationship with China. In September 2019, Microsoft President Brad Smith argued that Washington and Beijing must try to improve their relationship and address issues around technology exchanges.[59] Regarding the power that tech companies wield, Smith argued that they 'need to

[54] Microsoft, "Our corporate values" <https://www.microsoft.com/en-us/about/corporate-values> (accessed 22/12/21)
[55] Microsoft, "Empowerment begins with trust" *Trust Centre* <https://www.microsoft.com/en-us/trust-center> (accessed 22/12/21)
[56] Microsoft, "Corporate Responsibility" <https://www.microsoft.com/en-us/corporate-responsibility/> (accessed 22/12/21)
[57] Microsoft, "Our actions" <https://www.microsoft.com/en-us/corporate-responsibility/earn-trust?rtc=1> (accessed 22/12/21)
[58] *ibid.*
[59] Akito Tanaka, "US and China need to repair tech ties: Microsoft president" *Nikkei Asia* (9 September 2021) <https://asia.nikkei.com/Business/Technology/US-and-China-need-to-repair-tech-ties-Microsoft-president> (accessed 21/12/21)

assume a new level of self-responsibility and adapt to a future where we recognise that regulation is not only inevitable but, in fact, has an important role to play.'[60]

Microsoft has numerous partnerships with different parts of the US government. With the Department of Defence in particular, they have claimed to be a strong partner 'for more than 40 years' and have 'pledged to make available our best technology to support their mission.'[61] Microsoft was a finalist, along Amazon, for a single Joint Enterprise Defence Infrastructure (JEDI) contract, worth up to $10 billion over 10 years.[62] According to a report released by research groups Little Sis, Action Centre for Race and the Economy (ACRE), and MPower Change, Microsoft enjoys 'the coziest relationship with the federal government' from all the Big Tech companies.[63] It was reported that during the first two years of the Trump administration, 'Microsoft saw ties with the (Department of Homeland Security) skyrocket.'[64]

Overall, given the criteria set out on geopolitical postures in this research, Microsoft is a company which tends to refer to the US more explicitly as an official partner and source of its geopolitical outlook, in comparison to the other companies within the universe of cases. I therefore identify Microsoft's geopolitical posture as aligned. Due to its aligned geopolitical posture, I would expect Microsoft to show reluctance to engage with the Chinese market.

5.5.2. Microsoft's Behaviour in China

I analyse three of Microsoft's main decision-making processes on interactions with China: the concessions to and courtship of the CCP, LinkedIn's departure from China and the

[60] Tanaka, "US and China need to repair tech ties: Microsoft president"
[61] Toni Townes-Whitley, "Microsoft's commitment to the DoD remains steadfast" *Official Microsoft Blog* (6 July 2021) <https://blogs.microsoft.com/blog/2021/07/06/microsofts-commitment-to-the-dod-remains-steadfast/> (accessed 01/01/22)
[62] Jordan Novet, "Pentagon asks Amazon, Google, Microsoft and Oracle for bids on new cloud contract" *CNBC* (19 November 2021) <https://www.cnbc.com/2021/11/19/pentagon-asks-amazon-google-microsoft-oracle-for-cloud-bids.html> (accessed 20/11/21)
[63] Ongweso Jr., "Big Tech Has Made Billions Off the 20-Year War on Terror")
[64] *ibid.*

company's response to the Chinese state-based cyberattack of its Microsoft Exchange Server. I find that these examples reflect decision-making that was constrained predominantly by the company's business model, linked to relevant Chinese legislation.

Microsoft's business model produces less constraints in the Chinese market than other companies within the universe of cases. Due to the company's focus on selling to business customers rather than trying to tap customers, Professor Arun Sundararajan explained that 'it's been a lot easier for them to operate in China. The conflict of interest between Microsoft products and what the Chinese government is interested in controlling are minimal.'[65] According to a logic of rational profit maximisation under constraints, it therefore makes sense that 'Microsoft's ties in China is as tight as it gets in terms of an American tech company's presence and influence in China. It's not the most beholden to China in terms of revenue, but Microsoft has been an inspiration role model of sorts for China's tech scene since day one.'[66] What is particularly noteworthy is that China only accounts for around 10% of Microsoft's estimated $125 billion annual revenue.[67] China is therefore a less significant market for Microsoft, in comparison to the other four companies, and thus could be considered to have less incentives to make concessions to the CCP for the purpose of retaining full-fledged access to the Chinese market. Nevertheless, concessions to the CCP have been numerous. The fact that Microsoft has made numerous concessions to the CCP, despite its aligned geopolitical posture, suggests that geopolitical posture does not shape its decisions about whether or not to operate in China.

[65] Aaron Tilley, "Microsoft CEO Nadella Wades Into US-China Tensions in TikTok Pursuit" *Wall Street Journal* (4 August 2020) <https://www.wsj.com/articles/microsoft-ceo-nadella-wades-into-u-s-china-tensions-in-tiktok-pursuit-11596569063> (accessed 03/01/22)
[66] Hollie McKay, "Microsoft's three-decade history with China under the microscope ahead of potential TikTok acquisition" *Fox Business* (25 August 2020) <https://www.foxbusiness.com/technology/microsofts-three-decade-history-with-china-under-scrutiny-possible-tik-tok-acquisition> (accessed 21/12/21)
[67] *ibid.*

The Concessions to and Courtship of the CCP

Microsoft first entered the Chinese market in 1992. The company's co-founder, Bill Gates, has often sought to remain neutral and mediate between the US and China, at times has acted in a statesmanlike manner in relations with China. In January 2010, the Chinese Embassy in the US published a press report entitled 'Bill Gates bats for China'[68] as a response to the allegations of China's cyberattacks against Google. The report claimed that Gates had said 'that obeying local laws is a prerequisite for doing business in a foreign country.'[69] In 2015, President Xi Jinping visited the Microsoft headquarters in Redmond, received by Bill Gates and his wife.[70] In 2017, the company launched a 'customised variant of its Windows 10 software tailored for Chinese government use, complete with local encryption aimed to address "issues that matter" to its government customers.'[71] Microsoft also opened two research institutes for basic applied computer research and for the development of AI in China. In 2019, Microsoft came under scrutiny for its work with a Chinese military-operated university, as well as the fact that it enables the CCP to censor Bing, its search engine in China.[72] In February 2020, Xi wrote a personal letter of thanks to Gates for his cooperation during the COVID-19 outbreak.[73] In December 2021, Microsoft conceded to Chinese authorities' requests to suspend its search engine Bing's 'auto suggest function' for 30 days.[74] Overall, despite the Chinese market not representing an existential necessity for the company's profit and growth, there are numerous CPOs which indicate both concessions to and active courting of Chinese leadership.

[68] Embassy of the People's Republic of China in the United States of America, "Bill Gates bats for China" (27 January 2010) <https://www.mfa.gov.cn/ce/ceus/eng/xw/t654165.htm> (accessed 08/02/22)
[69] *ibid.*
[70] Vanessa Ho, "Chinese President Xi Jinping visits Microsoft, sees potential of new technology" *Microsoft News* (23 September 2015) <https://news.microsoft.com/features/chinese-president-xi-jinping-visits-microsoft-sees-potential-of-new-technology/> (accessed 21/12/21)
[71] McKay, "Microsoft's three-decade history with China under the microscope ahead of potential TikTok acquisition"
[72] *ibid.*
[73] *ibid.*
[74] Reuters, "Microsoft's Bing suspends auto suggest function in China at government's behest" (17 December 2021) <https://www.reuters.com/technology/microsoft-bing-says-suspended-auto-suggest-function-china-government-behest-2021-12-17/> (accessed 21/12/21)

This remains in line with the focus on profit maximisation at all costs, despite Microsoft's aligned geopolitical posture, which is closer to the US government than the postures of Google, Apple and Facebook.

LinkedIn's departure from China

Microsoft-owned LinkedIn professional networking service 'shut down' in China in October 2021, citing 'a significantly more challenging operating environment and greater compliance requirements.'[75] Is this evidence that the alignment with the US government on policies of conduct in foreign states matters after all? I will argue that it is not. LinkedIn had offered a localised service with a local name, Ling Ying, agreeing to censor posts in accordance with Chinese laws. However, there were clear signs of its struggles as it faced a population sceptical about publicly listing valuable contacts. Following the news of LinkedIn's departure from China, Eileen Danahoe, executive director of the Global Digital Policy Incubator at Stanford University and former US ambassador to the UN Human Rights Council, stated: 'it has gotten pretty ugly around the world where authoritarian governments are forcing the private sector, particularly US tech companies, into these dilemmas.'[76]

However, it is important to note that prior to LinkedIn's exit from the market, lawmakers in Washington had been angered by its complicity in China's information controls. Senator Rick Scott wrote to Microsoft's chief executive demanding to know why it had censored the LinkedIn accounts of three journalists, citing this censorship as 'gross appeasement and an act of submission to Communist China.'[77] Moreover, its exit from the market is not actually an exit at all – indeed, according to their local team statement, LinkedIn will continue operating

[75] Karen Weise and Paul Mozur, "LinkedIn to Shut Down Service in China, Citing 'Challenging' Environment" *The New York Times* (14 October 2021) <https://www.nytimes.com/2021/10/14/technology/linkedin-china-microsoft.html> (accessed 21/12/21)
[76] Weise and Mozur, "LinkedIn to Shut Down Service in China, Citing 'Challenging' Environment"
[77] *ibid.*

in China by 'eliminating the platform's social features' and repositioning its strategic focus 'to provide connection for job offerings and career services.'[78] Overall, LinkedIn's departure from China does not align with an aligned geopolitical posture, but rather can be traced to the competitive environment that it faced and the lack of popularity among Chinese users.

Chinese state-based cyberattack of its Microsoft Exchange Server

In July 2021, the Biden administration accused the Chinese government of breaching Microsoft email systems.[79] Microsoft said in March it 'detected inside its Microsoft Exchange systems – servers that companies keep inside their own networks, running Microsoft software – were linked to the Chinese Ministry of State Security' and once insider the servers, 'Chinese hackers had free run of emails, other sensitive corporate data and intellectual property.'[80] This incident caused US western allies, including the UK, EU, New Zealand and Australia, to confirm attribution and condemn Chinese actions, with UK Foreign Secretary Dominic Raab stating: 'the cyberattack on Microsoft Exchange Server by Chinese state-backed groups was a reckless but familiar pattern of behaviour. The Chinese Government must end this systematic cyber sabotage and can expect to be held account if it does not.'[81]

Microsoft attributed the attack to the Chinese state-backed group, Hafnium, however subsequently avoided making any additional statements. Despite being at the centre of the diplomatic spat between the Western allies and China, the company was able to remain neutral in its stance. The BBC reported that China's foreign ministry spokesman claimed that the US

[78] Forrester, "LinkedIn Has Not Given Up on the Chinese Market" *Forbes* (21 October 2021) <https://www.forbes.com/sites/forrester/2021/10/21/linkedin-has-not-given-up-on-the-china-market/?sh=7ce10bd53d42> (accessed 02/01/22)
[79] Zolan Kanno-Youngs and David E. Sanger, "US accuses China of hacking Microsoft" *The New York Times* (19 July 2021) <https://www.nytimes.com/2021/07/19/us/politics/microsoft-hacking-china-biden.html> (accessed 21/12/21)
[80] Kanno-Youngs and Sanger, "US accuses China of hacking Microsoft"
[81] Foreign, Commonwealth and Development Office, "UK and allies hold Chinese state responsible for a pervasive pattern of hacking" *GOV.UK* (19 July 2021) <https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking> (accessed 08/02/22)

and its allies had 'fabricated' the Microsoft hacking accusations, as the 'US had got its allies to make unreasonable criticisms against China.'[82] The political focus was therefore state-based and Microsoft, at least publicly, only engaged on a factual basis. Although the uproar from Western allies in defence of Microsoft could be said to reinforce the company's geopolitical position as a US company, the lack of engagement with the political and diplomatic reactions to the data breach renders this a relatively weak CPO. Counterfactually, Microsoft could have demonstrated that its geopolitical posture matters by issuing a public statement condemning China's actions and supporting the US government response, as well as engaged in more diplomatic efforts with the US government and its allies to coordinate a response to the cyberattack. Microsoft did not take these steps, but rather remained neutral and focused on mitigating the damage from the attack.

Microsoft's activities in China present a compelling case against the notion that business decisions are primarily guided by geopolitical postures. Although the company's alignment with the US government is more pronounced than that of other tech giants like Google, Apple and Facebook, this alignment has not translated into a corresponding reluctance to engage with the Chinese market or to make concessions to the CCP. From adapting its business model to suit Chinese interests to the strategic navigating Chinese legislation, Microsoft's actions reveal a calculated approach driven by profit maximisation. Even in the face of incidents such as the Chinese state-backed cyberattack on the Microsoft Exchange Server, the company's response has remained neutral and business-focused, steering clear of geopolitical posturing. The departure of LinkedIn from Chin is further explained by the competitive environment and the platform's lack of popularity, rather than geopolitical reasoning. This realignment of strategic

[82] BBC, "China says Microsoft hacking accusations fabricated by US and allies" *BBC News* (20 July 2021) <https://www.bbc.co.uk/news/world-asia-china-57898147> (accessed 08/02/22)

focus underscores the complexity of factors that determine corporate behaviour, including the constraints of the business model, relevant legislation, and internal company structure.

The case of Microsoft provides evidence supporting my hypothesis that rational profit maximisation under constraints, rather than geopolitical considerations, offers a more robust explanation for corporate decisions in the Chinese market. The case challenges the simplistic narrative that posits geopolitical alignment as the primary driver of business decisions and instead elevates the understanding of how companies navigate constraints to achieve their financial goals. As explained by Nancy Ayer Fairbank, 'Microsoft's overall motive is profit. Unlike many liberal democratic governments, Microsoft does not purport to act for the public good when doing so goes against their financial interests.'[83]

5.6. Case Study 2: Google

5.6.1. Geopolitical Posture: Non-aligned

Google defines its corporate values vaguely through '10 things we know to be true.'[84] Three of these points are relevant to conduct in foreign states. The first is that *democracy on the web works,* emphasising that 'google search works because it relies on the millions of individuals posting links on websites to help determine which other sites offer content of value.'[85] This emphasises the significance of Google's business interactions at a global scale. The second is that *you can make money without doing evil.* This point begins with the premise that 'google is a business' however sets out some 'guiding principles' on advertising specifically.[86] Finally, *the need for information crosses all borders* emphasises that 'our company was founded in California, but our mission is to facilitate access to information for the entire world, and in

[83] Fairbank, "The State of Microsoft?"
[84] Google, "10 things we know to be true" <https://about.google/philosophy/> (accessed 04/01/22)
[85] *ibid.*
[86] *ibid.*

every language.'[87] Overall, official company policy seems to be sufficiently vague to allow for complete flexibility in justifying interactions and activities in foreign states. The reference to democracy is the only indication of alignment with the US government, however there is no explicit attempt to identify the US as an official partner or as the source of the company's outlook.

In terms of public statements, evidence reveals that Google's decisions are not neutral, but rather shaped by their own code of conduct in foreign states, in line with my theorisation of a non-aligned posture. This was exemplified in November 2021 when Katie O'Donovan, Public Policy Manager at Google UK, testified before the UK Foreign Affairs Committee. When asked whether Google had a foreign policy, O'Donovan answered that 'I do not think we would describe ourselves as having a corporate foreign policy, but we certainly have a system of principles and approach both to the way we operate globally and in individual countries, and also in the way that we think about the internet and the way we think the internet should be governed.'[88] Moreover, she argued that 'we absolutely think there is value to us as Google and a shared value to society and the Governments to turn up, to engage and to have live dialogue with governments, regulators and legislators.'[89] When considering the impact of different states' regulatory authorities over the internet, O'Donovan pointed out that 'we are a global company with a global mission and we want that to be rooted in established norms.'[90] She explains that although there are challenges to a free and open internet at the moment, 'companies like ours can and should take a very great degree of responsibility, and we do.'[91] When asked whether Google has engagement with foreign ministries, she replied that foreign offices have special envoys for technology, 'who is the Consul-General based in San Francisco,

[87] Google, "10 things we know to be true"
[88] Foreign Affairs Committee, "Oral Evidence" (2 November 2021)
[89] *ibid.*
[90] *ibid.*
[91] *ibid.*

so through his office and him we would have engagement with the Foreign Office and its processes.'[92]

When referring to China in particular, O'Donovan confirmed Google does not operate in China. She was then asked what bearing a country's domestic approach to human rights has on Google's decision to operate in a country or exit the market, and she argued that 'our not being present in a market is not a neutral act' and that in China specifically 'we were not happy with the conditions that were put on us to operate that search engine,'[93] remaining sufficiently vague on the decision-making process. This last CPO reveals that China presents a particularly intriguing case for Google's geopolitical sensitivity. The company's decision not to operate in China, as explained by O'Donovan, was influenced by conditions that were not conducive to its principles and operational ethos. This shows how geopolitical posturing could impact Google's market decisions, even though this often intertwines with concerns about company reputation. All in all, the public statements from Google provide a clear indication of its posture as a non-aligned actor. The statements suggest that decisions are not neutral, but rather shaped by its own system of principles. There is a notable absence of any overt alignment with the US, neither positioning it as a partner nor as a determinant of its perspective.

Finally, whilst Google maintains partnerships with the US government, it does so with a degree of ambiguity, highlighting its non-aligned stance. Despite pursuing contracts for modernising the Pentagon's technology structure, Google has faced internal resistance. Most notable in 2018, when thousands of Google employees signed a petition – and some resigned in protest – to halt Project Maven, an initiative to provide the Pentagon with AI that could have been used to help improve US surveillance drones. In November 2021, there were reports of Google pursuing a contract to modernise the Pentagon's cloud technology and of the existence

[92] Foreign Affairs Committee, "Oral Evidence" (2 November 2021)
[93] *ibid.*

of contracts with the US Air Force and US Navy.[94] Lucy Suchman, a professor at Lancaster University, argued that these 'demonstrate the fragility of Google's commitment to staying outside the major merger that's happening between the D.O.D (Department of Defence) and Silicon Valley.'[95] In the context of Google's official company policy and public statements, such contracts can be interpreted as commercial opportunities rather than indicators of lessening independence from the US government.

Overall, I have identified Google's geopolitical posture as non-aligned. The company presents its business interactions as being driven by specific policies and postures that are not explicitly tied to the US government, both in substance and form. It is important to note that O'Donovan's statements, which were made after the decision to stop operating in the Chinese market, retrospectively refer to the lack of neutrality in past decision-making. It is crucial to understand that Google's non-aligned posture does not imply being apolitical; the company does not operate in a geopolitical vacuum. Although Google refrains from explicit alignment with the US government, its business decisions are shaped by specific internal policies and perspectives, free from explicit government ties. Google's geopolitical posture differs significantly from that of Microsoft. Whilst Microsoft demonstrates alignment, Google's official company policy, public statements, and lack of partnerships with the US government reveal its unaligned stance. Given its non-aligned company posture, we would expect Google to operate in China, as it is not bound by the US government. We would further expect Google's decisions to be explained by its own policies regarding conduct in foreign states and justified as such. These decisions would be in conflict with rational profit maximisation logic, and the identified constraints would not fully explain these decisions.

[94] Daisuke Wakabayashi and Kate Conger, "Google Wants to Work with the Pentagon Again, Despite Employee Concerns" *The New York Times* (3 November 2021) <https://www.nytimes.com/2021/11/03/technology/google-pentagon-artificial-intelligence.html> (accessed 04/01/22)
[95] *ibid.*

5.6.2. Google's Behaviour in China

I analyse three of Google's main decision-making processes on interactions with China: the reasons for and circumstances under which the company withdrew from the Chinese market in 2010, its behaviour as encapsulated by its attempts to re-enter the market throughout the 2010s, and the ambiguous response to employee activism against Project Dragonfly in 2018. I find the first two to reflect decision-making that was constrained by relevant Chinese legislation to the company's business model, whereas the third displays the effect of employee activism as a constraint.

Google's Withdrawal from Chinese Market 2010

Google's initial entry into the Chinese market, where its search engine complied with the Chinese government's censorship policies, can be interpreted as the company's effort to align with its then-corporate motto of 'don't be evil.' By providing censored search results, Google justified that it was making a compromise to expose Chinese users to a broader range of information than they had previously accessed, aligning with its mission 'to organize the world's information and make it universally accessible and useful.' In fact, Google's cofounders, Sergey Brin and Larry Page, reportedly conveyed to employees that it was preferable to provide censored results to Chinese users rather than no results at all.[96] Therefore, the company's initial entry into the Chinese market was framed as an endeavour to 'broaden the horizons of Chinese users and nudge the Chinese internet toward greater openness.'[97] The company portrayed its business ventures and adherence to censorship guidelines as necessary

[96] Nicole Perlroth, *This is how they tell me the world ends: The cyberweapons arms race*. Bloomsbury Publishing USA, 2021. p.204
[97] Matt Sheehan, "How Google took on China – and lost" *MIT Technology Review* (19 December 2018) <https://www.technologyreview.com/2018/12/19/138307/how-google-took-on-china-and-lost/> (accessed 20/12/21)

for a greater good. This approach aligns with the overarching goal of profit maximisation and company growth.

Google pulled from mainland China in 2010 after a cyberattack (Operation Aurora, targeting Google's intellectual property and Gmail accounts of human rights activists) and disputes with the Chinese government over censorship of search results.[98] Google revealed they had uncovered evidence of 'dozens of human rights activists connected to China being routinely accessed by third parties,' concluding they could 'no longer continue censoring (their) results on Google.cn.'[99] Importantly, they made an explicit reference to the tension between business interactions and their internal policies: 'figuring out how to make good on our promise to stop censoring search on Google.cn has been hard.'[100] Two CPOs are particularly important: first, Google declared their intent 'to continue R&D work in China and also maintain a sales presence there.'[101] To avoid losing the Chinese market completely, they ensured that users visiting Google.cn were redirected to its Hong Kong version, Google.cn.hk, where they offered uncensored search in simplified Chinese. However, they acknowledged the risks of the Chinese government blocking access to their services at any point – which it did, shortly thereafter. This CPO reveals that Google's goal was to maintain their presence in the Chinese market, but was constrained by Chinese legislation, following a profit maximisation logic.

Second, Google executives stated, 'we would like to make clear that all these decisions have been driven and implemented by our executives in the United States, and that none of our employees in China can, or should, be held responsible for them.'[102] This statement weakly alludes to the influence of the company's code of conduct in foreign states from higher levels shaping their decisions. However, it is important to contextualise this statement. Google's

[98] Sheehan, "How Google took on China – and lost"
[99] Google, "A new approach to China: an update" *Google Official Blog* (22 March 2010) <https://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html> (accessed 06/02/22)
[100] *ibid.*
[101] *ibid.*
[102] Google, "A new approach to China: an update"

search engine complied with Chinese government's censorship policies for four years until a cyberattack attributed to China was discovered. The subsequent security concerns and the CCP's decision to block Google.cn strongly suggests a profit maximisation logic rather than a decision-making process linked to geopolitical postures.

Google's decision to withdraw from China in 2010 was influenced by a combination of factors, including the company's internal structure, security concerns, and Chinese legislation. The decision to exit the market was prompted by a cyberattack targeting Google's intellectual property and the Gmail accounts of human rights activists, as well as disputes over censorship. This move can be interpreted as a demonstration of the company's ethical commitment, reflecting the influence of its internal structure as a constraint. Despite the withdrawal, Google strategically sought to maintain its presence by operating in Hong Kong and continuing research and development work in the country. However, within a year of the withdrawal, there were indications that some executives were advocating for the company's re-entry into the Chinese market.[103] If Google's code of conduct in foreign states had explained its exit from the market, we would expect Google to remain coherent to this decision.

Google's Attempts to Re-Enter Chinese Market

At first glance, Google's efforts to re-enter the Chinese market appear to reflect its non-aligned geopolitical posture. If Google's code of conduct in foreign states had caused its departure from the market in the first place, I would expect Google to adhere to this decision consistently. However, the subsequent decisions and conduct discussed below suggest that this non-aligned posture does not exert a substantial influence. None of the decisions conflict with rational profit maximisation logic, and none are substantiated in rhetoric or practice by a consistent code of conduct in foreign states.

[103] Perlroth, *This is how they tell me the world ends,* p.212

First, despite being praised for leaving China in protest over government censorship,[104] which would have provided evidence in support of the explanatory power of its geopolitical posture, Google's continued presence was evident. Just two years after the search engine's exit from the market, the company's Android operating system (OS) still ran on 84% of Chinese smartphones, and efforts were made to capitalise on its growth in China.[105] During a visit to China in 2013, former CEO Eric Schmidt attempted to persuade local developers to write applications for Android OS.[106] Throughout the 2010s, Google attempted to re-enter the Chinese market through projects including an 'everything but search' strategy and a partnership with a Chinese smart-watch maker, Mobvoi.[107] There were numerous rumours of Google's attempts to sway the Chinese government to approve ventures, which never materialised, such as a reintroduction of its Google Play app store in China, a reintroduction of Google Scholar, and a mobile-app store in conjunction with a Chinese company, NetEase.[108] Finally, in May 2017, Google became re-involved in China through its Artificial Intelligence programme, with the justification that 'the science of AI has no borders (…), neither do its benefits.'[109] Google also promoted use of TensorFlow, an AI software library developed by the Google Brain Team.[110] This evidence undermines the explanatory power of Google's geopolitical posture, as the reasons for its exit and attempts to re-enter are not coherent.

Additionally, in Washington frustration was expressed over Google's pursuit of the Chinese market whilst refusing to collaborate with the Pentagon on AI projects due to employee objections.[111] Whilst this is in line with Google's non-aligned posture, evidence shows that Google executives were driven by a strong desire to gain market share from various

[104] Yeo, "Geopolitics of search: Google versus China?." p.599
[105] *ibid.* p.599
[106] *ibid.* p.600
[107] Sheehan, "How Google took on China – and lost"
[108] *ibid.*
[109] *ibid.*
[110] *ibid.*
[111] *ibid.*

competitors, including Microsoft, Oracle, Apple, Amazon and Baidu.[112] In addition, the removal of Google's 'don't be evil' motto from its corporate code of conduct in 2018[113] and subsequent statements from former employees,[114] further indicate a focus on profitability over political concerns. Google's attempts to re-enter the Chinese market through various strategies and partnerships, and its eventual re-involvement in China through its Artificial Intelligence programme, signal a continued effort to balance profit maximisation under the constraint of its internal structure.

Project Dragonfly, 2018

In August 2018, reports emerged that Google was developing Project Dragonfly, a censored Chinese search engine. CEO Sundar Pichai emphasised the importance of the Chinese market,[115] indicating a focus on long-term profitability within legislative constraints. However, the project faced significant opposition from human rights activists and Google employees, prompting US Vice President Mike Pence to call for its termination, which ultimately occurred in December 2018. *The Intercept* leaked one of the Google's head of search, Ben Gomes' speeches to the Dragonfly team, in which he stated that 'the value of going into China' lies in the fact that it 'is one of the most interesting markets, arguably the most interesting market in the world today.'[116] Importantly, he addressed the volatility of the geopolitical scene, stating that 'at some level, at our scale, we need to maintain that optionality, in case suddenly the world

[112] Perlroth, *This is how they tell me the world ends,* p.212
[113] Suzanne Nossel, "Google is Handing the Future of the Internet to China" *Foreign Policy* (10 September 2018) <https://foreignpolicy.com/2018/09/10/google-is-handing-the-future-of-the-internet-to-china/> (accessed 20/12/21)
[114] Lauren Feiner, "Google sacrificed its 'don't be evil' mantra to grow bigger, former exec says" *CNBC* (2 January 2020) <https://www.cnbc.com/2020/01/02/google-abandoned-its-dont-be-evil-mantra-former-exec-says.html> (accessed 06/02/22)
[115] Nitasha Tiku, "Google's CEO Says Tests of Censored Chinese Search Engine Turned Out Great" *Wired* (15 October 2018) <https://www.wired.com/story/wired-25-sundar-pichai-china-censored-search-engine/> (accessed 06/02/22)
[116] Ryan Gallagher, "Leaked Transcript of Private Meeting Contradicts Google's Official Story on China" *The Intercept* (9 October 2018) <https://theintercept.com/2018/10/09/google-china-censored-search-engine/> (accessed 06/02/22)

changes or [the US president] decides his new best friend is [Chinese President] Xi Jinping.'[117] This statement is particularly strong in undermining the relevance of geopolitical posturing. The statement frames political factors such as US-China relations as both a constraint and a potential opportunity for Google's growth as a company, undermining the relevance of geopolitical posturing and strengthening instead the evidence of rational profit maximisation under constraints as the main decision-making mindset.

Despite initial claims that Project Dragonfly would not proceed following employee protests, it was later revealed that Google continued to work on the project.[118] This suggests that whilst employee activism may influence public statements, ultimate decision-making remains at the highest levels of leadership. The handling of Project Dragonfly by Google shows the interplay of profit considerations and employee activism, rather than the company's non-aligned geopolitical stance. If geopolitical posturing had been relevant to the decision-making, we would expect Google's actions to be in conflict with rational profit maximisation logic and to be substantiated by a consistent code of conduct in foreign states. Although the handling of Project Dragonfly is in conflict with rational profit maximisation, there is no evidence of the relevance of political factors. Instead, decision-making is explained by the constraint of the company's internal structure, encompassing corporate culture and employee activism. Despite the project's potential profitability driven by the Chinese market's size, internal protests, and human rights concerns led to its termination, indicating a prioritisation of ethical considerations over profit. In my theoretical framework, I highlight the distinction I made between political factors and ethical considerations, which are considered constraints to the company's ability to make profit due to enhance reputation, customer loyalty, and employee satisfaction.

[117] Gallagher, "Leaked Transcript of Private Meeting Contradicts Google's Official Story on China"
[118] Ryan Gallagher, "Google Employees Uncover Ongoing Work on Censored China Search" *The Intercept* (4 March 2019) <https://theintercept.com/2019/03/04/google-ongoing-project-dragonfly/> (accessed 04/01/22)

Overall, Google's withdrawal from the Chinese market in 2010, its attempts to re-enter the market and its response to Project Dragonfly in 2018 undermines the relevance of geopolitical posturing, and instead provides evidence towards rational profit maximisation under constraints. Evidence of the effect of Google's geopolitical posture was both insufficient and weak, in accordance with the process tracing method. However, as opposed to Microsoft, Google's decision-making process reflects a balance between profit maximisation and sensitivity to geopolitical contexts. Whilst the initial exit from the Chinese market could potentially be tied to its non-aligned geopolitical posture, its behaviour and justifications do not align to a coherent approach.

5.7. Discussion

The case studies of Google and Microsoft, representing companies with divergent geopolitical postures, indicate that whilst their official stances toward the US government vary, the drive behind their decision-making processes concerning business interactions is the same: rational profit maximisation under constraints. These constraints include each company's individual business model, relevant Chinese legislation, and internal structure.

Google, identified as have a non-aligned geopolitical posture, has made concessions to the CCP whilst carefully navigating its internal structure. Although its independent code of conduct in foreign states could appear to explain its exit from the Chinese market, subsequent behaviour did not consistently align with this stance. Google's handling of Project Dragonfly, in particular, could be explained by the constraints of the company's internal structure, primarily employee activism. Similarly, Microsoft, identified as having a geopolitical posture that is aligned with the US government, also made numerous concessions to the CCP despite its stronger ties to the US government. Even in response to events such as the Chinese state-based cyberattack on its Exchange Server, Microsoft maintained a relatively neutral stance rather than

using the situation as an opportunity to strengthen its geopolitical alignment. Therefore, despite the different geopolitical postures of these companies, their actions in the Chinese market are largely driven by the common objective of profit maximisation. Their business decisions reveal an interplay between the pursuit of profit, the constraints of their business models, and the regulatory requirements of the Chinese market, rather than a coherent and consistent adherence to their stated geopolitical stances.

5.8. Conclusion

In this paper, I aimed to determine whether tech companies like Google and Microsoft have geopolitical postures that influence their business decisions, particularly in high-stakes markets like China. I defined geopolitical postures and used classifications of 'aligned' for Microsoft and 'non-aligned' for Google to assess the impact of these postures on the companies' behaviour in China. The empirical analysis revealed that, despite differing public affiliations with the US government, neither Microsoft nor Google's geopolitical postures significantly influenced their operations in China. Instead, the findings point to profit maximisation as the driving force, constrained by their business models, relevant Chinese legislation, and internal company structures.

These findings have significant implications for both academia and policymaking. First, they show that in the case of US companies, public statements and official policies may not always accurately reflect the true drivers of corporate behaviour in international markets. This may require the US government to emphasise policies that acknowledge that geopolitical postures may be window dressing and even an ostensibly aligned company will engage with the peer competitor when profit maximisation demands it. However, whether alignment is beneficial or not to the US remains outside the scope of the article. My contribution lies in understanding how the US interacts with its tech industry within the context of foreign policy.

In contrast to China's strategic employment of tech companies as conduits for exercising institutional power,[119] the US embraces a laissez-faire approach. Identifying the motivations of US tech companies as units of analysis in IR allows for comparisons to be made with Chinese tech companies' motivations, and for comparisons to be made between the two governments' use of their tech private sectors in their competition with each other.

For tech companies, the findings suggest the need for clearer communication from these companies regarding their corporate objectives and geopolitical stances. This clarity might help reconcile public perception with corporate actions, especially in geopolitically complex regions. The diverse strategies of US tech companies not only shape their own trajectories but also influence global perceptions of the US tech sector. This can influence broader international relations, extending beyond the US-China context. For example, companies' compliance with demands from authoritarian regimes can undermine American competitiveness and national security whilst legitimising political oppression.[120]

Finally, the paper contributes to International Relations literature by developing a theory to understand whether tech companies have a form of foreign policy which I termed 'geopolitical postures.' This represents a methodologically rigorous attempt to contribute the growing debate among scholars, pundits and policymakers who increasingly recognise tech companies as significant political actors with distinct geopolitical postures akin to those of states. The concept of a geopolitical posture differs from corporate strategies or corporate diplomacy, addressing the broader discussion of whether tech companies now rival states as primary actors in global affairs. This article employs tools from IR to ground the concept of a non-state actor's

[119] Madison Cartwright, "Internationalising state power through the internet: Google, Huawei and geopolitical struggle." *Internet Policy Review* 9, no. 3 (2020): 1-18. p.3
[120] Klon Kitchen, "The New Superpowers: How and Why the Tech Industry is Shaping the International System" *National Affairs,* Number 29 (Fall 2021) <https://nationalaffairs.com/the-new-superpowers-how-and-why-the-tech-industry-is-shaping-the-international-system> (accessed 29/11/21)

foreign policy to tangible benchmarks, countering exaggerated claims of multinational corporations imposing constraints on states.

Appendix

The following table contains the positions of my interviewees and time of interview.

Table 2: List of interviews

Interviewee and Position	Time of Interview
Background Source *US-China Think Tank Researcher*	6 April 2022
Background Source *US-China Think Tank Researcher*	6 April 2022
Background Source *US-China Think Tank Researcher*	6 April 2022
Background Source *US-China Think Tank Researcher*	6 May 2022
Background Source *US-China Think Tank Researcher*	6 May 2022
Background Source *US-China Think Tank Researcher*	6 May 2022
Background Source *Official in the UK Department for Business, Energy and Industrial Strategy*	27 January 2021 (remote interview)

6. Conclusion

In this thesis, I examined the United States' approach to technology policy. My overarching research question was *how has the US approach to tech policy regarding the tech private sector affected its standing in the technological competition with China?*

In a series of three research articles, I first present empirical evidence of the US's strategic setbacks in the tech war. The first part of the thesis acknowledges the US's strategic losses, whilst the second part explores a potential reason for this decline, focusing on the lack of a consistent, unifying approach to tech policy. My analysis centres on two critical aspects of US tech policy: alliance management and private sector management. These correspond to areas where the US has faced significant challenges: international partnerships and government-industry relations.[1]

Article 2 characterises US alliance management as non-cooperative, revealing the challenges the US is facing in successfully influencing allies to counteract Chinese tech companies' presence in their own critical national infrastructures. Article 3 characterises the US approach to its private sector as laissez-faire, showing that US Big Tech companies operate under rational profit maximisation irrespective of their alignment with the US government.

In the following section, I first provide a summary and discussion of the findings for each article. This will be followed by a reflection on the limitations of the study and potential directions for future research. Finally, I examine the broader implications of these findings when considered collectively.

[1] Patricia M. Kim, Matthew Turpin, Joseph S. Nye Jr., Jessica Chen Weiss, and Eun A Jo Ryan Hass and Emilie Kimball, "Should the US pursue a new Cold War with China?" *Brookings Institute* (1 September 2023) <https://www.brookings.edu/articles/should-the-us-pursue-a-new-cold-war-with-china/> (accessed 02/10/23)

6.1. Summary and Discussion of Findings

Article 1: ***Targeting US Tech Companies: Europe's Soft Balancing Via Data Localisation***

In the first part of the thesis, I drew on existing statistics indicating the loss of confidence in the US by its allies. I provided an empirical representation of what occurs as a consequence of this loss of confidence. I show that US allies, more specifically EU member states, are explicitly seeking to curtail the presence of US tech firms in their cloud infrastructures through data localisation policies. I argue that the rise of data localisation policies among US European allies is not a side-effect, but a purposeful strategy of soft balancing against US leadership in tech.

Amidst the escalating US-China tech competition, US global leadership has been facing a crisis of legitimacy rooted in declining faith in American democracy. As I elaborated on in the introduction chapter, international polls reveal a growing perception that the US is no longer a beacon of democracy or a reliable partner.[2] The revelation of NSA surveillance and the perceived dysfunction of American democracy eroded the US moral high ground and its reputation for protecting individual rights.[3] This data shows that US influence has eroded on the global stage, but the real-life implications remain unclear. To address this gap, I provide an empirical case study of the loss of US influence on its allies. Specifically, I examined the EU's adoption of data localisation policies, which are regulations mandating the storage and processing of digital data within a state's territorial jurisdiction. I investigated why EU member states have embraced these policies despite their evident economic drawbacks and security inefficiencies. My central argument is that data localisation policies adopted by EU member states serve as a form of 'soft balancing' against US technological hegemony. To substantiate

[2] Kim, et. al., "Should the US pursue a new Cold War with China?"
[3] Brian Klaas, "The world is horrified by the dysfunction of American democracy" *The Washington Post* (11 June 2021) <https://www.washingtonpost.com/opinions/2021/06/11/pew-research-global-opinion-us-democracy/> (accessed 02/10/23)

this claim, I conducted a case study of the European Cybersecurity Certification Scheme for Cloud Services (EUCS). My findings indicate that the sovereignty requirements in the EUCS aim to reduce reliance on US tech companies, hinder US surveillance capabilities, and promote European tech industries. Despite facing significant criticisms for potentially disrupting global cybersecurity cooperation and creating divisions among EU member states, the persistence of EUCS substantiates my claim that this is a deliberate strategy of soft balancing.

The implications of my findings are three-fold. First, for European policymakers, the findings call for an approach to data localisation with more technical understanding and careful balancing of potential benefits against significant costs. Whilst these policies aim to reduce reliance on US tech companies, curb US surveillance capabilities and foster domestic industry, their economic and political costs cannot be overlooked. European policymakers may perceive the benefits of balancing against US tech dominance as outweighing the costs. Such a perspective considers the protection of privacy through data localisation a worthy trade-off despite its economic implications. However, this approach is not without its own set of costs and risks, which become clear through the stark division in opinions among EU member states. Whilst data sovereignty is often cited as a key justification for these policies, it is not clear whether it is truly the primary motivation or if it serves more as a rhetorical device used to justify data localisation policies. This uncertainty means that European policymakers need to weigh domestic interests and alliance dynamics against the broader impacts of their decisions on the global digital economy, ensuring a balanced approach that respects both sovereignty and economic considerations.

For the US, my findings that the EU is soft balancing through data localisation reveals the necessity to reassess its alliance management strategies if the US seeks to maintain its

'leadership' in tech among its allies, in terms of 'US efforts to lead on global rules and values.'[4] Rather than forcing allies into a 'with us or against us' choice, the US seeking collaborative paths may prove more beneficial to maintain the Western edge in technology whilst respecting the sovereign interests of its European allies. More collaborative approaches by the US may have resulted in different outcomes. Allies' support is crucial for US tech policies, ranging from restricting Chinese access to critical semiconductor technology to contesting surveillance technologies. Losing allies' support can have significant consequences on the US standing in the tech war, potentially leading to disruptions in global supply chains, reduced market access for US tech companies, weakened cybersecurity cooperation and negative economic repercussions for the US economy.

For IR scholars, this paper introduced the idea of data localisation policies as a form of soft balancing, challenging traditional understandings of alliance dynamics in the US-China competition context. Understanding data localisation policies as soft balancing provides a number of analytical benefits. First, it allows us to see the broader geopolitical context in which these policies are adopted. Data localisation policies are not simply about protecting data sovereignty or cybersecurity, they are also about states seeking to position themselves in a changing global order, in which the US and China are competing for dominance in technology. Second, understanding data localisation as soft balancing helps us understand the motivations of states that adopt them. These states are not simply trying to maximise data sovereignty. They are also trying to reduce their dependence on US tech companies, limit the US's ability to access their data, and promote domestic industry and economic growth. Third, understanding data localisation as soft balancing allows us to identify the potential consequences of these

[4] Karen Kornbluh and Julia Tréhu, "The New American Foreign Policy of Technology: Promoting Innovation, National Security and Democratic Values in a Digital World" *GMF Policy Report* (March 2023) <https://www.gmfus.org/sites/default/files/2023-03/Report%20-%20The%20New%20American%20Foreign%20Policy%20of%20Technology_1.pdf> (accessed 15/04/23)

policies for IR, as they can cause shifts in alliance dynamics and a departure from the traditional belief that data localisation policies would primarily be adopted by authoritarian states.[5]

Overall, in this paper I argued that data localisation policies adopted by US allies in Europe are strategic responses reflecting political resolve to soft balance against the US. This reframed understanding of data localisation as a form of soft balancing provides a new lens for understanding the complex and evolving motivations of states in the context of US-China competition.

In the second part of the thesis, I examined one possible explanation for the US decline in the tech war: its decentralised and sometimes inconsistent approach to tech policy. This approach has been criticised by scholars and policymakers for lacking a solid, unifying strategy.[6] I built on existing evidence of strategic losses in two specific areas of US tech policy: alliance management and private sector management.

Article 2: *My Way or the Huawei: US Influence on China's Involvement in the UK's Critical National Infrastructure*

Recognising the strategic losses experienced by the US in the tech war, as I presented in the first part of the thesis, in the second part I delve into the US tech policy itself. Article 2 focuses on alliance management. I characterise the US approach to alliance management as non-cooperative. I evaluated the strength of US international partnerships by examining the US's effectiveness at preventing a key ally, the UK, from adopting Chinese technology in their critical national infrastructures. My findings demonstrate the inconsistency of US efforts, with its success in the UK being highly contingent on very specific background conditions. This

[5] Dana Polatin-Reuben and Joss Wright, "An Internet with {BRICS} Characteristics: Data Sovereignty and the Balkanisation of the Internet." In *4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14)*. 2014 p.1

[6] Robert H. Wade, "The Paradox of US Industrial Policy: The Developmental State in Disguise." *Transforming Economies*, edited by Nübler, Irmgard, José Manuel Salazar-Xirinachs, and Richard Kozul-Wright. Switzerland: International Labour Organisation (ILO), 2014. Print. p.382

suggests that the US's current alliance management strategy is unsustainable in the long term, even with a member of its most trusted alliance network, the Five Eyes (FVEY). Overall, my findings show that US influence on its allies in the context of technological competition with China is limited. Even though US influence can be effective under specific geopolitical and domestic conditions, the US must develop a more cooperative strategy if it seeks to leverage alliances in its competition with China.

Specifically, I drew on the case of the UK's policy reversal from accepting the Chinese company Huawei's involvement in building its national 5G telecommunications networks in January 2020 to banning it in July. I considered this a deviant case as it interrupted the UK's previous policy pattern of warmly accepting Chinese investments across different sectors of the CNI. By employing within-case process tracing, I argue that US influence was a necessary condition in the UK's policy reversal on Huawei. However, it was not sufficient, as it interacted with favourable background conditions: the behaviour of other FVEY intelligence-sharing allies, specific geopolitical developments (notably China's security law for Hong Kong), and domestic political dynamics within the UK.

I drew a number of implications from the findings. First, on the limits of US influence: the findings illustrate that US influence, under specific conditions, can significantly impact an ally's policy decisions regarding Chinese technology companies. However, the effectiveness of this influence is not guaranteed and varies depending on the context and surrounding conditions. This indicates a degree of uncertainty in the US's ability to shape allied states' decisions in similar scenarios. Moreover, there were implications for US alliance management in tech. The UK policy reversal raises critical questions about the broader US approach to its allies. The conditional and inconsistent nature of US influence across different contexts suggests a fragmented and precarious strategy. Consequently, adopting more coherent and collaborative approaches with its allies, rather than influence ranging from persuasion to

coercion, may be more beneficial for the US to strengthen its position in the tech war. Indeed, a strategy emphasising collaboration, shared incentives, and innovation could be more effective in navigating the complex dynamics of international relations and technological competition.

Finally, the case of the UK policy reversal on Huawei reveals the strategic importance of telecommunications and digital infrastructure in the US-China tech war. US efforts to limit Chinese involvement in these areas are likely to continue as part of its broader strategy to challenge China's technological advancements.

Article 3: ***Do Big Tech Companies' Geopolitical Postures Matter? Microsoft and Google's Conduct in China***

In the third and final article, I examined the US government's approach to managing its private tech sector, particularly how its laissez-faire approach to tech policy shapes government-industry relations. Economic statecraft literature highlights China's centralised relationship with national tech champions as a cornerstone of its tech policy. I explored the extent to which US Big Tech companies align with the US government, and considered whether this alignment influences their business decisions. Whilst I did not directly compare the US and Chinese approaches, my findings contribute to the development of a framework for such comparisons. Regardless of their respective geopolitical postures, the alignment or lack thereof between US Big Tech companies and the US government does not appear to significantly impact their business decisions. These findings help to characterise US tech policy, in which companies operate with autonomy from the influence of US foreign policy. Whilst the implications of this autonomy remain outside the scope of my article, my research contributes to understanding how the US interacts with its tech industry. This is a crucial aspect of crafting effective tech policy. In contrast to China's strategic use of tech companies as conduits for institutional power, the US embraces a more hands-off approach.

Specifically, I analysed the influence of geopolitical postures on the business decisions of US tech giants Microsoft and Google in China. I challenged the argument that these companies have geopolitical postures that drive their business interactions in third countries and that these postures are an independent factor in US-China strategic competition over technological superiority. Using a small-N case study comparison and process tracing through semi-structured interviews and secondary sources, I show that Microsoft and Google's decisions are primarily guided by rational profit maximisation under specific constraints: the individual company's business model, relevant Chinese legislation, and internal company structure. I argue that a company's geopolitical posture, as reflected in official policies and public statements, has no identifiable effect on decision-making in the Chinese market. This 'posture' may, in fact, be an outcome of addressing reputational concerns whilst maintaining flexibility in business interactions.

My findings have significant implications for both academia and policymaking. First, I determine that decisions made by Microsoft and Google in the Chinese market are primarily driven by rational profit maximisation. This finding suggests that economic considerations outweigh geopolitical alignment in corporate decision-making. Contrary to expectations, the geopolitical postures of these companies that I identified, whether aligned, apolitical or non-aligned with the US government, do not play a role in their business decisions in China. This implies that public statements and official policies do not always accurately reflect the true drivers of corporate behaviour in international markets. This may require a reassessment of the US approach to its tech giants, emphasising policies that geopolitical postures may at times serve as window dressing. Even companies perceived as aligned may prioritise profit motives over geopolitical alignment, especially in lucrative markets like China.

However, whether alignment is beneficial or not to the US remains outside the scope of the article. My contribution lies in understanding how the US interacts with its tech industry within

the context of foreign policy, which is crucial for crafting tech policy. In contrast to China's strategic employment of tech companies as conduits for exercising institutional power, the US embraces a different approach. This provides a basis for comparative research on the differences between the US and China's tech policies across different geographies and sectors. If we consider alternative approaches to 'non-cooperative' and 'laissez-faire' that the US could adopt, these approaches need to be tailored to its political and economic landscape and account for the aims of this policy. What works for China is very likely not to be appropriate for the US. Rather than an industrial policy, the US could better acknowledge the independent agency of its tech companies, aiming for partnerships that serve mutual long-term interests. This approach would emphasise collaborative, mutually beneficial relationships between the government and the private sectors, recognising the different contributions and needs of each.

For tech companies, the findings reveal the disconnect between the US government and its tech sector, suggesting the need for clearer communication from these companies regarding their corporate objectives and geopolitical stances. This clarity might help reconcile public perception with corporate actions, especially in geopolitically complex regions. The diverse strategies of US tech companies not only shape their own trajectories but also influence global perceptions of the US tech sector. For example, Klon Kitchen argues that companies' compliance with demands from authoritarian regimes can undermine American competitiveness and national security whilst legitimising political oppression.[7]

Finally, this article contributes to IR literature by developing a theory to understand whether tech companies have foreign policies, or what I term 'geopolitical postures.' This represents a first attempt to address this issue in a methodologically rigorous way. My work complements the growing debate among scholars, pundits and policymakers, who increasingly

[7] Klon Kitchen, "The New Superpowers: How and Why the Tech Industry is Shaping the International System" *National Affairs,* Number 29 (Fall 2021) <https://nationalaffairs.com/the-new-superpowers-how-and-why-the-tech-industry-is-shaping-the-international-system> (accessed 29/11/21)

recognise tech companies as significant political actors with distinct geopolitical postures akin to those of states.[8] The debate extends to tech leaders themselves.[9] The perception of a blurred line between political and commercial aspects in the tech industry is gaining traction in the US. Nevertheless, theorisation on companies' geopolitical postures has hitherto been informal, with a clear lack of understanding and empirical testing of what it means to have such a posture. Existing theorisations of geopolitical postures of tech companies are insufficient in providing a benchmark towards which one can analyse their behaviour in third countries. If companies have geopolitical postures, there must be indications of the ways in which such postures constrain their behaviour. In this paper, I addressed the existing literature gap by identifying the indicators of a geopolitical posture and tested its effect on corporate decision-making in the tech industry.

The concept of a company foreign policy differs from corporate strategies or corporate diplomacy; it addresses the broader discussion of whether a handful of tech companies now rival states as the primary actors of global affairs, having 'taken control of aspects of society, the economy, and national security that were long the exclusive preserve of the state.'[10] Exaggerated claims of multinational corporations imposing constraints on states are not new, and as I outline in my broader literature review chapter, examples of such exaggerations are riddled throughout history. In this article, I employ tools from IR to counteract such exaggerations, grounding the concept of a non-state actor's foreign policy to tangible benchmarks. Moreover, identifying the motivations of US tech companies as units of analysis in IR allows for comparisons to be made with Chinese tech companies' motivations, and for

[8] Foreign Affairs Committee, "Oral Evidence: Tech and the future of UK foreign policy, HC 201" *House of Commons* (7 September 2021) <https://committees.parliament.uk/oralevidence/2662/pdf/> (accessed 09/11/21)
[9] Samantha Subin, "Palantir CEO says companies working with US adversaries should justify their position" *CNBC News* (23 November 2021) <https://www.cnbc.com/2021/11/23/palantir-ceo-companies-working-with-us-adversaries-should-justify-their-position-.html> (accessed 02/12/21)
[10] Ian Bremmer, "The Technopolar Moment: How Digital Powers Will Reshape the Global Order." *Foreign* Affairs (New York, N.Y.) 100.6 (2021): 112-28.

comparisons to be made between the two governments' use of their tech private sectors in their competition with each other.

6.2. Limitations and Directions for Future Research

In this section, I identify and address three limitations of my study. First, due to the contemporary nature of the topic and the challenges in accessing relevant interviewees, including political elite and tech industry representatives, data collection proved difficult. Accessing current employees and prominent figures within Big Tech was especially challenging, as they often refrained from sharing confidential insights. Whilst interviewees' perspectives were recent, this also meant their responses were likely influenced by their political or corporate affiliations, potentially obscuring their genuine convictions. However, the contemporaneity of the topic also brought an advantage: interviewees were recounting current events rather than recalling past ones, which often distorts reality.

To mitigate these data collection challenges, I ensured that the aim of the interviews was not to obtain the opinion of a large cohort of policymakers and company representatives, but rather to gain insights from high-level officials and employees who could provide otherwise inaccessible information. Moreover, I triangulated the words of high-level officials and employees with colleagues to ensure the information was truthful. Finally, my use of interviews is supplemented by an extensive use of secondary sources, treating them as public information, and acknowledging their potential bias.

The second limitation is related to the risks of conducting research on contemporary topics, as situations are evolving rapidly, especially in the realm of technology. Nevertheless, there is value in conducting research on a specific phenomenon within a specific timeframe with no knowledge of what may occur in the future. Aside from attempting to make sense of a complex reality, it can provide insights, or at the very least contribute to conversations, among scholarly,

policymaking and industry spheres on issues such as the rise of tech embassies in Silicon Valley and the increase of 'technology strategists' in companies working as quasi-diplomats. Such developments have consequences on our understanding of the role of non-state actors in global political dynamics. To address the concern of contemporaneity, I incorporated historical contexts into the literature review, contextualising current phenomena within a broader historical narrative.

Finally, the overarching variables of this study – the US approach to tech policy (independent variable) and the US standing in the tech war (dependent variable) – presented challenges due to their abstract nature and difficulty in direct quantification. To address this, I deconstructed these broad concepts into more observable and specific variables, enabling a more focused and rigorous analysis. The articles-based format of the thesis allowed for an examination of these variables separately, to ensure that that the overarching independent variable and dependent variable did not become aggregated. I believe the thesis as a whole provides a foundation for future research to further understand democratic states' tech policies at a time when authoritarian models appear more straightforward. In addition, each article, besides making a discrete contribution of its own to a concrete debate, lays the groundwork for future research. Article 1 paves the way for comparative studies on data localisation policies globally, an increasingly relevant topic. Article 2 opens avenues for exploring the variability of US influence across different sectors of critical national infrastructure (CNI) and US allies. Article 3's development of the 'geopolitical postures' concept invites further investigation across states and sectors, bridging the gap between the private sector and IR.

6.3. Implications of Findings

In this section, I discuss the broader implications of the findings of the study as a whole. First, this thesis reveals the complexities faced by states and policymakers in an increasingly

technology-driven international landscape. In this era of the 'fourth industrial revolution,'[11] developing long-term strategies for tech policy is difficult due to the rapid pace of technological development and constant regulatory changes. This research shows the necessity for new policy tools and approaches in the 21st century, echoing Madeleine Albright's observation on the disconnect between technological advancements and governmental responses.[12] I provided empirical evidence of the shortcomings of the US's current approach towards its allies and towards its tech companies. However, the wider implications apply to all states: crafting new tech policies and their foreign policy dimensions will require a focus on alliance building to successfully realise strategic objectives. In addition, I show the vital importance of aligning tech policies with foreign policies. As technological advancements reshape the global landscape, a deeper understanding of technology's implications on foreign policy becomes essential. The evidence I presented in Article 1 suggests the need for policymakers to possess a sophisticated grasp of technical aspects to avoid missteps in strategic decision-making.

Second, the role of alliances in crafting effective tech policies emerged as a pivotal takeaway of my thesis. As I detailed in Article 1, retaining tech superiority also entails setting the norms of how the internet and data should be governed. Scholars once perceived a strong alignment between the US and its allies on 'data sovereignty.' Dana Polatin-Reuben and Joss Wright in 2014 categorised approaches to data sovereignty into two camps: the US and its allies viewing data localisation as 'a threat to a free and open global internet,' whilst states like such as Russia, China and Brazil advocate 'for data sovereignty as a way of securing sensitive national data from foreign surveillance.'[13] In both Articles 1 and 2, I show that this is no longer the case. Particularly in Article 1, I trace how three significant events have eroded the

[11] Klaus Schwab and Nicholas Davis, *Shaping the future of the fourth industrial revolution*. Currency, 2018.
[12] Maggie Tennis, "Madeleine Albright on fascism, democracy and diplomacy." *Brookings Institute* (11 September 2018) <https://www.brookings.edu/articles/madeleine-albright-on-fascism-democracy-and-diplomacy/> (accessed 11/10/23)
[13] Polatin-Reuben and Wright, "An Internet with BRICS Characteristics"

confidence of EU member states in US leadership and US companies in the technological realm: the Snowden revelations, the Schrems decisions, and the US CLOUD Act. An important takeaway is that in an age of technological developments, coordinating and collaborating with allies on different standards of privacy and individual rights is crucial to develop effective long-term tech strategies which are mutually beneficial for governments and companies alike. This also means that traditional alliance dynamics may be challenged in the coming years.

Indeed, in the literature review chapter I touched on the concept of weaponised interdependence which Henry Farrell and Abraham L. Newman coin to explain that 'states with political authority over the central nodes in the international networked structures through which money, goods and information travel are uniquely positioned to impose costs on others.'[14] They point out that if its allies decide that the US has been 'abusing' weaponised interdependence in ways that conflict their core interests, they will defect. In particular, US West European allies are most likely to have control 'over key nodes in global networks, or to be credibly able to set up their own alternatives.'[15] Through this thesis, I confirm that the current non-cooperative approach embraced by the US in its alliance management has contributed to this defection among its allies. The US's diminishing appeal and credibility among its allies represents a critical development in the field of IR, signalling a potential shift in global alliances and power dynamics.

Third, my thesis addresses tech companies' growing influence in IR. Whilst some pundits have suggested granting tech giants like Amazon and Facebook seats at the United Nations,[16] others have expressed concern over their potential to challenge democratic governments.[17] I

[14] Henry Farrell and Abraham L. Newman. "Weaponized interdependence: How global economic networks shape state coercion." *International Security* 44, no. 1 (2019): 42-79. p.45
[15] *ibid.* p.78
[16] Ben Schott, "Give Amazon and Facebook a Seat at the United Nations" *Bloomberg* (3 October 2021) <https://www.bloomberg.com/opinion/articles/2021-10-03/give-amazon-and-facebook-a-seat-at-the-united-nations> (accessed 28/09/22)
[17] Foreign Affairs Committee, "Oral Evidence: Tech and the future of UK foreign policy, HC 201" *House of Commons* (2 November 2021) <https://committees.parliament.uk/oralevidence/2955/pdf/> (accessed 10/11/21)

question the extent of their influence and suggested limits to their significance in global policy. In Article 3, I explore how in a democratic state model like the US, even companies that are seemingly aligned with the government can give precedence to profit motives, particularly in lucrative markets such as China. This may lead us to be more cautious in overestimating their role in international politics, as states retain the power to regulate the digital.

Moreover, I sought to deepen our understanding of the roles tech companies play in state tech policies. Whilst the discussion of how states *should* involve tech companies in their tech policies falls beyond the scope of my research, my findings shed light on crucial considerations for future exploration. I characterised the US government's approach to industry partnerships as laissez-faire, which can be contrasted to the China's more interventionist approach. This distinction is important in understanding how tech policy varies between states, especially in tactics like trade protectionism, cyber espionage, or pressuring allies against engaging with rival tech companies. I discussed in Article 2 how the US government has been pressuring its allies not to adopt Huawei's 5G technology. The use of allies in efforts to undermine the others' tech companies is important because it allows governments to amplify their reach and impact. If the US government is able to convince its allies not to do business with Huawei, it will have a much greater impact on Huawei's business than if the US government were to try to undermine Huawei on its own.

A key question emerges regarding the future of US tech policy: is it in the US government's best interests that its tech companies follow a logic of profit maximisation? In other words, is it strategically beneficial for the US government to ensure its tech giants remain powerful players in its global technological competition with China by allowing maximum flexibility in their business interactions? My aim for Article 3 was to challenge the argument that US Big Tech companies have geopolitical postures which explain crucial company decisions. I did not make value judgements on whether they *should* have geopolitical postures and how closely

they *should* espouse American ideals. However, the strategic losses the US is facing in the tech war reveal the need to explore alternative approaches to its current non-cooperative and laissez-faire approach.

A democratic state like the US would require a tailored, flexible tech policy. It is important to note that the US and China have very different political and economic systems. What works for China is very likely not to be appropriate for the US. Therefore, the US would need to tailor its tech policy to its own political and economic system, accounting for the aims of this policy. In terms of private sector management, this might involve the US government fostering national security partnerships and acting as a genuine partner to tech companies in information sharing and technology purchasing.[18] As opposed to a form of industrial policy, such an approach would recognise the agency of the tech companies themselves and would therefore require the recognition of mutual long-term interests of both the state and tech companies.

Luciano Floridi explains that tech companies possess 'poietic' power to create new technologies and shape the digital landscape, therefore controlling the nature and speed of change.[19] On the other hand, states possess the power to regulate the digital world by setting laws, providing incentives and disincentives, and determining tax rates, therefore controlling the direction of change.[20] This framework points to a relationship where both parties are interdependent and vulnerable to each other's actions. For the state, tech companies are crucial innovators and economic drivers; for tech companies, the state provides the legal and infrastructural framework of their operations. This interdependence suggests that collaborative efforts would have to be mutually beneficial, such as through two-way information sharing, yet cautiously navigated to ensure privacy and data protection. Alternatively, the US could maintain its current laissez-faire approach, which has its own trade-offs in both its domestic

[18] Kitchen, "The New Superpowers"
[19] Luciano Floridi, "The fight for digital sovereignty: What it is, and why it matters, especially for the EU." *Philosophy & technology* 33 (2020): 369-378. p.371
[20] *ibid.*

context and in its competition with China. Balancing these considerations is key to developing a forward-looking tech policy that effectively harnesses the strengths of both the state and the tech sector.

Finally, my findings indicate that the US would benefit by focusing on alliance building and developing collaborative, mutually beneficial public-private partnerships with the tech industry to successfully realise its strategic objectives. This would require a focus on norm-setting, as well as a commitment to open societies and international cooperation. The pursuit of a flexible tech policy would be key to maintaining global influence in an era defined by technological competition and collaboration. Overall, this thesis addresses the complexities of US tech policy and its global implications, whilst also demonstrating the analytical benefits of anchoring technology-related studies in a more robust framework derived from international relations concepts.

Bibliography

AmCham EU, BSA, CCIA Europe, ITI. “European Cybersecurity Certification Scheme for Cloud Services” (14 June 2022) <https://www.itic.org/documents/europe/Final_EUCS_statement_1406.pdf> (accessed 11/04/23)

Apple Inc., *Annual Report Pursuant to Section 13 or 15(D) of the Securities Exchange Act of 1934,* United States Securities and Exchange Commission, Washington D.C. (2018)

Assaf, Dan. "Foreign Direct Investment in an Era of Increased Threats to Critical Infrastructures." In *Critical Infrastructure Protection IV: Fourth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, ICCIP 2010, Washington, DC, USA, March 15-17, 2010, Revised Selected Papers 4*, pp. 17-27. Springer Berlin Heidelberg, 2010.

Ayson, Robert. "The coercive power of shared values." *Political Science* 70, no.3 (2018)

Ayson, Robert. “NZ’s useful Huawei ambiguity” *Newsroom* (16 January 2020) <https://www.newsroom.co.nz/ideasroom/the-ban-that-isnt-new-zealand-and-huawei> (accessed 31/03/22)

Barnes, Julian and Adam Satariano. “US Campaign to Ban Huawei Overseas Stumbles as Allies Resist.” *The New York Times* (17 March 2019) <https://www.nytimes.com/2019/03/17/us/politics/huawei-ban.html> (accessed 17/03/20)

Barnet Richard J., and Ronald E. Müller. *Global Reach: The Power of the Multinational Corporations*. London: Jonathan Cape, 1975.

Barnett, Michael. "Culture, strategy and foreign policy change: Israel's road to Oslo." *European Journal of International Relations* 5, no.1 (1999)

Bary, Andrew. “Big 5 Tech Stocks Now Account for 23% of the S&P 500” *Barrons* (26 July 2021) <https://www.barrons.com/articles/big-tech-stocks-sp-500-51627312933?tesla=y> (accessed 03/01/22)

Bateman, Jon. “Biden is Now All-In on Taking Out China” *Foreign Policy* (12 October 2022) <https://foreignpolicy.com/2022/10/12/biden-china-semiconductor-chips-exports-decouple/> (accessed 12/10/22)

Bauer, Matthias, Hosuk Lee-Makiyama, Erik Van der Marel, and Bert Verschelde. *The costs of data localisation: Friendly fire on economic recovery*. No. 3/2014. ECIPE Occasional Paper, 2014

BBC. “China says Microsoft hacking accusations fabricated by US and allies” *BBC News* (20 July 2021) <https://www.bbc.co.uk/news/world-asia-china-57898147> (accessed 08/02/22)

BBC. “Hong Kong security law: What is it and why is it worrying?” *BBC News* (30 June 2020) <https://www.bbc.co.uk/news/world-asia-china-52765838> (accessed 03/11/20)

BBC. “Hong Kong: UK makes citizenship offer to residents” *BBC News* (1 July 2020) <https://www.bbc.com/news/uk-politics-53246899> (accessed 30/03/22)

BBC. “Huawei row: Australian MPs cancel UK trip amid tensions over leak” *BBC News* (15 February 2020) <https://www.bbc.com/news/world-australia-51513886> (accessed 31/03/22)

BBC. “Huawei: China attacks UK’s ‘groundless’ ban of 5G kit” *BBC News* (15 July 2020) <https://www.bbc.co.uk/news/technology-53412678> (accessed 15/07/20)

BBC. “Huawei: Government wins vote after backbench rebellion” *BBC News* (10 March 2020) <https://www.bbc.co.uk/news/uk-politics-51806704> (accessed 08/05/20)

BBC. “Huawei: MPs attack government over decision for 5G networks” *BBC News* (28 January 2020). <https://www.bbc.co.uk/news/uk-politics-51278305> (accessed 28/01/20)

Beach, Derek and Rasmus Brun Pedersen. *Process-tracing methods: Foundations and guidelines*. University of Michigan Press, 2019.

Bennett, Andrew, and Jeffrey T. Checkel, eds. *Process tracing*. Cambridge University Press, 2015.

Bertuzzi, Luca. “EU countries seek way out of impasse on sovereignty requirements for cloud services” *EURACTIV* (30 January 2023) <https://www.euractiv.com/section/cybersecurity/news/eu-countries-seek-way-out-of-impasse-on-sovereignty-requirements-for-cloud-services/> (accessed 08/03/23)

Bertuzzi, Luca. “Is data localisation coming to Europe?” *International Association of Privacy Professionals* (23 August 2022) <https://iapp.org/news/a/is-data-localization-coming-to-europe/> (accessed 11/03/23)

Blatchford, Andy. “Canada joins Five Eyes in ban on Huawei and ZTE” *Politico* (19 May 2022) <https://www.politico.com/news/2022/05/19/canada-five-eyes-ban-huawei-zte-00033920> (accessed 20/05/2022)

Booth, William, Jeanne Whalen and Ellen Nakashima. “Britain, resisting US pressure, to allow some Huawei equipment in 5G networks” *The Washington Post* (28 January 2020) <https://www.washingtonpost.com/world/europe/britain-resisting-us-pressure-to-allow-some-huawei-equipment-in-5g-networks/2020/01/28/52e708b4-4145-11ea-99c7-1dfd4241a2fe_story.html>(accessed 31/01/20)

Bourke, Latika. “Australian MPs delivers stunning rebuke to UK’s Dominic Raab on Huawei” *The Sydney Morning Herald* (7 February 2020) <https://www.smh.com.au/world/europe/australian-mp-delivers-stunning-rebuke-to-uk-s-dominic-raab-on-huawei-20200206-p53yjg.html> (accessed 31/03/22)

Bowler, Tim. “Huawei: Why is it being banned from the UK’s 5G network?” *BBC News* (14 July 2020) <https://www.bbc.com/news/newsbeat-47041341> (accessed 17/11/20)

Bradford, Anu. *The Brussels effect: How the European Union rules the world*. Oxford University Press, USA, 2020

Bremmer, Ian. "The Technopolar Moment: How Digital Powers Will Reshape the Global Order." *Foreign* Affairs (New York, N.Y.) 100.6 (2021): 112-28.

Briscoe, Forrest, and Abhinav Gupta. “Business Disruption From the Inside Out” *Stanford Social Innovation Review* 19, no. 1 (2020): 48-54

British Foreign Policy Group, “China’s Belt and Road Initiative: *Towards a British Response Strategy – Student Ambassador Series* (10 April 2019) <https://bfpg.co.uk/2019/04/chinas-belt-and-road-initiative-towards-a-british-response-strategy/> (accessed 01/02/20)

Brown, Michael, and Robert Atkinson. “The Real Contest with China,” *Foreign Affairs* (28 August 2023) <https://www.foreignaffairs.com/china/real-contest-beijing-industrial-strategy> (accessed 28/09/23)

Buchan, Lizzy. “Boris Johnson facing Tory revolt over Huawei 5G decision” *The Independent* (6 March 2020) <https://www.independent.co.uk/news/uk/politics/boris-johnson-huawei-5g-decision-trump-tories-a9380561.html> (accessed 10/03/20)

Bureau of Industry and Security, “Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List” *Department of Commerce,* Docket No. 200514-0100, RIN 0694-AH99 (15 May 2020) pp.29849-29863.

Caluag, Iris May Ellen Y. "The Political Power of Global Corporations, written by John Mikler." *Philippine Political Science Journal* 42, no. 1 (2021): 90-94.

Campbell, Mikey. “Peter Thiel calls Apple’s relationship with China a real problem” *Apple Insider* (7 April 2021) <https://appleinsider.com/articles/21/04/07/peter-thiel-calls-apples-relationship-with-china-a-real-problem> (accessed 20/12/21)

Campion, Andrew Stephen. "From CNOOC to Huawei: securitization, the China threat, and critical infrastructure." *Asian Journal of Political Science* 28, no.1 (2020)

Cartwright, Madison. "Internationalising state power through the internet: Google, Huawei and geopolitical struggle." *Internet Policy Review* 9, no. 3 (2020): 1-18.

Celeste, Edoardo. "Digital sovereignty in the EU: challenges and future perspectives." *Data protection beyond borders: Transatlantic perspectives on extraterritoriality and sovereignty* (2021): 211-228

Chee, Foo Yun. “Tech-sponsored study criticises plan to exclude non-EU cloud vendors” *Reuters* (6 March 2023) <https://www.reuters.com/technology/tech-sponsored-study-criticises-plan-exclude-non-eu-cloud-vendors-2023-03-06/> (accessed 12/04/23)

China Strategy Group, "Asymmetric Competition: A Strategy for China and Technology: Actionable Insights for American Leadership" (Fall 2020) <http://industrialpolicy.us/resources/SpecificIndustries/IT/final-memo-china-strategy-group-axios-1.pdf> (accessed 12/10/21)

Clarke, Laurie. "UK MP to US congressman: Huawei is already out of the 5G network" *New Statesman* (16 June 2020) <https://tech.newstatesman.com/security/uk-mp-us-congressman-huawei-5g-network> (accessed 21/06/20)

Connolly, Amanda, and Alex Boutilier. "Canada's Huawei decision was picking up momentum 2 years ago. So what is happening?" *Global News* (1 December 2021) <https://globalnews.ca/news/8414227/canada-huawei-ban-timeline/> (accessed 31/03/22)

Connolly, Amanda. "Huawei, Meng Wanzhou hit with new racketeering, corporate espionage charges in US" *Global News* (13 February 2020) <https://globalnews.ca/news/6547303/doj-adds-huawei-charges/> (accessed 05/05/20)

Cook, Katy, *The Psychology of Silicon Valley: Ethical Threats and Emotional Unintelligence in the Tech Industry*. Basingstoke, 2020.

Cooper, Charlie. "Britain toughens stance on China as it eyes US" *Politico* (13 July 2020) <https://www.politico.com/news/2020/07/13/boris-johnson-china-huawei-359741> (accessed 14/07/20)

Corera, Gordon. "Huawei: UK prepares to change course on 5G kit supplier" *BBC News* (20 February 2019) <https://www.bbc.co.uk/news/technology-47305420> (accessed 03/03/20)

Cory, Nigel, and Luke Dascoli. "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them" *Information Technology and Innovation Foundation* (July 2021) <https://www.gmfus.org/sites/default/files/2023-03/Report%20-%20The%20New%20American%20Foreign%20Policy%20of%20Technology_1.pdf > (accessed 11/03/22)

Cory, Nigel. "Europe's Cloud Security Regime Should Focus on Technology, Not Nationality" *Information Technology and Innovation Foundation* (27 March 2023) <https://itif.org/publications/2023/03/27/europes-cloud-security-regime-should-focus-on-technology-not-nationality/> (accessed 12/04/23)

Cory, Nigel. "France's "Sovereignty Requirements" for Cybersecurity Services Violate WTO Trade Law and Undermine Transatlantic Digital Trade and Cybersecurity Cooperation" (10 May 2022) <https://itif.org/publications/2022/05/10/france-sovereignty-requirements-cybersecurity-services-violate-wto-trade/#> (accessed 20/04/23)

Cory, Nigel. "Sovereignty Requirements in French – and potentially EU-Cybersecurity regulations: The latest barrier to data flows, digital trade, and digital cooperation among likeminded partners" *Information Technology and Innovation Foundation* (10

December 2021) <https://itif.org/publications/2021/12/10/sovereignty-requirements-france-and-potentially-eu-cybersecurity/> (accessed 11/04/23)

Cox, James Samuel. *Canada and the five eyes intelligence community*. Canadian Defence & Foreign Affairs Institute, 2013.

Daalder, Ivo. "Commentary: Britain sticks with Huawei for 5G – and jeopardises the Five Eyes alliance." *Chicago Tribune*. (30 January 2020) <https://www.chicagotribune.com/opinion/commentary/ct-opinion-5g-huawei-britain-ivo-daalder-20200130-xympy43dovds7m3gs4fvn5xapq-story.html> (accessed 31/01/20)

Davis, Nicholas, Landry Signé, and Mark Esposito, "Rethinking technology policy and governance for the 21st century" *Brookings Institute* (11 January 2022) <https://www.brookings.edu/articles/rethinking-technology-policy-and-governance-for-the-21st-century/> (accessed 11/09/23)

Dawson, Bethany. "Amazon booster its business in China by blocking reviews on books by leader Xi Jinping and following Communist Party 'edicts' says Reuters investigation" *Business Insider* (18 December 2021) <https://www.businessinsider.fr/us/amazon-collaborated-with-chinas-propaganda-arm-to-boost-sales-reuters-2021-12> (accessed 21/12/21)

De Coninck, Heleen, Carolyn Fischer, Richard G. Newell, and Takahiro Ueno. "International technology-oriented agreements to address climate change." *Energy Policy* 36, no. 1 (2008): 335-356.

Delcker, Janosch and Melissa Heikkila. "Germany, France launch Gaia-X platform in bid for 'tech sovereignty.'" *Politico* (4 June 2020) <https://www.politico.eu/article/germany-france-gaia-x-cloud-platform-eu-tech-sovereignty/> (accessed 09/03/23)

Department for Digital, Culture, Media and Sport. "Huawei to be removed from UK 5G networks by 2027." *GOV.UK.* (14 July 2020) <https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027> (accessed 15/07/20)

Devonshire-Ellis, Chris. "China's Belt and Road Initiative and the United Kingdom" *Silk and Road Briefing* (13 June 2018) <https://www.silkroadbriefing.com/news/2019/06/05/chinas-belt-road-initiative-united-kingdom/> (accessed 12/04/20)

Dutch Authority for Digital Infrastructure, "Cloud Certification" <https://www.dutchncca.nl/certification-schemes/cloud-certification> (accessed 14/03/23)

E&T, "Tory rebellion threatens Huawei's future in 5G rollout" *Engineering & Technology Magazine.* (17 April 2020) <https://eandt.theiet.org/content/articles/2020/04/tory-rebellion-threatens-huawei-s-future-in-5g-rollout/> (accessed 17/04/20)

Embassy of the People's Republic of China in the United States of America, "Bill Gates bats

for China" (27 January 2010) <https://www.mfa.gov.cn/ce/ceus/eng/xw/t654165.htm> (accessed 08/02/22)

European Union. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)." *Official Journal of the European Union*, vol. 59, no. 1, 4 May 2016, pp.1-88.

European Union Agency for Cybersecurity (ENISA), "EUCS – Cloud Services Scheme" (December 2020) <https://ec.europa.eu/newsroom/cipr/items/713799/en> (accessed 25/02/23)

Facebook, "The Facebook Code of Conduct" <https://s21.q4cdn.com/399680738/files/doc_downloads/governance_documents/2021/06/FB-Code-of-Conduct.pdf> p.56 (accessed 07/02/22)

Fairbank, Nancy Ayer. "The state of Microsoft?: the role of corporations in international norm creation." *Journal of Cyber Policy* 4, no. 3 (2019): 380-403.

Farrell, Henry, and Abraham L. Newman. "Weaponized interdependence: How global economic networks shape state coercion." *International Security* 44, no. 1 (2019): 42-79.

Feiner, Lauren. "Google sacrificed its 'don't be evil' mantra to grow bigger, former exec says" *CNBC* (2 January 2020) <https://www.cnbc.com/2020/01/02/google-abandoned-its-dont-be-evil-mantra-former-exec-says.html> (accessed 06/02/22)

Field, Matthew. "Cutting out Huawei from 5G network would cost Britain £7bn" *The Telegraph* (5 April 2019) <https://www.telegraph.co.uk/technology/2019/04/04/cutting-huawei-5g-network-would-cost-britain-7bn/> (accessed 12/11/20)

Floridi, Luciano. "The fight for digital sovereignty: What it is, and why it matters, especially for the EU." *Philosophy & technology* 33 (2020): 369-378.

Ford, Jonathan, and Laura Hughes, "UK-China relations: from 'golden era' to the deep freeze." *Financial Times.* (14 July 2020). <https://www.ft.com/content/804175d0-8b47-4427-9853-2aded76f48e4> (accessed 15/07/20)

Ford, Jonathan. "UK's reliance on China's nuclear tech poses test for policymakers" *Financial Times* (14 February 2019). <https://www.ft.com/content/7734e3be-2f6f-11e9-8744-e7016697f225> (accessed 15/03/20)

Foreign Affairs Committee, "Oral Evidence: Tech and the future of UK foreign policy, HC 201" *House of Commons* (2 November 2021) <https://committees.parliament.uk/oralevidence/2955/pdf/> (accessed 10/11/21)

Foreign Affairs Committee, "Oral Evidence: Tech and the future of UK foreign policy, HC 201" *House of Commons* (7 September 2021)

<https://committees.parliament.uk/oralevidence/2662/pdf/> (accessed 09/11/21)

Foreign Affairs Committee, "Oral Evidence: Tech and the future of UK foreign policy, HC 201" *House of Commons* (11 January 2022) <https://committees.parliament.uk/oralevidence/3247/pdf/> (accessed 11/01/22)

Foreign Policy. "5G Explained: Part One—Technology and Infrastructure." (2020) <https://foreignpolicy.com/2020/01/22/5g-cellular-huawei-china-networks-technology-infrastructure-power-map/> (accessed 25/02/20)

Foreign, Commonwealth and Development Office. "UK and allies hold Chinese state responsible for a pervasive pattern of hacking" *GOV.UK* (19 July 2021) <https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking> (accessed 08/02/22)

Foroohar, Rana. "Concentrated Power in Big Tech Harms the US." *Financial Times* (Sep 27, 2020). <https://www.proquest.com/trade-journals/concentrated-power-big-tech-harms-us/docview/2467985467/se-2.> (accessed 01/10/23)

Forrester. "LinkedIn Has Not Given Up on the Chinese Market" *Forbes* (21 October 2021) <https://www.forbes.com/sites/forrester/2021/10/21/linkedin-has-not-given-up-on-the-china-market/?sh=7ce10bd53d42> (accessed 02/01/22)

Frontier Economics, "The Extent and Impact of Data Localisation: Report prepared for DCMS" (1 June 2022) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1125805/Frontier_Economics_-_data_localisation_report_-_June_2022.pdf> (accessed 15/03/22)

Gallagher, Ryan. "Google Employees Uncover Ongoing Work on Censored China Search" *The Intercept* (4 March 2019) <https://theintercept.com/2019/03/04/google-ongoing-project-dragonfly/> (accessed 04/01/22)

Gallagher, Ryan. "Leaked Transcript of Private Meeting Contradicts Google's Official Story on China" *The Intercept* (9 October 2018) <https://theintercept.com/2018/10/09/google-china-censored-search-engine/> (accessed 06/02/22)

Gates, Robert M. "The Dysfunctional Superpower: Can a Divided America Deter China and Russia?" *Foreign Affairs* (29 September 2023) <https://www.foreignaffairs.com/united-states/robert-gates-america-china-russia-dysfunctional-superpower#author-info> (accessed 29/09/23)

Gilli, Andrea. "NATO and 5G: What Strategic Lesson?" *NDC Policy Brief, No.13* (2020)

Girma, Sourafel, David Greenaway, and Katharine Wakelin. "Who benefits from foreign direct investment in the UK?." *Scottish journal of political economy* 48, no. 2 (2001): 119-133.

Global Times. “China aims to become world leading technological power by 2049” *Global Times* (24 September 2012) <https://www.globaltimes.cn/content/734882.shtml> (accessed 09/10/23)

Google. “10 things we know to be true” <https://about.google/philosophy/> (accessed 04/01/22)

Google. “A new approach to China: an update” *Google Official Blog* (22 March 2010) <https://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html> (accessed 06/02/22)

Goujard, Clothilde and Laurens Cerulus. “Inside GAIA-X: How chaos and infighting are killing Europe’s grand cloud project” *Politico* (26 October 2021) <https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/> (accessed 01/04/23)

Goure, Dan. “The US Needs to Harness Big Tech to Compete with China” *The National Interest* (14 September 2022) <https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/us-needs-harness-big-tech-compete> (accessed 03/07/22)

Gramer, Robbie and Lara Seligman. “Can the US-UK Special Relationship Weather the Huawei Storm?” *Foreign policy* (30 January 2020) <https://foreignpolicy.com/2020/01/30/huawei-intelligence-united-states-britain-trump-5g-infrastructure-concerns-digital-espionage-special-relationship-five-eyes/> (accessed 04/02/20)

Greene, Robert and Paul Triolo, “Will China Control the Global Internet Via its Digital Silk Road?” *Carnegie Endowment for International Peace*. (8 May 2020) <https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857> (accessed 22/09/20)

Halpern, Sue. “The Terrifying Potential of the 5G Network” *The New Yorker* (26 April 2019) <https://www.newyorker.com/news/annals-of-communications/the-terrifying-potential-of-the-5g-network> (accessed 07/08/20)

Hare, Stephanie, "For your eyes only: US technology companies, sovereign states, and the battle over data protection." *Business Horizons* 59, no. 5 (2016): 549-561.

Harvey, Glenn. “Thousands of contracts highlight quiet ties between Big Tech and US military” *NBC News* (July 8, 2020) <https://www.nbcnews.com/tech/tech-news/thousands-contracts-highlight-quiet-ties-between-big-tech-u-s-n1233171> (accessed 26/11/21)

Heinrich, Thomas, "Cold war armory: military contracting in Silicon Valley." *Enterprise & Society* 3, no. 2 (2002): 247-284.

Helberg, Jacob. “Silicon Valley Can’t Be Neutral in the US-China Cold War” *Foreign Policy* (June 22, 2020) <https://foreignpolicy.com/2020/06/22/zoom-china-us-cold-war-unsafe/> (accessed 04/12/21)

Helm, Toby. “Pressure from Trump led to 5G ban, Britain tells Huawei” *The Guardian* (18 July 2020) <https://www.theguardian.com/technology/2020/jul/18/pressure-from-trump-led-to-5g-ban-britain-tells-huawei> (accessed 18/08/20)

Helvey, David. “Europe and the US must stand together on China” *Financial Times* (3 February 2020) <https://www.ft.com/content/a47faf4a-42b3-11ea-9a2a-98980971c1ff?shareType=nongift> (accessed 04/03/20)

Hemmings, John. “The UK risks plunging the Five Eyes alliance into crisis” *The Telegraph* (4 March 2020) <https://www.telegraph.co.uk/politics/2020/03/04/uk-risks-plunging-five-eyes-alliance-crisis/> (accessed 20/06/20)

Hilliard, Wesley. “Congress members demand Apple exit China in letter to Tim Cook” *Apple Insider* (21 May 2021) <https://appleinsider.com/articles/21/05/21/congress-members-demand-apple-exit-china-in-letter-to-tim-cook> (accessed 18/01/22)

Ho, Vanessa. “Chinese President Xi Jinping visits Microsoft, sees potential of new technology” *Microsoft News* (23 September 2015) <https://news.microsoft.com/features/chinese-president-xi-jinping-visits-microsoft-sees-potential-of-new-technology/> (accessed 21/12/21)

Hudson, Valerie M. "Foreign policy analysis: Actor-specific theory and the ground of international relations." *Foreign policy analysis* (2005): 1-30.

Hui, Sylvia. “UK-China ties freeze with debate over Huawei, Hong Kong” *AP News* (13 July 2020) <https://apnews.com/article/ab544e59150aa75dce22a4aff9c79d78> (accessed 15/07/20)

Jaisal, E. K. "The US, China and Huawei Debate on 5G Telecom Technology: Global Apprehensions and the Indian Scenario." *Open Political Science* 3, no.1 (2020)

Jakobsson, A. J., and M. S. Stolz. "Principled Big Tech: European pursuit of technological autonomy." *Finnish Institute of International Affairs* (2021).

Jie, Yu, and Joyce Hakmeh, “The UK’s Huawei Decision: Why the West is Losing the Tech Race” *Chatham House* (17 July 2020) <https://www.chathamhouse.org/2020/07/uks-huawei-decision-why-west-losing-tech-race> (accessed 17/07/20)

Kabelka, Laura. “Sovereignty requirements remain in cloud certification scheme despite backlash” *EURACTIV* (16 June 2022) <https://www.euractiv.com/section/cybersecurity/news/sovereignty-requirements-remain-in-cloud-certification-scheme-despite-backlash/> (accessed 12/04/23)

Kanno-Youngs, Zolan, and David E. Sanger. “US accuses China of hacking Microsoft” *The New York Times* (19 July 2021) <https://www.nytimes.com/2021/07/19/us/politics/microsoft-hacking-china-biden.html> (accessed 21/12/21)

Karp, Alex. “I’m a tech CEO, and I don’t think tech CEOs should be making policy” *The*

Washington Post (September 5, 2019) <https://www.washingtonpost.com/opinions/policy-decisions-should-be-made-by-elected-representatives-not-silicon-valley/2019/09/05/e02a38dc-cf61-11e9-87fa-8501a456c003_story.html> (accessed 03/05/22)

Kaska, Kadri, Henrik Beckvard and Tomas Minarik. "Huawei, 5G and China as a security threat." *NATO Cooperative Cyber Defence Center for Excellence* 28 (2019)

Kelion, Leo. "Huawei: Why the UK might hang up on 5G and broadband kit supplier" *BBC News* (10 July 2020) <https://www.bbc.co.uk/news/technology-53341080> (accessed 14/07/20)

Kharpal, Arjun. "China starts development of 6G having just turned on its 5G mobile network" *CNBC* (7 November 2019) <https://www.cnbc.com/2019/11/07/china-starts-6g-development-having-just-turned-on-its-5g-mobile-network.html> (accessed 02/01/20)

Kharpal, Arjun. "Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice." *CNBC* (4 March 2019) <https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html> (accessed 05/05/20)

Kharpal, Arjun. "Our special relationship is less special: UK-US bond tested by Britain's Huawei 5G decision" *CNBC* (29 January 2020) <https://www.cnbc.com/2020/01/29/uk-us-relationship-tested-with-britain-huawei-5g-decision.html> (accessed 03/02/20)

Kim, Patricia M., Matthew Turpin, Joseph S. Nye Jr., Jessica Chen Weiss, and Eun A Jo Ryan Hass and Emilie Kimball. "Should the US pursue a new Cold War with China?" *Brookings Institute* (1 September 2023) <https://www.brookings.edu/articles/should-the-us-pursue-a-new-cold-war-with-china/> (accessed 02/10/23)

Kitchen, Klon. "The New Superpowers: How and Why the Tech Industry is Shaping the International System" *National Affairs,* Number 29 (Fall 2021) <https://nationalaffairs.com/the-new-superpowers-how-and-why-the-tech-industry-is-shaping-the-international-system> (accessed 29/11/21)

Klaas, Brian. "The world is horrified by the dysfunction of American democracy" *The Washington Post* (11 June 2021) <https://www.washingtonpost.com/opinions/2021/06/11/pew-research-global-opinion-us-democracy/> (accessed 02/10/23)

Komaitis, Konstantinos. "The 'wicked problem' of data localisation." *Journal of Cyber Policy* 2, no. 3 (2017): 355-365.

Kornbluh, Karen and Julia Tréhu, "The New American Foreign Policy of Technology: Promoting Innovation, National Security and Democratic Values in a Digital World" *GMF Policy Report* (March 2023) <https://www.gmfus.org/sites/default/files/2023-03/Report%20-\%20The%20New%20American%20Foreign%20Policy%20of%20Technology_1.pd>

(accessed 15/04/23)

Landale, James. “UK Huawei decision part of wider strategic tensions with China” *BBC News* (12 July 2020) <https://www.bbc.co.uk/news/world-asia-china-53366301> (accessed 12/07/20)

Landler, Mark and Stephen Castle. “Johnson Risks a Rift with Trump by Granting New Access to Huawei” *The New York Times* (28 January 2020) <https://www.nytimes.com/2020/01/28/world/europe/johnson-trump-hwawei-rift.html?searchResultPosition=7> (accessed 21/02/20)

Landler, Mark. “Google Searches for a Foreign Policy” *New York Times* (27 March 2010) <https://www.nytimes.com/2010/03/28/weekinreview/28landler.html> (accessed 04/11/21)

Lee, Caitlin. “Winning the Tech Cold War” *The Rand Blog* (17 August 2023) <https://www.rand.org/blog/2023/08/winning-the-tech-cold-war.html> (accessed 03/10/23)

Lekkas, Nicolas. “GAFAM: The Big Five Tech Companies Facts (FAAMG)” *GrowthRocks* (18 August 2021) <https://growthrocks.com/blog/big-five-tech-companies-acquisitions/> (accessed 03/01/22)

Leskin, Paige. “Here are all the major US tech companies blocked behind China’s Great Firewall” *Business Insider* (10 October 2019) <https://www.businessinsider.com/major-us-tech-companies-blocked-from-operating-in-china-2019-5?r=US&IR=T> (accessed 03/01/22)

Levick, Laura, and Carsten-Andreas Schulz. "Soft balancing, binding or bandwagoning? Understanding institutional responses to power disparities in the Americas." *Canadian Journal of Political Science/Revue canadienne de science politique* 53, no. 3 (2020): 521-539.

Levy, Ian. “A different future for telecoms in the UK” *National Cyber Security Centre* (14 July 2020) <https://www.ncsc.gov.uk/blog-post/a-different-future-for-telecoms-in-the-uk> (accessed 15/07/20)

Levy, Ian. “The future of telecoms in the UK” *National Cyber Security Centre* (28 January 2020) <https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk> (accessed 01/02/20)

Lewis, James. "New Objectives for CFIUS: Foreign Ownership, Critical Infrastructure, and Communications Interception." *Fed. Comm. LJ* 57 (2004)

Luckenbaugh, Josh. “US better positioned for tech competition than China, report finds” *National Defense* (22 June 2023) <https://www.nationaldefensemagazine.org/articles/2023/6/22/us-better-positioned-for-technological-competition-than-china-report-finds> (accessed 03/10/23)

Maizland, Lindsay. “China’s Repression of Uighurs in Xinjiang” *Council on Foreign Affairs*

(30 June 2020) <https://www.cfr.org/backgrounder/chinas-repression-uighurs-xinjiang> (accessed 03/11/20)

Masters, Brooke. "Apple has too much power over its rivals" *Financial Times* (1 November 2021) <https://www.ft.com/content/94d9f964-10d8-4ff3-9781-821f3fc9ee3a> (accessed 27/12/21)

McCarthy, Daniel R. *Power, information technology, and international relations theory: The power and politics of US Foreign policy and internet*. Palgrave Macmillan, 2015.

McGee, Patrick. "Silicon Valley reboots its relationship with the US military" *The Financial Times* (May 17, 2021) <https://www.ft.com/content/541f0a02-ea27-43a4-b554-96048c40040d> (accessed 30/11/21)

McKay, Hollie. "Microsoft's three-decade history with China under the microscope ahead of potential TikTok acquisition" *Fox Business* (25 August 2020) <https://www.foxbusiness.com/technology/microsofts-three-decade-history-with-china-under-scrutiny-possible-tik-tok-acquisition> (accessed 21/12/21)

McKinsey & Company, "Localisation of data privacy regulations creates competitive opportunities" (30 June 2022) <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities#/> (accessed 16/03/22)

Microsoft. "Corporate Responsibility" <https://www.microsoft.com/en-us/corporate-responsibility/> (accessed 22/12/21)

Microsoft. "Empowerment begins with trust" *Trust Centre* <https://www.microsoft.com/en-us/trust-center> (accessed 22/12/21)

Microsoft. "Our actions" <https://www.microsoft.com/en-us/corporate-responsibility/earn-trust?rtc=1> (accessed 22/12/21)

Microsoft. "Our corporate values" <https://www.microsoft.com/en-us/about/corporate-values> (accessed 22/12/21)

Mikler, John. *The political power of global corporations*. John Wiley & Sons, 2018

Miller, Laura. "Inside Huawei's 5G implosion" *Wired* (21 July 2020) <https://www.wired.co.uk/article/huawei-uk-ban-5g> (accessed 08/08/20)

Mims, Christopher, "Move Over, GE. The Tech Conglomerates Are the New Leaders of Industry" *The Wall Street Journal* (November 27, 2021) <https://www.wsj.com/articles/move-over-ge-tech-conglomerates-amazon-apple-microsoft-are-the-new-leaders-of-industry-11637965497> (accessed 27/11/21)

Moerel, Lokke. "The Ebb and Flow of Trans-Atlantic Data Transfers: It's the Geopolitics, Stupid!" *Future of Privacy Forum* (4 April 2022) <https://fpf.org/blog/the-eb-and-flow-of-trans-atlantic-data-transfers-its-the-geopolitics-stupid/> (accessed 09/03/23)

Morgan, Richard. "Oversight through Five Eyes: Institutional Convergence and the Structure and Oversight of Intelligence Activities." *Global Intelligence Oversight* (2016)

Mozur, Paul, Mark Scott and Mike Isaac. “Facebook faces a new world as officials rein in a Wild Web” *The New York Times* (17 September 2017) <https://www.nytimes.com/2017/09/17/technology/facebook-government-regulations.html> (accessed 06/02/22)

Nakashima, Ellen and William Booth. “Britain bars huawei from its 5G wireless networks, part of a growing shift away from the Chinese tech giant” *The Washington Post,* (15 July 2020) <https://www.washingtonpost.com/national-security/britain-to-bar-huawei-from-its-5g-wireless-networks-part-of-a-growing-shift-away-from-the-chinese-tech-giant/2020/07/13/44f6afee-c448-11ea-b037-f9711f89ee46_story.html> (accessed 01/08/20)

Ni, Vincent. “TechScape: Xi Jinping’s ‘Little Red Book’ of tech regulation could lead the way” *The Guardian* (3 November 2021) <https://www.theguardian.com/technology/2021/nov/03/techscape-china-jack-ma-regulation> (accessed 03/01/22)

Nicas, Jack, Raymond Zhong and Daisuke Wakabayashi. “Censorship, Surveillance and Profits: A Hard Bargain for Apple in China” *The New York Times* (May 17, 2021) <https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html> (accessed 20/12/21)

Nicholls, Dominic. “MI6 needs to come out of the shadows and change culture of secrecy, warns spy chief” *The Telegraph* (30 November 2021) <https://www.telegraph.co.uk/news/2021/11/30/mi6-needs-come-shadows-change-culture-secrecy-warns-spy-chief/> (accessed 30/11/21)

Nix, Naomi. “Amazon is Flooding D.C. with Money and Muscle: The Influence Game” *Bloomberg* (7 March 2019) <https://www.bloomberg.com/graphics/2019-amazon-lobbying/> (accessed 18/01/22)

Norris, William J., *Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control*. Ithaca, NY, 2016

Nossel, Suzanne. “Google is Handing the Future of the Internet to China” *Foreign Policy* (10 September 2018) <https://foreignpolicy.com/2018/09/10/google-is-handing-the-future-of-the-internet-to-china/> (accessed 20/12/21)

Novet, Jordan. “Pentagon asks Amazon, Google, Microsoft and Oracle for bids on new cloud contract” *CNBC* (19 November 2021) <https://www.cnbc.com/2021/11/19/pentagon-asks-amazon-google-microsoft-oracle-for-cloud-bids.html> (accessed 20/11/21)

Nyman, Jonna. "‘Red Storm Ahead’: Securitisation of Energy in US–China Relations." *Millennium* 43, no. 1 (2014): 43-65.

O’Neil, Andrew. "Australia and the ‘Five Eyes’ intelligence network: the perils of an

asymmetric alliance." *Australian Journal of International Affairs* 71, no. 5 (2017): 529-543.

Office of Public Affairs, "Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with US Technologies" *US Department of Commerce* (15 May 2020) <https://www.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts> (accessed 15/05/20)

Ongweso Jr., Edward. "Big Tech Has Made Billions Off the 20-Year War on Terror" *Vice* (9 September 2021) <https://www.vice.com/en/article/4aveeq/big-tech-has-made-billions-off-the-20-year-war-on-terror> (accessed 18/01/22)

Organisation for Economic Cooperation and Development (OECD), "Protection of critical infrastructure and the role of investment policies relating to national security." *Paris: Organisation for Economic Co-operation and Development*, 2008.

Oswald, Franz. "Soft balancing between friends: transforming transatlantic relations." *Debatte: journal of contemporary central and Eastern Europe* 14, no. 2 (2006): 145-160

Ovide, Shira. "Why Washington Hates Big Tech" *The New York Times* (23 October 2020) <https://www.nytimes.com/2020/10/23/technology/why-washington-hates-big-tech.html> (accessed 19/12/21)

Owens, Jay. "The tech giants dominated the decade. But there's still time to rein them in." *The Guardian* (25 December 2019) <https://www.theguardian.com/commentisfree/2019/dec/25/2010s-tech-giants-google-amazon-facebook-regulators> (accessed 05/02/22)

Pape, Robert A. "Soft balancing against the United States." *International security* 30, no. 1 (2005): 7-45

Parliamentary Proceeding, "5G Network and Huawei" *House of Commons* 670 cc533-536 (27 January 2020) <https://hansard.parliament.uk/Commons/2020-01-27/debates/038EF380-E4D6-4A6D-A0D8-0FAEB1D0A9B0/5GNetworkAndHuawei> (accessed 28/10/20)

Parliamentary Proceeding, "Huawei and 5G", *House of Commons* 672 cc273-805WH (4 March 2020) <https://hansard.parliament.uk/Commons/2020-03-04/debates/9023564F-30E1-40C4-A9DE-E19DB8139E02/HuaweiAnd5G> (accessed 28/10/20)

Parliamentary Proceeding, "Telecoms Supply Chain" *House of Commons* Volume 663 (22 July 2019) <https://hansard.parliament.uk/Commons/2019-07-22/debates/7C7CE899-13EB-4C18-8678-44CB6CAA14F5/TelecomsSupplyChainReview?highlight=huawei%20american#contribution-4F9DB400-A3C6-4054-BA08-A1F588B19A9F> (accessed 28/10/20)

Parliamentary Proceeding, "UK Telecommunications" *House of Commons,* Volume 678 (14

July 2020) <https://hansard.parliament.uk/Commons/2020-07-14/debates/9467A1F1-B87B-4E16-AD0C-DFF02A51981A/UKTelecommunications?highlight=huawei%20american%20united%20states#contribution-8548AC01-3C2B-454A-86EC-9BF841EFDB57> (accessed 28/10/20)

Paul, Thazha V. "Soft balancing in the age of US primacy." *International security* 30, no. 1 (2005): 46-71

Payne, Andrew. *War on the Ballot: How the Election Cycle Shapes Presidential Decision-Making in War*. Columbia University Press, 2023.

Peniston, Bradley, 'How Will the Pentagon Create its AIs? The Algorithmic-Warfare Team is Charting a Path' (13 July 2017) <https://www.defenseone.com/technology/2017/07/artificial-intelligence-pentagon/139402/> (accessed 15/11/21)

Perlroth, Nicole. *This is how they tell me the world ends: The cyberweapons arms race*. Bloomsbury Publishing USA, 2021

Perrigio, Billy. "Bowing to US Pressure, UK Bans 5G Equipment from China's Huawei over Security Concerns" *Time* (14 July 2020) <https://time.com/5866643/uk-huawei-5g-ban/> (accessed 15/07/20)

Petry, Johannes. "Beyond ports, roads and railways: Chinese economic statecraft, the Belt and Road Initiative and the politics of financial infrastructures." *European Journal of International Relations* 29, no. 2 (2023): 319-351

Polatin-Reuben, Dana, and Joss Wright. "An Internet with {BRICS} Characteristics: Data Sovereignty and the Balkanisation of the Internet." In *4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14)*. 2014

Poulson, Jack. "Reports of a Silicon Valley/Military Divide Have Been Greatly Exaggerated" *Tech Inquiry* (July 7, 2020) <https://techinquiry.org/SiliconValley-Military/> (accessed 26/11/21)

Propp, Kenneth. "European Cybersecurity Regulation Takes a Sovereign Turn" *European Law Blog* (12 September 2022) <https://europeanlawblog.eu/2022/09/12/european-cybersecurity-regulation-takes-a-sovereign-turn/> (accessed 11/04/23)

Raab, Dominic. "Oral Statement to Parliament: Foreign Secretary's Statement on Huawei" *GOV.UK.* (28 January 2020) <https://www.gov.uk/government/speeches/foreign-secretary-statement-on-huawei> (accessed 12/02/20)

Reilly, James. *Orchestration: China's Economic Statecraft Across Asia and Europe*. Oxford University Press, 2021

Reuters. "Google employees push to stop Project Dragonfly" *Reuters* (27 November 2018) <https://www.reuters.com/article/google-workers-idINL4N1Y23E8> (accessed 04/02/22)

Reuters. “Microsoft’s Bing suspends auto suggest function in China at government’s behest” (17 December 2021) <https://www.reuters.com/technology/microsoft-bing-says-suspended-auto-suggest-function-china-government-behest-2021-12-17/> (accessed 21/12/21)

Reuters. “Tim Cook reportedly signed five-year $275bn deal with Chinese officials” *The Guardian* (7 December 2021) <https://www.theguardian.com/technology/2021/dec/07/apple-china-deal-tim-cook> (accessed 18/01/22)

Reuters. “UK in 5G talks with suppliers from Japan, South Korea: source” *Reuters* (3 June 2020) <https://www.reuters.com/article/us-britain-huawei-tech/uk-in-5g-talks-with-suppliers-from-japan-south-korea-source-idUSKBN23A3CY> (accessed 03/06/20)

Rifkind MP, Sir Malcom. "Foreign Involvement in the Critical National Infrastructure” Cm (Series) (Great Britain. Parliament); 8629 2013-14. Norwich (2013).

Riley-Smith, Ben. “US spy planes could be pulled from Britain as White House conducts major Huawei review” *The Telegraph* (4 May 2020) <https://www.telegraph.co.uk/news/2020/05/04/us-spy-planes-could-pulled-britain-white-house-conducts-major/> (05/05/20)

Roberts, Priscilla. "Economic statecraft with Chinese characteristics: Strange, new, and different, or old wine in new bottles?." *Journal of Current Chinese Affairs* 50, no. 3 (2021): 267-293.

Rotenberg, Marc. "Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection." *European Law Journal* 26, no. 1-2 (2020): 141-152.

Rühlig, Tim and Maja Björk. "What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe." *The Swedish Institute of International Affairs* (2020)

Sabbagh, Dan and Mark Sweney. “BT and Vodafone to lobby PM to allow use of Huawei equipment” *The Guardian* (17 January 2020) <https://www.theguardian.com/technology/2020/jan/17/uk-officials-frustrated-us-huawei-plan-b> (accessed 17/01/20)

Sandle, Paul and Guy Faulconbridge. “Britain set to ban Huawei from 5G, though timescale unclear” *Reuters* 13 July 2020.<https://www.reuters.com/article/us-britain-huawei/britain-set-to-ban-huawei-from-5g-though-timescale-unclear-idUSKCN24E0K3> (accessed 15/07/20)

Sanger, David and David McCabe. “Huawei Is Winning the Argument in Europe, as the US Fumbles to Develop Alternatives” *The New York Times* (17 February 2020) <https://www.nytimes.com/2020/02/17/us/politics/us-huawei-5g.html?searchResultPosition=1> (accessed 29/03/20)

Satariano, Adam, Stephen Castle and David E. Sanger. “UK Bars Huawei for 5G as Tech

Battle Between China and the West Escalates" *The New York Times* (14 July 2020) <https://www.nytimes.com/2020/07/14/business/huawei-uk-5g.html> (accessed 18/07/20)

Satariano, Adam. "Britain Defies Trump Plea to Ban Huawei from 5G Network" *The New York Times* (28 January 2020) <https://www.nytimes.com/2020/01/28/technology/britain-huawei-5G.html?searchResultPosition=8> (accessed 09/02/20)

Schott, Ben, "Give Amazon and Facebook a Seat at the United Nations" *Bloomberg* (3 October 2021) <https://www.bloomberg.com/opinion/articles/2021-10-03/give-amazon-and-facebook-a-seat-at-the-united-nations> (accessed 28/09/22)

Schwab, Klaus, and Nicholas Davis. *Shaping the future of the fourth industrial revolution*. Currency, 2018

Seawright, Jason, and John Gerring. "Case selection techniques in case study research: A menu of qualitative and quantitative options." *Political research quarterly* 61, no. 2 (2008): 294-308.

Shadmy, Tomer. "The Emergence of Responsibility as a Global Scheme of Governance" in Hannes Hansen-Magnusson and Antje Vetterlein, *The Routledge Handbook on Responsibility in International Relations.* New York, NY: Routledge, 2022.

Shane, Scott, and Saisuke Wakabayashi. "The Business of War: Google Employees Protest Work for the Pentagon" *The New York Times* (4 April 2018) <https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html> (accessed 03/01/22)

Sheehan, Matt. "How Google took on China – and lost" *MIT Technology Review* (19 December 2018) <https://www.technologyreview.com/2018/12/19/138307/how-google-took-on-china-and-lost/> (accessed 20/12/21)

Shepherd, Christian. "US blacklists Chinese nuclear company over theft of military tech" *Financial Times* (15 August 2019) <https://www.ft.com/content/9601ebda-bf24-11e9-b350-db00d509634e> (accessed 26/08/20)

Silver, Laura, and Aidan Connaughton, "Most Americans continue to think the US is less respected today than in the past," *Pew Research Centre* (22 June 2022) <https://www.pewresearch.org/short-reads/2022/06/22/most-americans-continue-to-think-the-u-s-is-less-respected-today-than-in-the-past/> (accessed 02/10/23)

Sitaraman, Ganesh. "Too big to prevail: The national security case for breaking up big tech." *Foreign Aff.* 99 (2020): 116.

Skolnikoff, Eugene B. *Science, technology, and American foreign policy*. MIT Press, 1967.

Skolnikoff, Eugene B. *The Elusive Transformation: Science, Technology, and the Evolution of International Politics*. Core Textbook. Princeton, NJ: Princeton University Press, 1994.

Sky News. “Huawei U-turn: Cyber attacks, levies and other possible repercussions of the UK’s 5G move” *Sky News* (15 July 2020) <https://news.sky.com/story/huawei-u-turn-cyber-attacks-levies-and-other-possible-implications-of-the-uks-5g-move-12028238> (accessed 16/07/20)

Smeets, Max. "US cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection." *Intelligence and National Security* 35, no. 3 (2020): 444-453.

Smith, Allan. “Impressive and a little scary: How Amazon and Jeff Bezos made Washington a second home” *NBC News* (6 September 2019) <https://www.nbcnews.com/politics/politics-news/king-hill-how-amazon-jeff-bezos-made-washington-second-home-n1033296> (accessed 18/01/22)

Smith, Nicholas Ross. "When hedging goes wrong: Lessons from Ukraine’s failed hedge of the EU and Russia." *Global policy* 11, no. 5 (2020): 588-597.

Smith, Karen E. "Missing in analysis: Women in foreign policy–making." *Foreign Policy Analysis* 16, no. 1 (2020): 130-141.

Snidal, Duncan. “Rational Choice in International Relations”, in Walter Carlsnaes, Thomas Risse and Beth A. Simmons, eds. *Handbook of International Relations,* 2nd ed. London: Sage, 2013, pp.85-111.

Solon, Olivia, and Sabrina Siddiqui. “Forget Wall Street – Silicon Valley is the new political power in Washington” *The Guardian* (3 September 2017) <https://www.theguardian.com/technology/2017/sep/03/silicon-valley-politics-lobbying-washington> (accessed 27/11/21)

Stevens, Betsy. "Corporate ethical codes: Effective instruments for influencing behavior." *Journal of Business ethics* 78 (2008): 601-609.

Stevens, Tim. “Huawei and UK foreign policy” *UK in a Changing Europe* (21 July 2020) <https://ukandeu.ac.uk/huawei-and-uk-foreign-policy/> (accessed 01/09/20)

Stevens, Tim. *Cyber Security and the Politics of Time*. Cambridge: Cambridge University Press, 2016.

Stewart, Heather and Dan Sabbagh. “UK Huawei decision appears to avert row with US” *The Guardian* (28 January 2020) <https://www.theguardian.com/technology/2020/jan/28/boris-johnson-gives-green-light-for-huawei-5g-infrastructure-role> (accessed 17/02/20)

Stokes, Bruce. “The Decline of the City Upon a Hill: As American Democracy Loses its Shine, American Power Suffers” *Foreign Affairs* (17 October 2022) <https://www.foreignaffairs.com/united-states/decline-city-upon-hill> (accessed 02/10/23)

Strand, John. “Ban Huawei? Not Europe” *Center for European Policy Analysis (CEPA)* (12 January 2023) <https://cepa.org/article/ban-huawei-not-europe/> (accessed 11/04/23)

Subin, Samantha. “Palantir CEO says companies working with US adversaries should justify their position” *CNBC News* (23 November 2021) <https://www.cnbc.com/2021/11/23/palantir-ceo-companies-working-with-us-adversaries-should-justify-their-position-.html> (accessed 02/12/21)

Sun, Haiyong. "US-China tech war: Impacts and prospects." *China Quarterly of International Strategic Studies* 5, no. 02 (2019): 197-212.

Tanaka, Akito. “US and China need to repair tech ties: Microsoft president” *Nikkei Asia* (9 September 2021) <https://asia.nikkei.com/Business/Technology/US-and-China-need-to-repair-tech-ties-Microsoft-president> (accessed 21/12/21)

Tennis, Maggie. “Madeleine Albright on fascism, democracy and diplomacy.” *Brookings Institute* (11 September 2018) <https://www.brookings.edu/articles/madeleine-albright-on-fascism-democracy-and-diplomacy/> (accessed 11/10/23)

The Economist, “China has become a laboratory for the regulation of digital technology” (11 September 2021) <https://www.economist.com/china/2021/09/11/china-has-become-a-laboratory-for-the-regulation-of-digital-technology> (accessed 03/01/22)

The Economist, “Democracies must team up to take on China in the technosphere” (19 November 2020) <https://www.economist.com/briefing/2020/11/19/democracies-must-team-up-to-take-on-china-in-the-technosphere> (accessed 30/10/21)

The White House. “National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems,” (4 May 2022) <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/> (accessed 09/10/23)

Tidy, Joe. “Huawei: How the UK’s decision affects the rest of the world” *BBC News* (28 January 2020) <https://www.bbc.co.uk/news/technology-51284393> (accessed 15/02/20)

Tiku, Nitasha. “Google’s CEO Says Tests of Censored Chinese Search Engine Turned Out Great” *Wired* (15 October 2018) <https://www.wired.com/story/wired-25-sundar-pichai-china-censored-search-engine/> (accessed 06/02/22)

Tilley, Aaron. “Microsoft CEO Nadella Wades Into US-China Tensions in TikTok Pursuit” *Wall Street Journal* (4 August 2020) <https://www.wsj.com/articles/microsoft-ceo-nadella-wades-into-u-s-china-tensions-in-tiktok-pursuit-11596569063> (accessed 03/01/22)

Townes-Whitley, Toni. “Microsoft’s commitment to the DoD remains steadfast” *Official Microsoft Blog* (6 July 2021) <https://blogs.microsoft.com/blog/2021/07/06/microsofts-commitment-to-the-dod-remains-steadfast/> (accessed 01/01/22)

Treverton, Gregory F., and Pari Esfandiari, "Viewing tech giants as a geopolitical force" *The Hill* (31 January 2020) <https://thehill.com/opinion/technology/480823-viewing-tech-giants-as-a-geopolitical-force> (accessed 01/12/21)

Urdinez, Francisco, Fernando Mouron, Luis L. Schenoni, and Amâncio J. de Oliveira. "Chinese economic statecraft and US hegemony in Latin America: an empirical analysis, 2003–2014." *Latin American Politics and Society* 58, no. 4 (2016): 3-30.

Vallejo, Justin. "White House could pull US military and intelligence operations out of UK as part of Huawei review, reports say" *The Independent* (5 May 2020) <https://www.independent.co.uk/news/world/americas/huawei-review-white-house-uk-trump-boris-johnson-5g-network-a9498821.html> (accessed 05/06/20)

Vogels, Emily A. "56% of Americans support more regulation of major technology companies" *Pew Research Centre* (20 July 2021) <https://www.pewresearch.org/fact-tank/2021/07/20/56-of-americans-support-more-regulation-of-major-technology-companies/> (accessed 26/12/21)

Wade, Robert H., "The Paradox of US Industrial Policy: The Developmental State in Disguise." In *Transforming Economies*, edited by Nübler, Irmgard, José Manuel Salazar-Xirinachs, and Richard Kozul-Wright. Switzerland: International Labour Organisation (ILO), 2014. Print

Wakabayashi, Daisuke and Kate Conger. "Google Wants to Work with the Pentagon Again, Despite Employee Concerns" *The New York Times* (3 November 2021) <https://www.nytimes.com/2021/11/03/technology/google-pentagon-artificial-intelligence.html> (accessed 04/01/22)

Walt, Stephen M. "Big Tech Won't Remake the Global World Order" *Foreign Policy* (8 November 2021) <https://foreignpolicy.com/2021/11/08/big-tech-wont-remake-the-global-order/> (accessed 27/12/21)

Ward, Andrew, and Jim Pickard, "Hinkley go-ahead after 'national security' safeguards" *Financial Times* (15 September 2016) <https://www.ft.com/content/0cde26b6-7b66-11e6-b837-eb4b4333ee43> (accessed 21/01/20)

Warrell, Helen, and George Parker. "US attacks UK's decision on Huawei" *Financial Times* (28 January 2020) <https://www.ft.com/content/e3d38d0e-41c5-11ea-a047-eae9bd51ceba> (accessed 01/02/20)

Warrell, Helen, and Nic Fildes. "UK review of Huawei eyes impact of US sanctions" *Financial Times* (1 June 2020) <https://www.ft.com/content/9e581ace-69ec-4a42-81c3-c28d2bb40aa1> (accessed 01/06/20)

Warrell, Helen, Sebastian Payne and Nic Fildes. "UK ministers seek to placate Tory rebels over Huawei deal" *Financial Times* (13 March 2020) <https://www.ft.com/content/c8144666-6516-11ea-b3f3-fe4680ea68b5> (accessed 02/11/20)

Waters, Richard. "Jeff Bezos warns US military it risks losing tech supremacy" *Financial Times* <https://www.ft.com/content/b38c5cf6-198a-11ea-97df-cc63de1d73f4>

(accessed 08/02/22)

Weinberger, Sharon, “Meet America’s newest military giant: Amazon” *MIT Technology Review* (8 October 2019) <https://www.technologyreview.com/2019/10/08/75349/meet-americas-newest-military-giant-amazon/> (accessed 18/01/22)

Weise, Karen, and Paul Mozur, “LinkedIn to Shut Down Service in China, Citing ‘Challenging’ Environment” *The New York Times* (14 October 2021) <https://www.nytimes.com/2021/10/14/technology/linkedin-china-microsoft.html> (accessed 21/12/21)

Weiss, Charles. “How Do Science and Technology Affect International Affairs.” *Minerva (London)* 53, no. 4 (2015): 411–430.

Weiss, Linda. "Re-emergence of Great Power Conflict and US Economic Statecraft." *World Trade Review* 20.2 (2021): 152-68.

Weiss, Linda, and Elizabeth Thurbon. "Developmental state or economic statecraft? Where, why and how the difference matters." *New Political Economy* 26, no. 3 (2021): 472-489.

Wertime, David, and Protocol China Staff, “US Tech Wants to Work More With China” *Protocol* (17 March 2021) <https://www.protocol.com/newsletters/protocol-china/tech-workers-on-china?rebelltitem=2#rebelltitem2> (accessed 03/01/22)

Williams, Greg. “Big Tech is now a geopolitical force – and that should worry us all” *Wired* (9 April 2020) <https://www.wired.co.uk/article/big-tech-geopolitics> (accessed 01/12/21)

Wintle, Thomas. “Huawei ban from UK’s 5G network risks $23.6bn economic hit – report” *CGTN* (10 September 2020) <https://newseu.cgtn.com/news/2020-09-09/Huawei-ban-from-UK-s-5G-network-risks-23-6bn-economic-hit-report—TE41jbvIoE/index.html> (accessed 17/11/20)

Wu, Emily. “Sovereignty and Data Localisation” *Harvard Kennedy School Belfer Center for Science and International Affairs* (July 2021) <https://www.belfercenter.org/sites/default/files/2021-07/SovereigntyLocalization.pdf> (accessed 27/04/22)

Xu, Ruike. *Alliance persistence within the Anglo-American special relationship: The post-Cold War era*. Springer, 2017.

Xuetong, Yan. "Bipolar rivalry in the early digital age." *The Chinese Journal of International Politics* 13, no. 3 (2020): 313-341

Yadron, Danny, Spencer Ackerman and Sam Thielman. “Inside the FBI’s encryption battle with Apple” *The Guardian* (18 February 2016) <https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple> (accessed 18/01/22)

Yang, Lin. “How Facebook’s Zuckerberg Went from Courting to Criticising Beijing” *VOA News* (5 September 2020) <https://www.voanews.com/a/silicon-valley-technology_how-facebooks-zuckerberg-went-courting-criticizing-beijing/6195455.html> (accessed 21/12/21)

Yeo, ShinJoung. "Geopolitics of search: Google versus China?." *Media, Culture & Society* 38, no. 4 (2016): 591-605