Alma Mater Studiorum - Università di Bologna

DOTTORATO DI RICERCA IN

SCIENZE POLITICHE E SOCIALI

Ciclo 34

Settore Concorsuale: 14/A2 - SCIENZA POLITICA

Settore Scientifico Disciplinare: SPS/04 - SCIENZA POLITICA

RISING CHINA AND INTERNET GOVERNANCE: MULTISTAKEHOLDERISM, FRAGMENTATION AND THE LIBERAL ORDER IN THE AGE OF DIGITAL SOVEREIGNTY

Presentata da: Riccardo Nanni

Coordinatore Dottorato

Daniela Giannetti

Supervisore

Sonia Lucarelli

Co-supervisore

Matteo Dian

Esame finale anno 2022

TABLE OF CONTENTS

To my family

ACKNOWLEDGEMENTS

The author thanks Sonia Lucarelli and Matteo Dian for their role as supervisors, George Christou for his mentorship, Daniela Giannetti for her role as programme coordinator, and the two referees, Jamal Shahin and Joe Burton, for their valuable comments. A special thanks goes to the creators and developers of Bigbang, Niels Ten Oever, Christoph Becker, Nick Doty, and Sebastian Benthall, for their help in conducting network analysis. The author also wishes to thank the twenty-nine interview participants, without whom this research would have not been possible.

Furthermore, the author thanks Mauro Santaniello, Claudia Padovani, Farzaneh Badii, Milton Mueller, Bhawna Pokharna, Sung Chull Kim, Andrea Ghiselli, Simone Dossi, Tatiana Tropina, Ashwin Mathew, Elisa Oreglia, Shaun Breslin, Francesco Niccolò Moro, Giampiero Giacomello, Andrea Calderaro, Lorenzo Zambernardi, and Antonio Fiori for their comments on this project at conferences and in other settings.

Finally, a special mention goes to Max Warrack and Mariska Versantvoort for coordinating the East Asia Study Group (EASG) and the Group Critique, respectively. Through these initiatives at the Politics and International Studies (PAIS) department of the University of Warwick this research project received important comments and major improvements.

ABSTRACT

In its open and private-based dimension, the Internet is the epitome of the Liberal International Order in its global spatial dimension. Therefore, normative questions arise from the emergence of powerful non-liberal actors such as China in Internet governance. In particular, China has supported a UN-based multilateral Internet governance model based on state sovereignty aimed at replacing the existing ICANN-based multistakeholder model. While persistent, this debate has become less dualistic through time. However, fear of Internet fragmentation has increased as the US-China technological competition grew harsher.

This thesis inquires "(To what extent) are Chinese stakeholders reshaping the rules of Global Internet Governance?". This is further unpacked in three smaller questions: (i) (To what extent) are Chinese stakeholders contributing to increased state influence in multistakeholder fora?; (ii) (how) is China contributing to Internet fragmentation?; and (iii) what are the main drivers of Chinese stakeholders' stances?

To answer these questions, Chinese stakeholders' actions are observed in the making and management of critical Internet resources at the IETF and ICANN respectively, and in mobile connectivity standard-making at 3GPP. Through the lens of norm entrepreneurship in regime complexes, this thesis interprets changes and persistence in the Internet governance normative order and Chinese attitudes towards it. Three research methods are employed: network analysis, semi-structured expert interviews, and thematic document analysis.

While China has enhanced state intervention in several technological fields, fostering debates on digital sovereignty, this research finds that the Chinese government does not exert full control on its domestic private actors and

concludes that Chinese stakeholders have increasingly adapted to multistakeholder Internet governance as they grew influential within it. To enhance control over Internet-based activities, the Chinese government resorted to regulatory and technical control domestically rather than establishing a *splinternet*. This is due to Chinese stakeholders' interest in retaining the network benefits of global interconnectivity.

Keywords: China; Liberal International Order; Internet governance; Regime Complexity; Digital Sovereignty.

INTRODUCTION

Will China fragment the Internet? Is China bringing authoritarian influence in the (multistakeholder) governance of the Internet's resources? Is China rewriting the protocols (and rules) of the global Internet?

These questions are widespread in the media and policy environment (see for example: Murgia, Gross 2020). The US-China trade competition that burst under the Trump administration invested technological development and led to new and increasing protectionist measures (Ciuriak 2019; Poggetti 2021), firing up the media and policy debates around China's role in Internet governance. However, sectors of academia and the technical communities invite more nuanced views (Mueller 2017; Negro 2020; Sharp, Kolkman 2020).

After all, critical views have been emerging in the literature throughout the last two decades warning against oversimplified views of the Internet and its politics (Morozov 2011). Liberational expectations on cyberspace have been followed by disillusion over the failure of online platforms to serve as a safe space for progressive civil society organisations, such as during the Arab Springs. In their aftermath, the PRISM scandal revealed a massive surveillance programme in a liberal democracy such as the US, while new scandals connecting social media with surveillance in totalitarian states and unethical meddling in democratic elections (such as the Cambridge Analytica case) raised calls for platform regulation and increased control on online activities by the public authority (Radu 2019).

Beyond the level of platforms and their public role, the literature has been systematically observing a turn to infrastructure in Internet governance, whereby technical matters related to the backbone of the Internet, including its addressing system as well as the physical infrastructure, have become politicised and have been used for political ends by state actors (DeNardis,

Musiani 2016; Musiani 2013). In this context, China has often been portrayed as a state actor ready to detach from the global Internet by establishing a national *splinternet* while promoting a more state-centric Internet governance model internationally (Murgia, Gross 2020; Segal 2016; 2018).

This thesis observes the interaction of Chinese public and private actors in selected core aspects of Internet governance to interpret the normative impact and drivers of their actions. Through this analysis, this thesis explores whether, how, and why Chinese stakeholders contest or adapt to existing norms in Internet governance, including the Internet's core protocols allowing global interconnectivity.

Open questions in Internet governance

Observing the rise of China in the realm of Internet governance is of utmost importance as it strikes at the very heart of the Liberal International Order. As a US creation, the Internet's predecessor Arpanet is representative of Washington's Cold-war era technological leadership, which in turn is a tool for hegemony (Carr 2015). The establishment of multistakeholder governance mechanisms for the Internet in the 1990s under US guidance is epitomical of the US's hegemony in the so-called 'unipolar decade'. The prominent role recognised to private actors in the governance mechanisms of a technology that now connects several billion people all over the globe represents the global spread of the Liberal Order in its free-market tenet (Santaniello 2021; Scholte 2017).

Here, the Liberal International Order is defined as the order established after World War II under US leadership based on free market and international law, institutionally represented in such organisations as the World Trade Organisation (WTO) and the United Nations (UN) respectively. Normatively, the Liberal International Order is state-centric and sovereignty-based in the Westphalian tradition but allows and recognises actorness to non-state actors in

its free-market characterisation. Global governance, conceived as 'governance without government' (Rosenau 1992), features a transnational element that entails non-state actors across national lines interacting in policymaking. After all, the UN itself grants corporations and non-governmental organisations roles in several of its agencies' policy-making processes (Clapham 2022). While after World War II such order could be seen as mainly a 'club' of Western nations, inasmuch as the communist bloc did not participate in globalised free market, from the 1990s onwards the Liberal Order has reached global spatiality (Parsi 2018). This, of course, does not entail global acceptance of liberal normativity and the fadeaway of contestation à la Fukuyama (1989), but rather the solidification of a global order based on universalistic claims (such as the treaty-based institutionalisation of universal human rights) with a conflicting Westphalian element of state sovereignty and non-interference in domestic affairs. The Westphalian element allows for the inclusion of countries featuring a non-liberal domestic polity within the institutions of the Liberal International Order (Ikenberry 2018).

When it comes to Internet governance, its multistakeholder characterisation is epitomical of the Liberal International Order in its free-market tenet. Conversely, Internet governance models based on state sovereignty have historically been promoted by emerging and contesting authoritarian states (Flonk, Jachtenfuchs, Obendiek 2020). In this view, challenges to the normative order (Kettemann 2020) of the Internet from non-liberal actors in hegemonic competition with the US can be read within the broader debate on the future of the Liberal International Order. Within this debate, the rise of China has been discussed for two decades. From the mid-2010s onwards the geopolitical competition between the US and China has become strongly focused on technological leadership – leading to forms of protectionism and reciprocal sanctions (Ciuriak 2019), thus fostering debates on the return of the state in Internet governance and the rise of digital sovereignty (Creemers 2020a; Haggart, Tusikov, Scholte 2021).

Observing Chinese norm entrepreneurship in the regime complex for Internet governance through a variety of computational and qualitative

methods allows one to qualify and interpret the extent and impact of Chinese stakeholders' contestation to Internet governance norms. In this study, the author observes the processes of normative contestation, but also adaptation, to the existing norms, conducted by Chinese stakeholders within the Internet governance regime complex. While the regime complex entails hundreds of norm-making actors and venues (Radu 2019), this thesis looks at three key fora: the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), and the Third Generation Partnership Project (3GPP). As better illustrated in Chapter 1, these three bodies deal with key technical and eminently political aspects of Internet governance: the management of critical Internet resources, including unique identifiers such as IP addresses (ICANN); the creation of Internet standards, including the aforementioned critical resources (IETF); and the establishment of mobile connectivity standards such as the fifth-generation telephony technology (5G) (3GPP). These allow an observation of normative contestation at the core of the Internet infrastructure (DeNardis, Musiani 2016), while looking also at the development of a strongly politicised technology such as 5G, which may influence the functioning of the Internet's basic standards in the near future (Ten Oever 2021).

Coherently with the multistakeholder characteristics of the Internet governance regime complex, this thesis analyses not only the actions of China and Chinese governmental actors, but also those of Chinese non-state stakeholders. While the unknowns of governmental control on private actors are manifold when looking at China, this thesis makes no prior assumptions on the extent to which such control exists (Galloway 2015). Instead, it observes the behaviour of companies and other stakeholders within ICANN, IETF, and 3GPP and includes the views of several groups of stakeholders through interviews. In particular, this thesis incorporates opinions from the technical community, that is, those people involved in standard-making on a daily basis. Such experts possess technical knowledge otherwise inaccessible to social scientists, which provides them with a privileged view on political topics and allows them to reach qualitatively different conclusions on similar questions

compared to policy experts. Furthermore, their role in the making of such technology is of utmost political salience given the politicisation of the issue in question. Incorporating their views in this research provides basis for nuanced interpretations often missed in International Relations (IR) literature (Tanczer, Brass, Carr 2018).

Whether China is contributing to recentralising governance in the hands of states and to fragmenting the Internet is an open question in the literature. What will the "Internet of the future" look like if standard-making and resources distribution moves into the hands of state-centric agencies? (How) will seamless cross-border communication work across *splinternets*? Conversely, should Internet fragmentation not take place, and should authoritarian powers like China increasingly accept multistakeholderism and the existing Internet architecture, what will the existing liberal-informed Internet governance mechanisms look like in the near future?

This research has implications for all these matters. In turn, the debates addressed in the forthcoming chapters touch directly upon the debate on the rise of China in the Liberal International Order. While findings on Internet governance are not straightforwardly transferable to the whole of the order, this research suggests that there are facets of it that create incentives and conditions for actors to adapt to existing normative orders other than challenging them (Ikenberry 2018).

Thesis structure

Chapter 1 of this thesis unpacks the research question and locates it in the broader debates on the sovereigntist challenge to multistakeholder Internet governance and the question of Internet fragmentation. The chapter develops the claims illustrated above on the connection between the Internet, its governance mechanisms, and the global spatiality of the Liberal Order in its free-market tenet, positioning the 'multistakeholderism' and 'fragmentation'

debates in the broader context of the question of China's rise and the future of the Liberal International Order.

Chapter 2 illustrates the theoretical approaches and the research methods adopted in this research. Literature on regime complexity and norm entrepreneurship is addressed to conceptualise the global Internet governance ecosystem and to observe the actions and influence of Chinese stakeholders within it.

Chapter 3 begins the empirical part of this thesis with an exploratory computational analysis on ICANN, IETF, and 3GPP mailing list exchanges. In this chapter, one can observe the activeness of Chinese actors in shaping the outcome of these three bodies' policy- and standard-making.

Chapter 4 builds on Chapter 3 by providing a qualitative exploration of Chinese stakeholders' engagement and influence in the standardisation and distribution of critical Internet resources, with particular focus on the unique identifiers (IP address and domain names).

Chapter 5 also expands on the computational analysis of Chapter 3, this time to observe Chinese stakeholders' engagement and influence in 3GPP, that is, in the making of mobile connectivity standards from 3G to 5G.

Chapter 6 draws together the findings to reach general conclusions on the debates addressed in this research. It builds connections among the debates in question and discussing the transferability of findings in other fields of interest for the question of the future of the Liberal Order.

Finally, the conclusive chapter draws the final lines of this research and illustrates some of the open questions that remain unanswered in the field.

CHAPTER 1

SETTING THE SCENE: INTERNET GOVERNANCE AND CHINESE STAKEHOLDERS' ENGAGEMENT

1.1 *Introduction*

Multistakeholderism in Internet governance has been subjected to criticism and contestation since the establishment of ICANN in 1998. The liberal characterisation of the multistakeholder mechanisms of Internet governance emerges normatively in its openness to private stakeholders' participation and limited state role (Scholte 2017), coherently with the idea of transnationality in global governance surged to prominence in the 1990s (Rosenau 1992). The extent to which such openness is a rhetorical artifice hiding power dynamics has been debated through time (Cath 2021; Palladino, Santaniello 2021). As a matter of fact, the special role played by the US Department of Commerce (DoC) through its contractual position vis-à-vis ICANN has been one of the main points of contention until the contract's recission in 2016 (Mueller 2017). In that context, the ICANN-centred multistakeholder governance model was contested by emerging authoritarian powers, chiefly Russia and China, who sought to push forward a state-based model (Flonk, Jachtenfuchs, Obendiek 2020; Glen 2014). The sovereigntist stances in Internet governance contributed to a growing debate over the risk of Internet fragmentation (Hoffmann, Lazanski, Taylor 2020), with normative contestation remaining an ongoing subject (Negro 2020).

This chapter will dive deeper into such debates. In particular, this doctoral project aims to observe the influence of Chinese actors, that is, China's government and Chinese non-state Internet stakeholders, on the norms of Global Internet Governance. This addresses a topic of increasing policy importance amid growing tension and competition between the US and China

in the technology sector, while addressing the scholarly debates on Internet fragmentation and digital sovereignty, that is, the return of states in Internet governance (Haggart, Scholte, Tusikov 2021; Mueller 2017).

The macro-question this thesis addresses is "*(To what extent) are Chinese stakeholders reshaping the rules of Global Internet Governance?*". This is further unpacked in three smaller questions: (i) (To what extent) are Chinese stakeholders contributing to increased state influence in multistakeholder fora?; (ii) (how) is China contributing to Internet fragmentation?; and (iii) what are the main drivers of Chinese stakeholders' stances?

Through these questions, this research project contributes to two major debates in the global Internet governance literature: (i) multistakeholderism and the role of governments in global Internet governance (Palladino, Santaniello 2021); and (ii) alignment and fragmentation of the Internet (Mueller 2017).

The first debate concerns relations among stakeholder groups in global Internet governance and the future of the multistakeholder system; the second debate focuses instead on whether the global Internet is here to stay or will yield regional and national *splinternets* – that is, whether China is creating a separate national Internet, or controlling (aligning) online information flows domestically through regulations while participating in and shaping the rules of the global Internet (Mueller 2017). This has implications for the realm of Internet governance strictly conceived as the management of the Internet's critical resources (Raymond, DeNardis 2015; Mueller, Badiei 2020), but also for the realm of standard-making (Harcourt, Christou, Simpson 2020; Ten Oever 2020). Together, these two debates feed into the emerging literature on digital sovereignty, with the return of state in Internet governance and the establishment of state-led control on the Internet architecture as two main features (Haggart, Scholte, Tusikov 2021).

While these debates are often framed dichotomously, this research rejects the most dualistic views and tries to elaborate a nuanced interpretation of Chinese actors' role in Internet governance, acknowledging ambiguities in normative acceptance and contestation. As observed throughout the chapter,

contestation of the Liberal International Order comes not only from emerging state powers and their national actors, but also from inside the 'core' of the Liberal Order itself (Deudney, Ikenberry 2018). In the same way, criticism of multistakeholderism and private-based governance does not come purely from emerging non-liberal powers, but also from Western allies and Western scholars (Belli 2015; Cath 2021; Santaniello 2021). Nonetheless, while acknowledging this criticism, this thesis' focus will be on contestation from emerging actors, that is, China's state- and non-state stakeholders.

Through this analysis, this project contributes to the broader debate on China's rise and its challenge to the Liberal International Order. In particular, it looks at Internet governance as a peculiar, largely private-based governance mechanism, whereby a number of public and private stakeholders enjoy actorness in policymaking in a myriad of loosely coupled regime settings, thus blurring the lines of what is often identified as 'national strategy' (Nye 2014).

In this context, this research finds that Chinese stakeholders have engaged in a process of contestation as well as adaptation to the norms and rules of multistakeholder global Internet governance. While refraining from a technical fragmentation of the Internet for the sake of (economic) network benefits, the Chinese government has resorted to practices of alignment of the Internet to domestic regulation in order to control online activities domestically (Mueller 2017). On a broader theoretical level, the study illustrated in the forthcoming chapters is exemplary of how regime complexes create venues for policy influence for a variety of public and private actors as norm entrepreneurs (Radu et al. 2021), but also yield normative rigidity that makes such regimes resilient to reform (Leal-Arcas, Morelli 2018). Such regime resilience pushes contestants to accept the regime's norms.

Interpreting the way in which Chinese actors beyond the government, as well as the Chinese government itself, act in the governance of such an omnipresent tool as the Internet, enabler of most twenty-first century technological innovations, can provide new nuance to the debate on China's rise and the future of the Liberal International Order. Furthermore, the unknowns on the relationship between Chinese non-state stakeholders and the

Chinese government present a *sui generis* challenge to multistakeholderism and the broader Liberal International Order (Pupillo 2019). If China's government were in full control of its domestic private actors, the former would be able to increase state-centricity in multistakeholder governance by leveraging the latter without renegotiating the formal norms and processes of the existing governance mechanism.

Encompassing views from a heterogeneous group of Internet stakeholders, this research contributes to the existing literature by incorporating technologists' views and experiences in the analysis. True, technologists participate in technological innovation processes on behalf of the company or entity they work for, creating a potential bias in their views. Nonetheless, their work and its outcome are most often unintelligible to lay observers. This means that the macro-level analyses conducted by International Relations (IR) scholars on techno-political matters may often miss or misinterpret the political aspects that emerge and concretise in everyday technological development processes (for example, standardisation activities), unless technologists' views are incorporated in the analysis. Building on decades of Science and Technology Studies (STS) literature (Levinson, Cogburn 2016; Musiani 2020), Tanczer, Brass and Carr (2018) illustrate in their analysis on scientific diplomacy that scientists' views are structurally underrepresented in literature despite their role in shaping the final policy. As technical experts possess privileged access to matters that fall outside the scope and expertise of policy scholars, failing to include their views in research on technopolitical questions can yield misinterpretations. For example, fears in the media of China drifting Internet standards and the Internet architecture through the so-called 'New IP' (Murgia, Gross 2020) have been smoothed by the technical community based on technological path dependences that exist in standard-making activities (Internet Governance Project 2020; Sharp, Kolkman 2020). This aspect will be better observed later in this thesis.

Since the field of global Internet governance is a broad one whose borders are blurred (Mueller, Badiei 2020), this research adopts Raymond and DeNardis' (2015, 3) definition that identifies six subsets of Internet governance:

"(i) control of 'critical Internet resources,' (ii) setting Internet standards, (iii) access and interconnection coordination, (iv) cybersecurity governance, (v) the policy role of information intermediaries, and (vi) architecture-based intellectual property rights enforcement."

In this view, this thesis will focus on the two subtopics of critical Internet resources (CIRs) governance and mobile Internet technology (from 3G to 5G) standardisation processes. Through the former, one can observe Chinese stakeholders' interactions at the core of Internet governance, that is, the making of the Internet infrastructure and the management of its unique identifiers, such as the Internet Protocol (IP) Addresses and the Domain Name System (DNS). Through the latter, one can address Chinese stakeholders' behaviour on a topic of utmost centrality in the US-China trade competition (Ciuriak 2019), other than one that may affect the future development of Internet infrastructure by creating increasing technological dependence on fully determined network as illustrated later in this thesis (Ten Oever 2020). In this way, this thesis addresses Chinese influence on deeply politicised facets of Internet governance carrying strong weight for International Relations.

While seemingly a purely technical matter, CIRs are eminently political: online censors target IP addresses and Domain Names to individuate and clamp down on unwanted contents and political activities. Therefore, if (or when?) governments carry influence in the establishment of the Internet's basic protocols, strong political implications may follow (Segal 2016). WikiLeaks was a case in point: when the website was shut down, it became inaccessible in many countries by typing its domain name in the Uniform Resource Locator (URL) bar or through a common browser search. However, by typing its IP address into the URL bar, the website would open (Deibert 2009). CIRs also have important implications for Intellectual Property Rights (IPRs) (World Intellectual Property Organization 2020, hereafter WIPO). These can trigger broader political disputes involving public and private actors. This applies to the establishment and distribution of domain names, including country-code Top-Level Domains (ccTLDs, such as '.it'), generic Top-Level Domains (gTLDs, such as '.com'), and brand domains that resemble geographical

indicators (such as '.amazon'). For example, attempts by the e-commerce giant Amazon.com to establish a '.amazon' Brand TLD triggered reactions from the Brazilian and Peruvian governments, raising a dispute within ICANN (ICANN 2017). In other words, CIRs are analysed in this research project given their political and economic salience.

As for mobile Internet technology standards, they represent a cross-cutting issue over the six subsets identified by Raymond and DeNardis (2015). First, each generation of mobile Internet standards aims to strengthen and widen access and interconnection. Matters of specifications compatibility affect mobile interoperability. Furthermore, issues of cybersecurity governance centred on 5G infrastructures, whether warranted or not, have been raised in the context of the US-China technological competition (Ciuriak 2019; The Economist 2020). Stances taken by different private and governmental actors in this field and their transformation through time are indicators of geopolitical and market repositioning. Key technologies affecting major global markets such as digital and mobile devices have historically been considered tools of US hegemony in the free market-based Liberal Order (Kania, Costello 2018). Finally, architecture-based intellectual property rights enforcement is always an issue at stake when it comes to standardising Internet-based technology in any form (IPLytics 2020; Kim, Lee, Kwak 2020). To this, it must be added that 5G can enable IoT devices aimed at many sensitive and strategic sectors, including medicine and the military among others (D. Wang et al. 2018). The interests of the companies competing in mobile Internet standardisation processes, as well as those of their domestic countries and economies, influence the outcome of standardisation processes and the existence of one universal standard and/or several local specifications. While mobile Internet technologies do not constitute Internet standards[1], the behaviour of the actors involved in standard-

[1] Internet Standards are voluntary protocols and specifications allowing networks interconnections, that is, the functioning of the Internet. They are elaborated at the IETF (2021b). Mobile Internet connectivity is a set of technologies allowing data to be

making hints at whether there is interest in keeping the Internet universal or fragmentation is bound to take place (Mueller 2017; Tilli, Kantola 2017).

To part of the literature, only CIRs governance constitutes fully-fledged Internet governance in its strictest sense (Mueller, Badiei 2020). Mobile Internet constitutes instead a key connectivity technology that gained geopolitical centrality amid the US-China trade war. Nonetheless, mobile Internet technologies are putting strain on the functioning of the basic Internet architecture, and with mobile connectivity switching to all-IP from 4G onwards, the difference between mobile network operators and Internet service providers has faded, yielding increasing overlap between telephony and Internet infrastructure (Ten Oever 2021). Therefore, they must be incorporated in this analysis according to the present author, not least because of their high geopolitical value amid the US-China competition (Ciuriak 2019), which is ongoing at the time of writing.

Based on micro-level observations of the relations among Chinese stakeholder communities and their interaction with other stakeholder communities in selected Internet governance and standardisation fora, this thesis observes their impact on Internet governance and standardisation processes norms and elaborates on the consequences for the Liberal International Order at large.

The next two sections will place the debates on Chinese stakeholders' engagement in global Internet governance in the broader context of the IR-theoretical scholarship on China's rise and the future of the Liberal International Order. Sections 1.4 and 1.5 respectively address the relevance of multistakeholderism and Internet fragmentation for the Liberal International Order. Next, section 1.6 describes the internal functioning and decision-making mechanisms of the governance venues under analysis in this thesis, mapping the venues in which different actors can cast their power. Finally, section 1.7 draws conclusions.

---

exchanged between devices through the Internet. Its standards therefore do not constitute 'Internet Standards' (3GPP 2021b).

1.2 *China's rise, the Liberal International Order, and contestation in global governance*

The debate on the crisis of the Liberal International Order has been the object of academic discussion for at least two decades (Acharya 2018; Duncombe, Dunne 2018; Ikenberry 2018; Mearsheimer 2019). Contextually, the power shift towards Asia and the supposed beginning of the 'Asian Century' have been core matters of discussion in the literature (Abramowitz, Bosworth 2006; Phillips 2013), driven by the debate on China's rise (Bo 2018; Buzan 2010; Friedberg 2005; Glaser 2011; Ikenberry 2008; Mearsheimer 2006; Zheng 2005). The way China has conducted its diplomatic activity at various levels of global governance and within the designated bodies has led observers to portray this emerging international actor either as a rule-breaker or as a rule-shaper – hinting at times at its willingness to become a rule-maker. Whether or not China's growing assertiveness will result into a reshaping of the rules of the existing order or to the establishment of a new one – whether or not following a hegemonic war – is the main open question (G. Chan, Lee, L. H. Chan 2011; L. H. Chan, Lee, G. Chan 2008; Pang, Lye 2012).

This debate is reflected in the field of global Internet governance. As introduced above, the existing multistakeholder governance model is a liberal-informed one and China has posed as a critic of it in favour of a multilateral/intergovernmental one (Flonk, Jachtenfuchs, Obendiek 2020; Negro 2020).

To contextualise the debate on China and Internet governance, one needs first to look at the broader question of China's rise and its positioning vis-à-vis the Liberal International Order. Recalling from the introduction, the Liberal Order was established at the end of World War II in the wake of US global hegemony and expanded globally after the Cold War (Parsi 2018). Normatively, it entails contrasting values, such as state sovereignty and universal human rights, but also a free-market tenet that provides ground for private-based transnational governance (Rosenau 1992; Scholte 2017).

At the systemic level, part of the broader debate on China's rise and the

decline of the Liberal International Order focuses on the likelihood of a hegemonic war and the likelihood of the replacement of the existing order with one led by China. The Chinese academic, political, and diplomatic communities have always stressed the peacefulness of China's rise. Famously elaborated by Zheng Bijian (2005), senior Chinese International Relations scholar and politician, the concept of 'peaceful rise' soon entered western debate. It was however in the same year that Friedberg (2005) first warned that China's rise was likely to lead to a hegemonic war with the US. After mapping several diverse theoretical approaches to China's rise, he concluded that

> *"[a]t the turn of the twentieth century, many observers in both Britain and Germany predicted that the two powers would be drawn together ineluctably by their growing economic links and societal connections […]. Such hopes were eventually borne out, of course, but only after the passage of another half century and two horrific wars. There is every reason to hope that U.S.-China relations will follow a smoother and more peaceful course. But neither history nor theory can provide any assurances that it will be so"* (Friedberg 2005, 45).

Such view was soon echoed by Mearsheimer (2006), who dubbed China's rise as necessarily 'unpeaceful'. Restressing Friedberg's (2005) conclusion, Mearsheimer finds in the security dilemma posed by the anarchical international system, whereby no state can be reassured over others' intentions, the reason for US's and China's quests for regional, as a proxy for global, hegemony to end in war. The challenge for China's international image as a rising power was acknowledged by its domestic elite, to the extent that the expression 'peaceful rise' was changed to 'peaceful development' in the Chinese Communist Party's (CCP) official policy to render it less threatening to a foreign audience (Kissinger 2011).

While widespread, the 'China threat theory' is not accepted by the whole Western academic community, especially in its most extreme and deterministic fashion as expressed in Mearsheimer's (2006) 'offensive realism'. On the contrary, in an optimist liberal reading, Ikenberry (2008; 2011; 2018) stressed on several occasions the resilience of the Liberal International Order in

accommodating the assertiveness of newly emerged powers. If China is allowed to grow powerful in the existing order, the argument goes, it will have no incentive to disrupt and replace it. Since the Liberal International Order allowed China to become the second most economically powerful country in the world by accepting it within its institutions, however defined, and organisations, such as the World Trade Organisation, China is set to become a member of the international order and see no need to confront the US militarily. The state might, in his view, pose as a revisionist on specific elements of the international order, but not as an order-maker.

It would however be a blunt simplification to assume that the whole 'China's rise debate' debate runs along a realism-liberalism dichotomy. Whereas Mearsheimer (2006) and Ikenberry (2008; 2011; 2018) are the two ends of the spectrum, Glaser (2011) falls in between, maintaining that structural elements of the international system do play a role in pushing US and China towards competition and confrontation. Nonetheless, the rational management of the confrontation by the elites of the two countries can avoid armed conflicts in his view. Mearsheimer's (2001) offensive realism foresees the 'tragedy of great power politics', a scenario in which tension between existing and rising powers are doomed to escalate to armed conflicts and culminate in a hegemonic war. While acknowledging the centrality of the systemic level of analysis, Glaser (2011) adds the element of individual/group reasoning in the analysis, reaching the profoundly different conclusion that hegemonic war can be avoided if elites act rationally.

In the Chinese scholarship, the non-deterministic line is followed by J. Wang (2011), who maintains that

> *"[i]f the international community appears not to understand China's aspirations [and needs], the Chinese people may ask themselves why China should be bound by rules that were essentially established by the Western powers. China can rightfully be expected to take on more international responsibilities. But then the international community should take on the responsibility of helping the world's largest member support itself"*.

In J. Wang's (2011) account, the capacity of state leaderships to communicate and acknowledge each other's intentions and needs can prevent a hegemonic war. This interactionist approach appears dominant in Chinese IR literature (Qin 2012; Yan 2014), although theoretical understandings differ.

This recalls closely, albeit heterogeneously, the approach adopted by the English School of International Relations. As one of its most prominent exponents, Buzan (2014) conceives the community of states as an international society, rather than an international system, in which states are the main actors interacting based on a self-established norm system created through time, either through the customary elaboration of patterns of behaviour (primary institutions) or the intentional establishment of norms, rules, and possibly organisation-based regimes (secondary institutions). Being state actors interacting in a societal system, he maintains that the rise of a new power to great power status is a two-way process that requires the emerging power to adapt to the existing systems of incentives and constraints and the existing great powers to accommodate some of the assertions coming from the former. Developing his analysis on the basis of historical elements combined with "the key elements of material power and social structure" (Buzan 2010, 34), he concludes that a US-China hegemonic war is not necessarily going to happen, as long as state leaderships will be capable of accommodating the aforementioned two-way process.

The debate on China's adaptation and contestation to the Liberal International Order (Ikenberry 2018), rather than its existential threat, is complicated by the emergence of private-based governance and regime complexity. Private-based governance encompasses technical standard-making venues as well as sectors of market and economic governance where such actors as companies or civil society enjoy actorness and can influence decision-making (Zürn 2018). In turn, regime complexity defines a governance ecosystem whereby one macro-topic is addressed by an indefinite number of fora, more or less global in scope, which are loosely interdependent and at times partially overlapping in scope and membership (Nye 2014).

Regime complexity and private-based governance are two intertwined

concepts as the former creates venues for a multitude of public and private actors to participate in policymaking, whereas the latter fosters the creation overlapping regimes whereby a variety of actors addresses partially overlapping topics of interest (Gómez-Mera 2016; Kawabata 2020; Westwinter 2021).

In this view, this thesis does not focus on the debates on the (real or presumed) existential threat of China to the Liberal International Order. Rather, it focuses on the normative challenge that China (and its domestic stakeholders) pose to the Liberal International Order in terms of influence in policymaking and in terms of the reshaping of the existing rules and norms of liberal-informed global governance. This is done by observing multistakeholder, private-based global Internet governance in selected venues as an example of a public-private governance regime complex where several stakeholders enjoy actorness and carry their interests along and across traditional national and geopolitical lines.

1.3 *Global Internet governance: what it entails and why it matters*

The history of Internet governance as we know it in the twenty-first century is deeply entrenched with the development of Liberal International Order and the tensions and challenges therein. A starting point can be identified with the so-called ‘DNS war’ of 1994-1998, whereby the first backlash between states supporting a multilateral system of governance and states supporting a multistakeholder one for CIRs took place. At this stage, multilateralists already pushed for a UN-based supervision of CIRs, pointing at the International Telecommunication Union (ITU) as the legitimate body (Leaffer 1998). However, the US authorities and epistemic communities pushed forward the establishment of a multistakeholder mechanism whereby CIRs management was to be conducted (mainly) by private actors, with governments maintaining a pure consultative role. This system was formalised

in ICANN. Despite the role of governments being relegated to the consultative Governmental Advisory Committee (GAC), the US retained a special role as ICANN was founded as a private not-for-profit organisation incorporated in Californian law and the US government retained a special connection through the so-called 'IANA contract'[2], which formalised the supervision of the US Department of Commerce over IANA (Mueller 2017).

While this solidified the passage of the Internet to the civilian realm from the military Arpanet project, in line with the process of commercialisation already launched through the establishment of the World Wide Web, it did not encompass its emancipation from the US government. In this view, the establishment of ICANN in this form epitomised the global expansion of the Liberal International Order in its free-market tenet and a restatement of US hegemony in the so-called 'unipolar decade'. In the realm of Internet governance specifically, the establishment of ICANN formalised the concept of multistakeholderism as a governance principle for the Internet, although it was still contested (Palladino, Santaniello 2021).

However, the new mechanism fit within an ensemble of existing venues for standardisation and CIRs governance. For example, the IETF preceded ICANN and was founded in 1986. Its standard-making activity nowadays is mainly industry-led. While the IETF makes standards for the Internet to function, the World Wide Web Consortium (W3C) was founded in 1994 to set the standards for the Web as we know it, whereas the much-older Institute of Electrical and Electronics Engineers (IEEE) sets connectivity standards such as IEEE 802.11, better known as Wi-Fi. The work carried out in W3C and IEEE is industry-based, much like in 3GPP, the main body responsible for the elaboration of mobile connectivity standards from the third generation (3G) onwards since 1998 (Nye 2014).

In other words, the 1990s signalled the emergence of a globalised, strongly private-based regime complex for the management and development of the Internet and Internet-enabled technologies. In this, ICANN came to be central

[2] IANA: Internet Assigned Numbers Authority.

in the management of CIRs, epitomising the multistakeholder management of the Internet by private and – to a lower extent – public actors.

In more historical and technical detail, the management of CIRs takes the name of 'IANA stewardship'. The IANA functions, conducted by ICANN, entail three core elements: IPs and AS (Autonomous System) numbers distribution; DNS root zone management; and management of the protocol parameters (Scholte 2017). An IP is a unique numerical identifier for network-connected devices; an AS number is "a globally unique identifier that defines a group of one or more IP prefixes run by one or more network operators that maintain a single, clearly-defined routing policy" (African Network Information Centre 2020, hereafter AFRINIC); the DNS is a hierarchical system of servers and databases that translates domain names into IPs; the protocol parameters involve such global technical operational standards that allow Internet-connected devices to exchange data: these include the Transmission Control Protocol (TCP) and Hypertext Transfer Protocol (HTTP) (Scholte 2017)[3].

The establishment of ICANN to oversee the IANA functions concluded the so-called 'DNS war' in favour of multistakeholderism, although the qualifications illustrated above apply regarding the US's role (Leaffer 1998). Point B of the memorandum of understanding that preceded the IANA contract and recognised ICANN's role in the IANA functions reads: "[b]efore making a transition to private sector DNS management, the DOC requires assurances that the private sector has the capability and resources to assume the important responsibilities related to the technical management of the DNS" (ICANN

[3] TCP allows "data [to be] transferred with an end-to-end reliability from the source host to the destination host". TCP/IP is also referred to as the 'Internet Protocol Suite', that is, the series of fundamental protocols (which includes, but is not limited to, TCP and IP) allowing device identification and data exchange through the Internet to work the way it does; HTTP "is used in communication between the web pages and web servers. It allows users to download pages and connect to servers located in different parts of the globe" (Internet Corporation for Assigned Names and Numbers 2011; hereafter ICANN).

1999). Importantly, while the MoU referred strictly to DNS management, the IANA contract referred to the whole of the IANA functions (Mueller 2017; Scholte 2017).

It must be underlined for the sake of completeness that ICANN's role in the IANA functions is one of supervision rather than direct management: for example, ICANN allocates IPs to the Regional Internet Registries (RIRs)[4], which in turn distribute them to final users. As for the DNS management, ICANN establishes TLDs, but the sale of domain names to end users is done by the so-called registries through the so-called registrars, both of which act based on a contract with ICANN.

In historical terms, the establishment of ICANN signposts a passage from Internet governance by the technical community to multistakeholder Internet governance. Before ICANN, the IANA activities were conducted by Jon Postel and the IETF was a niche body of technical experts, while with the foundation of ICANN a variety of stakeholders gained an institutionalised role in Internet governance (Palladino, Santaniello 2021). In time, the IETF itself saw its participation expanding, with a strong presence of corporate actors (Belli 2015). In other words, while the Internet prior to the 1990s was mainly governed by the US government and mainly US-based epistemic communities, from 1998 onwards, the largely private-based multistakeholder ecosystem centred on ICANN has taken form. Within the debate on digital sovereignty, the return of state in Internet governance, and the future of multistakeholderism, this signals that governmental presence in private-based Internet governance has historically never completely faded away, reminding one of the Internet's military (thus state-centric) origins (Ten Oever 2021).

[4] "A Regional Internet Registry (RIR) is a not-for-profit international organization that deals with the allocation of Internet Protocol (IP) address space (IPv4 and IPv6) and the Autonomous System numbers within a geographical region." IPv4 and IPv6 refer to the two versions of IPs currently in use, IPv6 being the newest generation. While technically incompatible, the two versions have been bridged through protocols allowing devices using one IP version can communicate with those using the other (ICANN 2020).

In the wake of ICANN's foundation, around the beginning of the twenty-first century, China posed as a staunch multilateralist, as opposed to the multistakeholder system epitomised by ICANN (Cai 2018a; Mueller 2017). The ITU-centred system envisaged by multilateralists would have been largely based on a one-state-one-vote system, with non-state stakeholders in marginal positions. Currently, the ITU itself has incorporated multistakeholder consensus-based decision-making procedures. However, when it comes to regulatory decisions or decisions on which consensus cannot be built, it is the state representatives who decide by majority votes (Glen 2014).

In turn, the multistakeholder model headed by ICANN grants governments a merely consultative role in the IANA functions (Mueller 2017), whereas the basic Internet protocols and standards are elaborated at the IETF, a private- and consensus-based engineering body. While governments are not formally excluded from IETF work, its main contributors are engineers from tech multinationals (Arkko 2021; Belli 2015; Internet Engineering Task Force 2020, hereafter IETF), although its consensus-based decision-making process limits the influence of these major actors (Harcourt, Christou, Simpson 2020).

At the beginning of the twenty-first century, China's main *casus belli* against ICANN was the latter's recognition of Taiwan as a member of the Governmental Advisory Committee (GAC). This led to the Chinese government's boycott of ICANN's meetings and GAC activities. The extent to which such boycott was actually in place is debated (Creemers 2020a), but this is better observed in the forthcoming chapters. What matters at this stage is that the Chinese government held a critical position against ICANN amid the Taiwan question. In addition, China and other countries from the developing world criticised ICANN amid its formal relation to the US DOC (Glen 2014; Hurel and Santoro Rocha 2018; ICANN 1999; Mueller 2017).

However, between 2003 and 2005, the two rounds of the World Summit on the Information Society (WSIS), a UN-sponsored global multistakeholder forum, did not conclude with a phase out of the ICANN-centred governance model. WSIS concluded instead with the adoption of the so-called 'Tunis Agenda' and the establishment of the multistakeholder policy forum known as

the ‘Internet Governance Forum’ (IGF) (International Telecommunication Union 2005, hereafter ITU). Most importantly, the Tunis Agenda recognised multistakeholderism as a guiding principle of global Internet governance as provided by the Working Group on Internet Governance (WGIG) in its working definition of the term (WGIG 2005). This working definition consolidated the existing multistakeholder governance mechanism by stipulating that

> *“Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet”* (WGIG 2005, 4).

While the Tunis Agenda seemingly strengthened the global acceptance of multistakeholderism as a governance principle for the Internet, with the Chinese government progressively normalising relations with ICANN between 2006 and 2009 (Creemers 2020a), the World Conference on International Telecommunications of 2012 (WCIT-12) was interpreted as a reawakening of the multilateralist-multistakeholderist divide. Held by the ITU to discuss and approve a revised version of the International Telecommunication Regulations (ITRs)[5], it concluded with their rejection by US-led bloc of countries, maintaining that the new rules would allow too much governmental intervention in the communication sectors (Schackleford, Craig 2014). In this context, Glen (2014) identifies a threefold cleavage over multistakeholderism. Firstly, the supporters of the existing system are identified as ‘open multistakeholderists’. The middle of the spectrum is occupied by ‘open multilateralists’, supporters of a multilateral form of Internet governance that allows consultative and participatory space to non-state actors. Finally, at the other end of the spectrum lie the ‘repressive multilateralists’, supporters of a

[5] ITRs “serve as the binding global treaty designed to facilitate international interconnection and interoperability of information and communication services” (ITU 2020a).

strongly state-centric Internet governance system. China, together with Russia, was identified as one of the most outspoken members of this latter group. This led many to dub WCIT-12 as the 'Internet Yalta' (Klimburg 2013), although this is disagreed upon by the global Internet governance scholarly community (Mueller 2013).

At the time of writing, the importance of WCIT-12 and its meaning for both the ITU and the multistakeholder model are being reconsidered (Winseck 2020). However, it remains in the literature as a moment in which major normative tension in governance was experienced and perceived (Palladino, Santaniello 2021).

The following year, the PRISM scandal hit the US, with Edward Snowden's revelations tarnishing the US's reputation and casting further doubts on the legitimacy of its exceptional role in Internet governance. This triggered the launch of the so-called 'IANA stewardship transition' by the second Obama administration, which made ICANN independent from the US government in 2016, thus eliminating one of the main points of criticism against the organisation (Mueller 2017). A recent article by Negro (2020) stresses China's ambivalence in its participation in both the ITU and ICANN. While the latter has become increasingly accepted and participated in by Chinese stakeholders, Chinese presence and influence in the ITU keeps growing. According to Negro (2020), this means that China's challenge to the ICANN-based Internet governance system is still there but must not be given a dichotomous reading. In fact, at the same time, high-ranking Chinese politicians and functionaries have endorsed ICANN and the multistakeholder principle.

In line with these findings, the post-IANA stewardship transition debate on China and multistakeholderism has become more nuanced. A degree of ambiguity is recognised by many and the duality of the early 2000s debate has faded (Mueller 2017; Negro 2020; Shen 2016). Meanwhile, Chinese scholarship on the topic has become more prominent internationally, both from China-based Chinese scholars and from Chinese scholars abroad.

As for the issue at stake, ambiguity in China's stance towards

multistakeholderism emerges from Chinese literature too. The role of Chinese private actors is extensively analysed by Shen (2016), who maintains that China has become more participatory and influential in technical standardisation activities through its private actors' presence in multistakeholder fora. She also contributes to contextualising this in the broader Chinese foreign policy strategy, which currently runs under the label of 'Belt and Road Initiative' (BRI) or 'One Belt One Road' (OBOR) (一带一路 yidai yilu) (Shen 2018). On the other hand, Cai (2018a) acknowledges the role of Chinese private actors in multistakeholder governance, but maintains the Chinese government is central. In her words, "[b]oth the multilateralism and multi-stakeholder approaches recognize the role of different actors in global cyber governance; their major difference lies in the positioning of those actors, particularly in who is to play a dominant role" (Cai 2018a, 59). She underlines that China supports state centrality in Internet governance and defines this approach as "multilateral pluralism based on cybersovereignty" (Cai 2018b, 647).

Whether and to what extent Chinese private actors are state-controlled is an open question and casts doubts on the future of multistakeholderism inasmuch as formally private entities may serve to enhance state influence in multistakeholder governance. This is an overarching question in the fields of CIRs as well as mobile Internet technology standards.

This leads the discussion to the second subset of this research's analysis. Attempts to study China's policies in mobile Internet technologies standardisation processes are very few at the academic level, despite 5G having drawn attention in politics and the media. Both Zhong (2019) and Pupillo (2019) helped to shed light on the complicated and non-transparent relationship between the two. To be sure, the fact that Chinese private actors have grown stronger has pushed China into further acceptance of the multistakeholder system, where its domestic companies play a major role in standardisation processes (Shen 2016). Nonetheless, this does not allow to discard forms of state control on private companies. Kim, Lee and Kwak (2020) observe

China's 5G standardisation policies through the lenses of techno-nationalism. To them, techno-nationalism "commonly features when developing countries start to drive technological catch-up and economic development" (Kim, Lee, Kwak 2020, 3) and entails state empowerment, growth orientation, and global connection. Through these lenses, Kim, Lee and Kwak (2020) see patterns of alliance between government, telco, and operators (whether public or private) in an effort to create domestic technology and reduce import-dependence, while contributing to global standardisation as first movers rather than 'catch-uppers'.

Through a different theoretical lens, Tang (2019) reaffirms this view of government policy (which includes funds and R&D coordination) supporting the progressive 'going out', that is, growth and expansion in the global market, of Chinese tech companies. This view is restressed by Gong (2019), who underlines governmental recognition of the need to push international standardisation to achieve comparative advantage. Further Chinese literature on the topic is often concentrated on the policy implications of Huawei's condition amid the US-China trade war (Ma 2020), while Zhou (2019) observed Chinese tech companies' internationalisation and relative growth until achieving a leading role in 5G standardisation. In this, Zhou (2019) sees the source of such capacity in inter-sector research and development (R&D), but the role of political relations remains unaddressed.

In other words, the question of political control over private companies remains unanswered and scholars within China and the West (different political situations notwithstanding) have developed heterogeneous views. What emerges from Chinese and non-Chinese literature on Chinese engagement with standardisation is a strong government role, at least in policy coordination. Whether this translates simply as more engagement in multistakeholder governance (Shen 2016), a form of 'open' or 'repressive' multilateralism (Glen 2014), or similarly 'multilateral pluralism based on cybersovereignty' (Cai 2018b) is open to debate. The boundaries between coordination, influence, and control remain blurred amid the authoritarian characteristics of the Chinese government (Jia, Winseck 2018; M. Jiang 2012; Pupillo 2019; Segal 2018;

Zhong 2019).

Overall, it can be observed that the multistakeholder conception of Internet governance differed from a multilateralist understanding deeply enough as to yield normative confrontation (Flonk, Jachtenfuchs, Obendiek 2020). While states remain undeniably a central actor in the international order, multi-actor understandings of IR need to be adopted when observing such fields as global Internet governance where private actors can exert extensive power (Keohane, Victor 2011; Nye 2014).

A deeper discussion of these aspects is provided in the forthcoming sections of this chapter. Debates around the future of multistakeholder Internet governance as a facet of the Liberal International Order and its characteristics and adaptation to contestation will be followed by the second debate addressed in this thesis, that is, Internet fragmentation. Inasmuch as the Internet was created under principles of openness and universal accessibility, allowing everyone to access the same contents from everywhere an Internet connection is provided, whether the Internet is to remain a single intercommunicable 'network of networks' strikes at the very heart of the Liberal Order in its global spatial dimension (Mueller 2017; Parsi 2018; Scholte 2017).

To summarise and conclude, debates on the Chinese influence on the future of multistakeholderism and Internet fragmentation are deeply entrenched with the future of the Liberal International Order. There is disagreement in the literature on the extent to which China's government is in control of non-state stakeholders' choices and actions. However, it must be underlined that companies' and state's policies towards the multistakeholder governance system differ. Whereas the Chinese government boycotted ICANN amid Taiwan's presence in the Governmental Advisory Committee, commercial stakeholders were still participating in ICANN – although the overall Chinese participation in ICANN was limited in its initial stage (Creemers 2020a; Negro 2020). While this cannot tell much on the control relationship – whether real or presumed – between Chinese stakeholders and the party-state, it provides a nuance on actors' behaviour and the need for a theorisation that accounts for everyone's actorness while taking power relations into account. Furthermore,

what emerges from the literature is that the relationship between Chinese actors and the existing global Internet governance system needs a non-dualistic, nuanced reading that has only recently started emerging. To this, a multi-actor approach needs to be adopted, along with definitions of such concepts as 'state-influence' and 'fragmentation' that encompass their multifaceted nature. This brief introduction to the questions at stake provides an explanatory overview of the techno-political dynamics at stake behind the most technical caveats of global Internet governance.

1.4 *The question of multistakeholderism: what is at stake for the Liberal Order*

One takeaway of section 1.3 is that both multistakeholder Internet governance and the concept of one, open universal Internet are deeply entrenched with liberalism and constitute a facet of the Liberal International Order. After all, the 'multistakeholderist vs. multilateralist' contestation illustrated in the previous section and summarised in Table 1.1 is one of 'liberals vs. sovereigntists' (Flonk, Jachtenfuchs, Obendiek 2020).

	Multistakeholderism (private-based governance)	**Multilateralism (state-based governance)**
Type of actors and their roles	*Private actors*: make (most) decisions; *Public actors*: mostly in consultative roles.	*Private actors*: consultative/uninvolved. *Public actors*: make majority-vote decisions.
Political connotation	Liberal	Sovereigntist
Governance fora	ICANN, IETF, IGF, 3GPP, W3C, others.	Most UN fora (ITU), other state-based orgs.

Table 1.1: 'multistakeholder' and 'multilateral' Internet governance in sum.

As anticipated, the debate has developed in a less dichotomous fashion

(Negro 2020), with criticism levelled against multistakeholderism from within the Western-liberal world. For instance, Santaniello (2021) pinpoints that the 2018 speech by French president Macron at the Internet Governance Forum portrays a shift towards a more state-interventionist stance in Western democracies, one that falls within the broader spectrum of digital sovereignty practices. From a different perspective, Cath (2021) finds obstacles in human rights advocacy in technical standard-making at the IETF due to longstanding conceptions of technological neutrality. While this falls outside the scope of this thesis, it is important to stress the heterogeneity of Western approaches to multistakeholderism and the non-dichotomous nature of the 'liberal vs. sovereigntist', or 'multistakeholderist vs. multilateralist' debate.

A further criticism levelled against multistakeholderism is that it is often unbalanced in favour of powerful corporate actors, thus constituting a fully-fledged form of private governance mechanism in its neoliberal sense, rather than a strongly private-led but mixed public-private setting. While this is debated, it connects directly to the fact that around 80% of IETF participants were from tech multinationals by 2015 (Belli 2015). Observing authoritative figures, Cisco, Huawei, Ericsson, Google, and Juniper are the main yearly contributors to the IETF's work in terms of Requests for Comments (RFCs) – that is, IETF's technical documents including anything from networking protocols down to meeting notes (IETF 2020) – published in 2020 (Arkko 2021). In other words, influence in the making of Internet standards and their management is strongly skewed in favour of industry, which sums to business actors' formal role in policymaking in ICANN's Supporting Organisations (SOs) (Palladino, Santaniello 2021; Scholte 2017).

The overwhelming role of multinationals in the establishment of the Internet's basic protocols is evident. To be sure, technologists formally participate in the IETF's work in a personal capacity. Furthermore, decision-making is based on rough consensus, where dissenting opinions are considered but do not constitute a veto. This entails that any meaningful open opposition to a proposed standard can be influential, no matter how powerful the proponent. Nonetheless, virtually every participant is sponsored by an entity

and works on its behalf. As the wealthiest entities are also those who can pool the deepest (in terms of technical knowledge) and broadest (in terms of human resources) expertise, tech multinationals represent the leading actors in the IETF (Belli 2015). Numbers are not necessarily symptomatic of influence, as companies like Amazon do not participate in the IETF but can influence standard-making by choosing which standards to adopt. Nonetheless, big techs' size and their capacity to participate and pool expertise make them capable of creating and establishing standards that are more likely to become widespread in the industry (Harcourt, Christou, Simpson 2020).

Furthermore, prior to the IANA stewardship transition that took place in 2016, there was broad criticism against ICANN amid its ties to the US DOC as mentioned above (Carr 2015; Mueller 2017; Negro 2020). Despite the transition, criticism has not faded, as ICANN still constitutes a private entity incorporated in Californian law. However, following Snowden's revelations and the PRISM scandal, which triggered the IANA stewardship transition, criticism against ICANN's current form and ties awakened in the liberal field as well.

Despite this, Mueller (2017) finds the IANA stewardship transition rid ICANN of one of the most outstanding arguments against its roles. Furthermore, Scholte (2017) finds that the community of individuals participating in ICANN, including Chinese ones almost independently of their stakeholder affiliation, widely sees ICANN as a legitimate actor in the role it conducts in global Internet governance. This, of course, does not mitigate criticism from the broader community of people involved in Internet governance at large. Most everyday users of the Internet, for example, are not aware of the existence of ICANN and its role, despite the pervasiveness of the Internet in most individuals' life (Jongen, Scholte 2021). Nevertheless, these findings, along with Negro's (2020) study on China's ambiguity in its relationship to ICANN and the ITU as illustrated in section 1.2, cast a multifaceted light on the challenges faced by the multistakeholder (that is, liberal-informed) global Internet governance system by such actors as the Chinese government.

In brief, contradiction in multistakeholderism is found inasmuch as it entails a role for governments, companies, and civil society at least (WGIG 2005), but in practice there is overlap with the concept of private-based governance owing to the heavy presence of so-called 'big techs' (Belli 2015; Palladino, Santaniello 2021; Santaniello 2021). As anticipated in the previous sections of this chapter, this creates tension between the concepts of private-based governance and public-private governance.

Debates notwithstanding (GAC 2015b), this thesis focuses on the increasing role of states in the existing Internet governance complex and the potential shift to multilateralism under the push of a non-liberal power, that is, China. The terms 'multistakeholderism' and 'private-based governance' will be used interchangeably, as derivatives of liberalism and the Liberal International Order in their free-market form. However, a preference for the term 'multistakeholderism' must be expressed due to its all-encompassing meaning when referred to the public and private actors involved in Internet governance, despite the pre-eminence of the latter in decision-making. In turn, multilateralism is conceptualised as opposed to multistakeholderism as a governance model as it is most often promoted by non-liberal powers – as per Table 1.1.

While multilateralism is intrinsic in the Westphalian characteristics of the Liberal International Order (Deudney, Ikenberry 2018), in the context of Internet governance it is conceived as a sovereigntist alternative to the liberal-informed ICANN-centred multistakeholder model (Flonk, Jachtenfuchs, Obendiek 2020). The normative divide between multistakeholderism and multilateralism can also be observed in the characteristics of the IETF and the ITU as standardisation venues. This is not only the case in the private-based vs. state-based nature of the two bodies: to be precise, the ITU seeks consensual decisions among industry participants and uses state representatives' majority vote only in case of major impasses or when regulatory aspects are at stake (see for example: Glen 2014). However, in the ITU, governments have permanent and decisional representation and ITU standards (recommendations) are approved by member states. While their implementation is not mandatory,

recommendations are often incorporated in national laws as standards *de jure* (ITU 2021). In contrast, the IETF is private- and consensus-based as described above. Finally, the ITU is historically specialised in telecommunication in a stricter sense (that is, telephony), a technology whose infrastructure is built on a different 'philosophy' than the Internet's.

Furthermore, telecommunication and Internet infrastructures work in different ways: while the Internet was built on a building-block approach, where new specifications are created using the existing ones in previously unexpected ways, telephony works on fully determined infrastructures. Moreover, the Internet infrastructure is a 'dumb pipe' used by intelligent endpoints (devices) to connect to each other. Conversely, telephones are dumb devices, and the interconnection work is done by the infrastructure. While this is a simplified illustration of the functioning of the two types of infrastructure, also considering their historical and growing interconnection in the functioning (Maxigas, Ten Oever 2021; Negro 2020), it is a useful benchmark to gauge the security implications of the two types of infrastructure. For example, while surveillance in telephony can be easily done by controlling the infrastructure, Internet surveillance requires control on the endpoints. Furthermore, this characteristic of the Internet makes it less easy to disrupt. After all, the founding idea of the Internet was to have a distributed communication infrastructure in the Cold war era that could not easily be disrupted in case of military emergency (Leiner et al. 1997).

A line of thinking similar to that applied to the IETF is applicable to 3GPP, which constitutes this research's focus for the mobile Internet technology standards subsets.

To begin with, 3GPP does not possess legal personality, but is constituted by seven national and regional Standards Development Organisations (SDOs) with mixed private and public participation, as illustrated in detail later in this chapter. Through membership to these, organisations can formally participate by sending their affiliates to Technical Specification Groups' work (3GPP 2020). As Pohlmann, Blind and Hess (2020) show, 3GPP, while participated in by both private and public entities, is strongly private-driven. Huawei, Ericsson,

Nokia, Samsung, and Qualcomm are among the main proponents of 5G standardisation proposals – which roughly translates as major (prospective) patents owners. To be sure, state-owned enterprises such as the Chinese manufacturer ZTE are also present, along with technical public entities. Yet, the five aforementioned Chinese, European, South Korean, and US companies are the leaders in the standard-making process and are private actors responding to IPR and market needs. State-company relations notwithstanding, 3GPP work is private-based and business-oriented. Decisions are made based on consensus, with voting as a last resort (3GPP 2020). For the sake of completeness, it must be understood that 3GPP is not the only standardiser of new generations of mobile Internet technologies. Besides, there are ad hoc bodies that have been working alongside 3GPP in elaborating 5G-based technologies as 5G developed (Blanco et al. 2017). However, mobile connectivity work was initiated in 3GPP and, from 3G to 5G, the most globally influential standards were elaborated in this venue. This qualifies it as the most influential standard-making forum in this sector (ITU 2020b; Ten Oever 2020).

The final specifications for a mobile connectivity generation emerged from intra-3GPP interactions are then referred to the ITU Radiocommunication Sector (ITU-R), which analyses and accepts or rejects them based on the requirements it made explicit before the launch of the standardisation activity. In the case of 5G, such requirements were specified in ‘International Mobile Telecommunications 2020’ (IMT-2020) (ITU 2020b).

To put it briefly, 3GPP fits the business-led, private-based governance ecosystem illustrated above. Membership is mixed, with contributors from companies as well as public bodies such as academia. However, criticisms similar to those raised against the IETF related to a few network manufacturers’ leading position in the standardisation process can be raised.

In this case, such criticism is mitigated by the consensus-based decision-making process, which means that meaningful opposition by minor actors can influence decision-making. After all, big actors have an interest in having their own standards adopted universally and gain in terms of royalties as well as scale economies. Standards scalability is therefore a central factor, which

shapes standardisation activities as a coordination game (DeNardis 2014).

A major difference with the IETF's way of working must be underlined. Whereas the latter adopts the building-block approach illustrated above, 3GPP makes full architecture the way telephony works. While it is true that new generations of mobile connectivity can work on top of previous generations' infrastructure in their non-standalone (NSA) version, the final deployment is always that of a new architecture for every generation (Blanco et al. 2017; Dahlman, Parkvall, Sköld 2021). Furthermore, final specifications need to be submitted to the ITU for approval as standards (recommendations, in ITU jargon).

To conclude, multistakeholderism is a governance mechanism where power is unbalanced, despite stakeholders participate nominally on equal footing and in different roles. While public and private actors are involved, the decision-making process is strongly private-driven. As per Table 1.1, its connotation is liberal and emerged in the 1990s with the globalisation of the Liberal International Order in its free-market aspects.

1.5 *Internet fragmentation: a challenge to the Liberal Order in its global spatial dimension?*

To begin a discussion on the second topic of this dissertation, namely Internet fragmentation, a mapping of the basic Internet architecture need be made. The Internet architecture is acceptedly divided into four layers according to the so-called TCP/IP model summarised in Table 1.2. Numbered from one to four from the deepest to the one 'closest' to the user, the TCP/IP four layers are: the network access layer (also known as 'link layer' or 'network interface layer'); the Internet layer (or 'network layer'); the transport layer; and the application layer (International Business Machines Corporation 2020, hereafter IBM; ICANN 2011; Russell 2013; Socolofsky, Kale 1991). Sometimes, a fifth layer is added before the network access layer: the hardware layer (IBM 2020).

Nr.	Layer name	Protocols (examples)
4	Application	HTTP/DNS/SMTP/FTP
3	Transport	TCP/UDP/QUIC
2	Internet	IP
1	Network access	Wi-Fi/Ethernet/5G
	(Hardware layer)	

Table 1.2: the TCP/IP model (Harcourt, Christou, Simpson 2020; Russell 2013).

As summarised in Table 1.2, the network access layer provides interface to the networking hardware, such as the ethernet and gateways; the Internet layer is a group of internetworking specification, with the IP as the most important one; the transport layer provides reliable end-to-end transmission of the datagrams (packages) transferred from an IP address to another. Two of the most important protocols at this layer are TCP and UDP (User Datagram Protocol); finally, the application layer provides direct service to users, including FTP (File Transfer Protocol) and SMTP (Simple Mail Transfer Protocol) (ICANN 2011).

To be sure, the taxonomy of technical layers has been subjected to debate (DeNardis 2016). The IETF, for example, adopts the TCP/IP model, while the Open Systems Interconnection (OSI) features a seven-layer stratification (physical, data link, network, transport, session, presentation, and application layers) (DeNardis 2016). However, OSI was superseded by the TCP/IP model,

which now constitutes the basis upon which the basic working protocols of the Internet are elaborated at the IETF (Russell 2013; Socolofsky, Kale 1991).

Debates on Internet fragmentation do not always adopt a strictly technical perspective. On the contrary, political, economic, and regulatory considerations are made. A rapid Google Scholar search for 'Internet fragmentation' delivers about 493,000 results. A few irrelevant results notwithstanding, the first ten articles approach the issue from technical, regulatory, commercial, media, and political perspectives. More strictly technical, political, and economic articles emerge if the search is restricted to the 2016-2020 timespan, which suggests the term has been narrowed down and clarified in time. Nonetheless, the risk of the term 'fragmentation' being used as a catchphrase is high.

To begin with, a 'Future of the Internet Initiative' White Paper for the World Economic Forum (WEF) identified three types of fragmentation: technical, governmental, and commercial. Technical fragmentation entails "conditions in the underlying infrastructure that impede the ability of systems to fully interoperate and exchange data packets and of the Internet to function consistently at all end points"; governmental fragmentation takes place in the presence of "[g]overnment policies and actions that constrain or prevent certain uses of the Internet to create, distribute, or access information resources"; finally, commercial fragmentation consists of "[b]usiness practices that constrain or prevent certain uses of the Internet to create, distribute, or access information resources" (Drake, Cerf, Kleinwächter 2016, 4). Of course, the three ideal-types of fragmentation can intersect. For example, government policies can create market incentives for companies to push towards the creation of incompatible technical standards that will be adopted by law and to which every ISP or service provider operating in the country must adapt. This is a hypothetical (and possibly extreme) example, but it is explanatory of potential intersections among the three ideal-types.

Other definitions of fragmentation based on commercial or regulatory considerations can be found. For example, the principle of 'net neutrality', albeit falling outside the scope of this thesis, is held to have prevented many commercial forms of fragmentation, as it entails ISPs not being allowed to

selectively restrict content delivery (Kourandi, Krämer, Valletti 2015). Furthermore, DeNardis (2016) brings clarity to the fragmentation debate by pinpointing that, historically, the Internet is not a unified whole. It is in fact a 'network of networks', most of which are privately managed and interoperable only through the adoption of common protocols. She identifies four overlapping conceptual categories: physical infrastructure; logical resources (such as IP addresses and other protocols); application and content layer; and legal layer (cutting across the previous three). By assessing the status of fragmentation in the four conceptual categories, DeNardis (2016) sheds light on the many-fold nature of the factors that may yield fragmentation. Digital literacy, accessibility (for example, connectivity, digital divide), language (most people consume contents in their local language solely), and other social elements create non-communicating 'bubbles' of users without formal fragmenting elements being in place the regulatory, commercial or other levels.

Nonetheless, Mueller (2017) criticises most definitions of fragmentation as too broad and distinguishes between 'alignment' and 'fragmentation'. To Mueller (2017), 'fragmentation' can only refer to the creation of a technically separate Internet, whereas every other regulatory limitation to or control of information fluxes within a country is to be dubbed as alignment to domestic legislation. In short, when states like China censor Internet contents and platforms or browsers (such as Google, Facebook, WhatsApp), they 'align' the Internet to national regulation, rather than fragmenting it. As a matter of fact, the DNS used in China is the IANA-established one and the Chinese Internet infrastructure continues to operate through TCP/IP (Mueller 2020a). The mere use of a Virtual Private Network (VPN) allows one to overcome the restrictions imposed by the so-called 'Great Firewall of China', allowing full access to Internet contents available abroad. This allows Chinese companies not to lose the network benefits, that is, the scale economies provided by being in a technically unified Internet: technically separate *splinternets* would force international device manufacturers to produce devices with different specifications for different markets in order to operate on technically separate 'internets' (Mueller 2017).

What emerges from this debate in the literature is the deeply political nature of the concept of fragmentation. For example, despite the fact that 'commercial fragmentation' exists as a definition (Drake, Cerf, Kleinwächter 2016), few would accuse Netflix of fragmenting the Internet because it makes certain contents available in certain countries and not in others. This is simply attributed to a system of incentives and constraints (economic, regulatory, IPR-related, etc.) within which the company makes microeconomic decisions. Nonetheless, fears of fragmentation are bigger when powerful state actors are involved (Hoffmann, Lazanski, Taylor 2020), even though with a VPN it is (technically) simpler to overcome China's 'Great Firewall' than Netflix's restrictions. Arguably, this is because many in the literature implicitly recognise that potential fragmentation from powerful state actors with deeply different political values and identities could undermine the ideological basis of the existing Internet governance model (Segal 2016). To conclude, for fragmentation to take place, there needs to be a political purpose followed by a technical split within the infrastructure such that devices connected to different networks cannot intercommunicate due to the adoption of incompatible identifiers.

In this sense, Internet fragmentation challenges the global spatiality of the Liberal International Order. As established in the introduction of this chapter, the Internet and its multistakeholder governance epitomise the US's hegemony during the so-called 'unipolar decade'. If one conceives the Internet as a global network of networks allowing users to exchange data seamlessly between network-connected devices anywhere such connectivity is provided, hampering such exchange hits at the core of the Liberal Order in its global spatial dimension.

1.6 *A few notes on policy- and standard-making functioning*

Having identified the importance of Internet fragmentation and the future

of multistakeholderism for the Liberal International Order, it is necessary to observe the detail of the functioning of Internet governance fora to make sense of the several venues for policymaking and influence that the regime complex opens up to a variety of public and private actors. Therefore, this section offers a panoramic of the functioning of the three fora analysed in this thesis, namely ICANN, IETF, and 3GPP.

1.6.1 *Internet Corporation for Assigned Names and Numbers*

To begin with, ICANN is a private not-for-profit entity registered in California. As in any private organisation, decisions are made by the Board of Directors. The Board of Directors consists of sixteen voting members and four non-voting liaisons. Half the voting members (eight) are appointed by the Nominating Committee (NomCom), two by the Generic Names Supporting Organisation (GNSO), two by the Country-code Names Supporting Organisation (ccNSO), two by the Address Supporting Organisation (ASO), one by the At-Large Advisory Committee (ALAC) along with the Regional At-Large Organisations (RALOs), and the sixteenth voting member is the President/CEO (appointed *ex officio*). The four non-voting liaisons are from the IETF, the Governmental Advisory Committee (GAC), the Security and Stability Advisory Committee (SSAC), and the Root Server System Advisory Committee (RSSAC) (ICANN 2019).

The NomCom is made of fifteen voting members from the GNSO (seven), ALAC (five), ASO (one), ccNSO (one), and the IETF (one). These are accompanied by three non-voting members from GAC, SSAC, and RSSAC and three non-voting co-chairs (ICANN 2019).

A further distinction is between Advisory Committees (ACs) and Supporting Organisations (SOs). The former represents a specific stakeholder group’s interests and formulates broad advice for the Board, while the latter formulates policy subjected to Board adoption. ALAC is the advisory committee representing users and it is composed of RALOs, in turn consisting of individual affiliates, whose membership is either direct or through a national

users' organisation. ALAC is the only AC appointing a voting member of the Board. SSAC advises the Board on matters of security and stability of the naming and address allocation system and is composed of interested technologists. Similarly, RSSAC advises the Board on matters of administration, integrity, and functioning of the Root Server System, consisting of twelve operators administering thirteen 'identities' (or 'root services') managing more than one thousand machines called 'instances', a hierarchy that constitutes the apex of the DNS (Conrad 2020). Finally, GAC groups together governments. These can be national governments, but also supranational authorities such as the European Commission, international organisations such as the European Organisation for Nuclear Research (CERN) and the ITU, and contested territories such as Taiwan (referred to as Chinese Taipei) and Palestine. Several forms of engagement are foreseen by the ICANN bylaw to allow different forms of governmental organisations, other than governments, to participate (ICANN 2019). GAC consensus advice can be rejected with a 60% majority vote of the Board, which then must provide their reasoning.

As for SOs, the GNSO makes policy on generic Top-level Domains (gTLDs). Its Council is divided in two houses for voting purposes: contracted parties and non-contracted parties. The former are registries and registrars. Registries are contracted by ICANN to manage a TLD. gTLDs such as '.com' are most often managed by private organisations, whereas ccTLDs are more often managed by state-sponsored registries. Registrars sell gTLDs to final users (that is, website owners) on behalf of the registries (ICANN 2021). The second house, non-contracted parties, is composed of commercial constituencies (business, intellectual property, Internet Service Providers) and non-commercial constituencies (non-commercial users and not-for-profit organisations). The GNSO Council has the power to start Policy Development Processes (PDPs) in the manners specified by ICANN bylaws. Bylaws also specify the majorities needed for decision-making and policy adoption in PDPs, the outcome of which is subject to approval by the GNSO Council and finally the ICANN Board. PDPs are conducted by ad hoc working groups receiving comments from outside the group itself and in which GNSO non-members can

also participate (ICANN 2019).

The ccNSO plays a similar role to GNSO, but for country-code Top-level Domains (ccTLDs). This means participation in ccNSO sees many more state-controlled or state-related entities, such as the China Internet Network Information Centre (CNNIC), manager of the '.cn' ccTLD (ICANN 2019).

Finally, ASO supports the Board in policies related to the allocation of IP addresses. Its membership is from the RIRs. RIRs manage IP distribution in the five regions of the world (roughly corresponding to continents) under ICANN's coordination (ICANN 2019).

The three SOs plus ALAC and GAC participate in the Empowered Community (EC). Set up in the wake of the completion of the IANA stewardship transition, the EC can reject ICANN and IANA budgets, recall directors or the whole Board, and approve bylaw amendments among other things (ICANN 2019).

To summarise, while the Board has a final say on ICANN's decisions, several actors are involved in policy making, whether with an advisory or policy-making role. It must be stressed that advice, while non-binding, carries weight: rejecting GAC advice requires a qualified majority of 60% followed up by a motivation. GAC pressure on the Board has brought about several conundrums, at times followed up by judicial arbitration (Council on Foreign Relations 2017, hereafter CFR).

1.6.2 *Internet Engineering Task Force*

The IETF was founded in 1986 in a rather informal fashion. Currently, it has an administration, and it is part of the Internet Society, with headquarters in Virginia (US) (Camarillo, Livingood 2020). Participation in the IETF is formally on a voluntary basis, but registration fees, travel costs (meetings are held thrice a year in different continents for a week), and the high expertise needed to participate proficiently in working groups make it necessary for most participants to be sponsored. Furthermore, the importance IETF-made standards have for the basic functioning of the Internet makes it a venue that

big technology companies want to have influence in (Belli 2015). Therefore, IETF rules request that participants disclose potential conflicts of interest. For example, IETF policies state that "[i]f you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion" (IETF 2021a).

IETF work is conducted by rough consensus, that is, dissenting opinions are noted but do not constitute veto, whereas significant opposition, albeit small, means consensus on a document has not been reached. IETF work is divided into areas: Application and Real-Time; General; Internet; Operations and Management; Routing; Security; and Transport. Each area has one to three directors and is composed of working groups.

Working groups (WGs) conduct work in face-to-face meetings and remotely through their open mailing list. WGs' work is based on Internet Drafts (IDs) and RFCs. The latter contains anything from research notes to technical standards, while the former is temporary documents constituting informal, openly available but not quotable, informational notes on the work conducted by or proposed to a group on a given specification.

Once a specification is agreed upon and reaches standard status through consensual decision-making, it is listed as 'Internet Standard' on the Official Internet Protocol Standards of the IETF's RFC Editor (RFC Editor 2021). For a specification to become Internet Standard, there is not only a need for consensus in the competent WG, but also a period of trial and general acceptance by the Internet community (Bradner 1996). As worded in RFC 2026, IETF's authoritative RFC for the basic definition of standards and the standard process,

> *"an Internet Standard is a specification that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support, and is recognizably useful in some or all parts of the Internet"* (Bradner 1996, 3).

On a concluding note, it is worth stressing that IETF standards are

voluntary industry standards and have no *de jure* enforceability (Bradner 1996). This also makes it challenging to identify *de facto* Internet standards, as several proposed standards not yet recognised as fully-fledged Internet standards are in fact fully deployed (Harcourt, Christou, Simpson 2020).

1.6.3 *Third Generation Partnership Project*

Finally, 3GPP works differently from the aforementioned bodies. Founded in 1998 to establish the new 3G technology upon initiative of the European Telecommunications Standards Institute (ETSI), the main European telecommunication standards development organisation (SDO), it now involves seven SDOs covering the main economies of Europe, North America, and Asia: ETSI (European Telecommunications Standards Institute, Europe), ATIS (Alliance for Telecommunications Industry Solutions, USA), ARIB (Association of Radio Industries and Businesses, Japan), TTC (Telecommunication Technology Committee, Japan), TTA (Telecommunications Technology Association, South Korea), CCSA (China Communications Standards Association, 中国通信标准化协会, zhongguo tongxin biaojunhua xiehui, China) and TSDSI (Telecommunications Standards Development Society, India). The country or region label simply refers to where the SDO is established, but not necessarily to membership, as in some cases membership is open to any entity operating in the SDOs' territorial scope independently of its country of origin. For example, Huawei is a member of ETSI (European Telecommunications Standards Institute 2020a; hereafter ETSI).

Most SDOs, including ETSI, are public-private in membership (including Board membership) and operate with a mix of private and public funds. For instance, ETSI has been established as a private entity by the European Conference of Postal and Telecommunications Administrations (CEPT) upon input from the European Commission in 1988 (ETSI 2020b). Similarly, CCSA has public-private membership, but works under the supervision of the

Ministry of Industry and Information Technology (MIIT, 工业和信息化部) and the Standardization Administration of China (SAC, 国家标准化管理委员会), respectively, a ministry and a public regulatory authority (China Communications Standards Association 2020; hereafter CCSA).

Procedures in 3GPP work are instead similar to the IETF, in a way. There are three TSGs: Radio Access Network (RAN), Core Technology (CT), and Service and System Aspects (SA). Each of these is subdivided in working groups (WGs). Standards are discussed, elaborated, and approved on the basis of 'absence of significant opposition', a principle similar to the IETF's rough consensus. Conversely to the IETF, participants here need to be affiliated to an entity which is a member of one of the seven SDOs making up the 3GPP (3GPP 2020).

Once specifications for a new generation of mobile connectivity standards (such as 5G) are approved, they need to undergo ITU scrutiny. New generations of mobile Internet standards are elaborated based on guidelines released in advance by the ITU Radiocommunication Sector (ITU-R). International Mobile Telecommunications 2020 (IMT-2020) contains ITU's requirements for 5G specifications, while 4G requirements were contained in IMT-Advanced. The correspondence between generations and the relevant ITU document is not as straightforward, especially as each 'G' label if first and foremost a commercial one. For example, 4G is generally held to encompass three different but related mobile technologies: Long-Term Evolution (LTE), LTE-Advanced, and LTE-Advanced Pro (ITU Development Sector 2021, hereafter ITU-D). What is significant in this section is that specifications are made in accordance with ITU initial requirements, and it is then up to the ITU Radiocommunications Sector (ITU-R) to select the proposed standards that meet requirements and can be recognised as, for example, 5G (Guttman 2018; ITU 2021). After this technical process, the proposed specification is recognised as a recommendation (standard) and formally approved by ITU member states' vote (3GPP 2020).

It is worth recalling that this has juridical implications: being a UN agency, ITU standards (recommendations) can be incorporated in states' law and become standards *de jure*. Furthermore, once a standard is recognised by the ITU, it is recognised as international independently of its geographical spread in terms of implementation. When China deployed a home-grown 3G standard (known as TD-SCDMA) incompatible with those implemented in the EU and the US, the latter claimed at the World Trade Organisation (WTO) that China was setting up technical barriers to trade. However, the case was dropped as deploying an ITU-recognised standard cannot be deemed a barrier, independently of its geographical spread. This is to stress that the ITU recognises as mobile telecommunications standard any set of specification coherent with its initial requirements, independently of the final number of approved standards and independently of their interoperability (Stewart et al. 2011)[6].

1.6.4 *A final remark*

This short outline of ICANN, IETF, and 3GPP functioning is not a complete account. However, it is essential to provide a first glance of how decision-making works and how power can be distributed within each venue.

The private nature of these venues, as well as their complex conformation that allows different actors to interact in different subsections, create channels of influence for a variety of actors whose impact will be explored according to the methods and theoretical approaches illustrated in the next chapter.

[6] At the user level, when China deployed TD-SCDMA, devices produced for the Chinese market would not be able to connect to 3G in Europe and vice-versa. However, the Chinese government allowed the smallest domestic operator, China Unicom, to deploy the 'European' standard. A user with a phone produced for the European market could thus only connect to 3G in China by choosing China Unicom as provider.

1.7 *Conclusion*

Internet governance is a broad field, and its borders are still debated (Hofmann, Katzenback, Gollatz 2017; Mueller, Badiei 2020). The question of states' growing role in Internet governance is one that is gaining centrality in the literature (Haggart, Tusikov, Scholte 2021), with a clearly proactive role having been adopted by states in such fields as data localisation and protection (Liu 2020). However, such dynamics may not be equally spread all over each terrain of Internet governance. Some may display a stronger path dependence and provide an incentive for emerging stakeholders to adapt to the existing normative framework and procedures, while some will see a more widespread attempt to change norms and power distribution among stakeholders.

As the field is broad, this thesis focuses on debates on two tenets of Internet governance on the technical side, namely the making and governance of critical Internet resources and standard-making in mobile Internet connectivity. This research therefore explores Chinese stakeholders' process of contestation, adaptation, and adoption of norms around three relevant venues for the two aforementioned governance subsets: ICANN, IETF, and 3GPP. Observing such venues allows to address normative questions at the core of Internet governance and topics of central geopolitical importance such as the mobile connectivity infrastructure, with implications for the Liberal Order in its free-market tenet.

To do justice to the ambiguities and complexities in the field, this thesis sheds light on the drivers, role, and impact of Chinese stakeholders in and towards Internet governance and standardisation processes within the three aforementioned bodies, contributing to broader debates on multistakeholderism and Internet fragmentation. This is done through a regime-theoretic approach and the use of a combination of computational and qualitative methods as illustrated in Chapter 2. Through these lenses, this work sheds new light on the impact of China's rise on the Liberal International Order.

CHAPTER 2

THEORY AND METHODS

2.1 *One Internet, a multi-layered governance model: norm entrepreneurship in a regime complex*

To recap from Chapter 1, this thesis asks: "*(To what extent) are Chinese stakeholders reshaping the rules of Global Internet Governance?*". In particular: (i) (To what extent) are Chinese stakeholders contributing to increased state influence in multistakeholder fora?; (ii) (how) is China contributing to Internet fragmentation?; and (iii) what are the main drivers of Chinese stakeholders' stances?

A key takeaway from the previous chapter is the multifaceted characterisation of multistakeholder Internet governance as a largely private-based regime complex where multiple actors cast their influence in a variety of loosely interdependent venues with partially overlapping competences (Nye 2014).

This chapter elaborates on the theoretical approach adopted to conduct this thesis. Interactions within the three observed fora (ICANN, IETF, 3GPP) are studied through three methods: expert interviews, thematic document analysis, and network analysis as illustrated in the forthcoming sections.

The next section illustrates the theoretical approach at the basis of this research, while section 2.3 illustrates the 'whats' and 'whys' of the author's methodological choices. Section 2.4 addresses the ethical issues emerged throughout this research and section 2.5 draws the concluding lines of this second chapter.

2.2 *Theoretical choices: Internet governance as a regime complex and the question of digital sovereignty*

As anticipated in Chapter 1, the author conceives the Internet governance ecosystem as a regime complex (Nye 2014). Addressing Internet governance under this lens allows one to make sense of the variety of venues of policy-making influence that can be accessed and leveraged by a multitude of public and private actors in a governance mechanism made of loosely interdependent and partially overlapping fora (Abbott, Faude 2022).

This offers ground for this thesis' contribution to the emerging literature on digital sovereignty. In the ongoing dialectic between different forms of public and private power in Internet governance (Shen 2016; Ten Oever 2021), states are seeking to reassert their authority on the Internet infrastructure and its making (Haggart, Scholte, Tusikov 2021). Nonetheless, regime complexity blurs the lines of national interest and power relations among actors, thus limiting states' options for direct influence in Internet governance.

Digital sovereignty as a concept has experienced growing attention in the wake of the US-China technological competition. Nonetheless, definitions are blurred, ranging from individual empowerment vis-à-vis the collection and treatment of personal data to states' and the EU's quests for reduced dependence on foreign industries in technological innovation (Pohle, Thiel 2020). Owing to the concept's novelty, most literature has focused on the discursive characteristics of digital sovereignty, as practices are yet to emerge (see for example: Tjahja, Nanni, Baiduk 2022).

Despite this, trends in policy practice can be traced. After all, digital sovereignty was introduced *ante litteram* in other political contexts. This includes China, which has officially introduced the concept of 'cyber sovereignty' (网络主权, wangluo zhuquan) in 2010, within the White Paper on the (state of) the Internet in China (中国互联网状况, zhongguo hulianwang zhuangkuang) (Creemers 2020b).

Indeed, the focus on public authorities' enhanced quest for power in

Internet governance is older than the digital sovereignty debate in academic literature. For example, states' turn toward the Internet infrastructure as a place of and tool for political contestation is a relatively long-standing issue (Musiani 2013; 2020). This is not only in terms of standards, but also in terms of architectural deployment: with the DNS4EU initiative, the EU seeks to strengthen its autonomy in and regulatory control on the process of DNS resolution (Huston 2022). However, the EU is not the first public authority to turn towards the DNS in its regulatory effort, as China has established the so-called 'DNS Rules' in 2017 (MIIT 2017). Furthermore, the market-protectionist stances taken by world powers in 5G deployment amid concerns over China's undue influence over dataflows along new telephony infrastructures is also part of this broader trend (Ciuriak 2019; Poggetti 2021).

While such specific instances are better addressed in the empirical part of this thesis, they help to trace a few lines of digital sovereignty practices and how this thesis' focus on infrastructure politics feeds into this emerging literature.

As the literature debates the return of the state in Internet governance, one must bear in mind that states have never left Internet governance in the first place (Ten Oever 2021). For example, the US played a role in establishing and maintaining the Internet and then ICANN (Mueller 2017). Rather, one should look at the debate on digital sovereignty as an attempt from public authorities to expand their share of power in Internet governance vis-à-vis private actors and competing state actors. In the Internet governance regime complex, no single authority is likely to emerge as the one regulator of the Internet, its infrastructures, and the technologies based on it. As anticipated, this is due to the variety of venues for policy influence that regime complexity creates.

Regime complexity is a late development in regime theory, which emerged in the early 1980s with Krasner (1982) as one of its founders. According to him, a regime consists of "principles, norms, rules, and decision making procedures around which actor expectations converge in a given issue area" (Krasner 1982, 185). Criticised and transformed several times (Strange 1982), the concept of regime came to be closely connected to institutional liberalism (Keohane,

Martin 1995). In Krasner's (1982) view, much as for liberal institutionalists (Keohane, Martin 1995), the underpinnings of the international system are those recognised by realists: international anarchy and the incapacity of states to collaborate amid reciprocal mistrust. In this context, regimes are set up by states to create incentives and disincentives that can ensure collaboration on specific issue areas to avoid anarchy's suboptimal outcomes. In game-theoretical terms, suboptimal outcomes are those deriving from such games as the prisoner's dilemma, whereby the individual incentive to defect prevents actors from collaborating and reaching an optimal outcome (Axelrod 1980).

Amid the emergence of constructivist approaches in the 1990s (Wendt 1992), regime theory incorporated a cognitivist approach whereby actors' interests and actions gave form to regimes and regimes shaped and reshaped actors' interests and actions in turn (Jönsson 1993). Other than adding a cognitivist component to the already-existing rational one in regime theory, the 1990s witnessed the systematic incorporation of non-state actors as agents in IR theory (P. M. Haas 1993).

This incorporation opened the door to the concept of regime complexity emerged in the early 2000s. Raustiala and Victor (2004) were the earliest to elaborate this concept, which was later applied to such fields as environmental governance by Keohane and Victor (2011) and Internet governance by Nye (2014). According to Nye (2014), a regime complex is a set of loosely interrelated regime subsets with little or no clear-cut hierarchical relation. Regime complexity is a framework adopted to conceptualise the relations among subsets of Internet governance and among state and non-state actors within them. As for the three bodies addressed in this thesis, participants to one are often unaware of the details of the work conducted in other bodies. However, their activities are interrelated and influence each other's. It is the same in the case of 5G development and TCP/IP: the former is developed at 3GPP and the latter at the IETF, with different groups of people (often) from the same companies working on them. However, 5G enables such technologies (such as IoT devices) as to put in question the efficiency of TCP/IP as a workable set of protocols, triggering debate on the development of additional

and/or alternative ones. Despite this, technological path dependencies in Internet development make TCP/IP difficult to replace and issues related with 5G-enabled IoT persistent. This research assumes a bidirectional relation between the regime complex and actors, whereby the former shapes the latter's interests and behaviour and the latter shapes the former's rules and norms.

This thesis maintains that regime complexes offer several venues for influencing policymaking to a multitude of public and private actors. As anticipated in Chapter 1, this creates a set of opportunities and constraints for state actors. On the one hand, states can cast influence in industry-based decision-making through SOEs or politically controlled private actors. On the other hand, such actors' interests may not be fully overlapping with those of the central government, especially when it comes to private actors, thus blurring the delineation of a clear-cut and coherent 'national interest' – however defined.

The complex interaction of several partially overlapping governance settings yields overlapping and potentially incoherent normative settings (Kettemann 2020). In such context, several public and private actors act as norm entrepreneurs in shaping the norms, rules, and principles of Internet governance, throughout and within the several hundred organisations involved in Internet norm-making (Radu 2019). The role of norm entrepreneurs in IR Theory has been explored at least since the 1990s, with the landmark publication by Finnemore and Sikkink (1998) exploring norms' generation and development until adoption or failure thereof. Within Internet governance, Hurel and Lobato (2018) explored the role of private companies as norm entrepreneurs, focalising on cybersecurity norm-making as an aspect that is traditionally inscribed within states' competence. Radu et al. (2021) coined the term 'normfare' to refer to the effort of norm-creation on a vast scale in which several (types of) actors are engaged in the several layers of the Internet infrastructure and its governance.

While complexity yields a multi-layered normative framework with no clear-cut hierarchy, according to Kettemann (2020), an Internet normative order has taken shape. Such order consists of three layers: international norms, national norms, and transnational norms. Norms can be enshrined in law or be

non-legal. In other words, norms are looked at in terms of functionality rather than legal formality (Forst, Günther 2011). In Kettemann's (2020) definition, norms can be either rules or principles: "rules 'encode' definitive commands (*Rechtsfolgen*), while principles only do so *prima facie*" (Kettemann 2020, 256. Emphasis in the original). While this definition of rules and principles resonates with political science literature, the latter tends to identify norms as a third separate category rather than a collective name for rules and principles. Finnemore and Hollis (2016, 438) define norms as "collective expectations for the proper behavior of actors with a given identity", a definition that identifies four elements for a norm to exist: "(1) identity, (2) behavior, (3) propriety, and (4) collective expectations" (Finnemore, Hollis 2016, 438-439).

Departing from these three definitions of norms, rules, and principles, one can observe that the transnational layer of the Internet's normative order hosts a variety of private-based, non-legal norms that regulate both the process of Internet norm-making itself and its final outcomes. For example, the IETF creates voluntary industry standard with no *de jure* validity, but they bound industry to the adoption of certain protocols and affect users' rights (for example, privacy) and behaviour online. Norms elaborated transnationally are at the core of this thesis, which focuses on multistakeholder, private-based governance. Standardisation processes create influential technical rules, while ICANN bylaws and policies affect the global management of the Internet's critical resources despite coming from a private organisation.

The interaction of public and private norms is a bidirectional one, whereby state-sponsored actors by the rules of private governance, but governments' push to influence (infrastructural) policies limits private actors' actions (Musiani 2020).

To summarise, regime complexes open a variety of venues for a variety of public and private actors to interact and participate in norm-making as norm entrepreneurs (Hurel, Lobato 2018; Radu 2019; Radu et al. 2021). Based on the framework of norm entrepreneurship in regime complexes, the next section of this chapter illustrates the methods selected to conduct such analysis. The mix of computational and qualitative methods selected reflects the need to analyse

this phenomenon at many layers of interaction, coherently with the structure of the Internet governance regime complex. Such characteristics compel one to incorporate the views of those involved first-hand in standardisation and governance activities, especially when they possess such technical expertise whose understanding is beyond that of social sciences. This addresses the structural underrepresentation of such profiles in IR research on the politics of technology (Tanczer, Brass, Carr 2018).

In conclusion, through the regime complexity lens this thesis illustrates how the institutional settings and mechanisms of opportunities and constraints illustrated create venues for Chinese stakeholders' influence, contestation, as well as adaptation to the existing norms and institutions of global Internet governance. This raises two main theoretical expectations that have been anticipated above and will be addressed in the empirical chapters. First, regime complexes blur the lines of national interest as they allow a variety of state and non-state actors to influence policy-making processes through a variety of venues. This reduces a government's capacity to cast control on national actors, despite quests for digital sovereignty, but also increases actors' capacity to contest norms through 'forum-shopping', that is, shifting competences from one forum to another (Hofmann 2019). Second, influence in a regime subset is never completely independent of influence in the other subsets of the same regime complex. Therefore, challenging norms in one subset entails challenging norms in others. This makes norms rigid and creates incentives for norm entrepreneurs to adapt to the existing normativity rather than contesting them.

2.3 *Methodological choices*

On a methodological level, in order to explore China's contribution to the definition of internet governance, two subsets of global Internet governance will be explored: *(i) critical Internet resources (CIRs) governance at ICANN*

and standardisation at the IETF, and *(ii) mobile Internet standard-making at 3GPP*, as recalled in section 2.1. Chinese stakeholders' interactions are observed within each forum and then analysed in conjunction, as regime complexity entails a form of interdependence among them.

This research adopts three different data collection methods: qualitative semi-structured expert interviews, documents analysis, and network analysis through mailing lists interaction. Each method brings information and serves as a control basis for the analysis conducted with other methods.

2.3.1 *Semi-structured expert interviews*

To start with, interviews help to gauge stakeholders' intentions and perceptions, as well as their understandings and interpretations of historical facts. In conjunction with other quantitative and qualitative methods, they can both provide hints at what is deemed politically important in a certain policy realm and serve as corroboration for findings obtained through other methods. To be sure, interviews do not provide a fully systematised interpretation of stakeholders' perceptions, but rather in-depth narratives from key profiles (King, Horrocks, Brooks 2019). Nonetheless, their usefulness remains intact, especially in corroborating other research findings and gauging the views of key persons involved in processes otherwise too technical to be fully interpreted by social science researchers.

Other than playing this role, in this thesis' particular case expert interviews helped to explore the behaviour of Chinese stakeholders as norm entrepreneurs in Internet governance within the theoretical framework illustrated in the previous section of this chapter. During the earlier interviews, this thesis' field of enquiry was fully defined, leading to identify it with the ICANN, IETF and 3GPP policy realms. Furthermore, interviews helped to establish the time references for documents and network analyses. Additionally, since these organisations meet just a few times per year (and in 3GPP's case, the meetings are not public), interviews represent a much more feasible qualitative study methods than others, such as participant observation, which has been

successfully used elsewhere (Cath 2021; Scholte 2017). Finally, when accompanied by the findings derived from the two other methods illustrated below, interviews help to gauge the drivers of Chinese stakeholders' actions and stances in the governance complex.

While it was necessary to carry out the interviews online owing to the Covid-19 pandemic, they proved proficient and were conducted coherently with recent methodological developments on remote interviewing (Gray et al. 2020; Salmons 2015). Building on the two other methods described below, interviews allowed the author to interpret how Chinese stakeholders' stances within the Internet governance regime complex, particularly within the three fora in question, changed in time, differentiating among different stakeholder groups. Collecting first-hand views from Chinese research participants, along with Westerners' perspective on Chinese stances, allowed the author to interpret how Chinese stakeholders' approaches and strategy within and towards the regime complex changed over time. Furthermore, this helped gauge the relationship between Chinese stakeholders and norms within the fora in question, including how these actors adapted and adopted such norms.

Interview questions were elaborated based on four working statements, which were corroborated, confirmed, or disconfirmed through the interview process. Two working statements concern mobile Internet technologies, whereas the third and fourth statements concern CIRs governance: *(i) Chinese-elaborated mobile connectivity standards are competing (i.e. not coexisting) with EU and US ones; (ii) governments and government-controlled actors' influence in global technical standardisation processes has increased and China has contributed to it*; *(iii) China's re-accession to ICANN's GAC has increased governmental influence on IPs and DNS root management;* and *(iv) China's increased participation in the IETF has enhanced the likelihood of separate (i.e. coexisting, not competing) Internet standards being created.*

As per Table 2.1, 'coexisting standard' refers to a specification that is separate from and incompatible with the acknowledged universal one(s), while 'competing standard' refers to one that is aimed at becoming universal, thus not 'coexistent' with a separate, incompatible one.

	Coexisting standards	**Competing standards**
Mobile Connectivity	*Local* deployment; *Incompatibility* with universal specifications. Proponents are *not in competition*, but deploy their standards in different markets.	Aimed at *universal* deployment. A proponent is in *competition* with the proponents of other sets of standards aimed at universal deployment.
	3G standards are different in Europe and China. Devices produced for the European market cannot connect to 3G in China.	With universal 5G standards, devices produced for the European market can connect to 5G in China and vice-versa.
Critical Internet Resources	*Local* deployment; *Incompatibility* with universal standards.	Aimed at *universal* deployment.
	The utilizers of such standards *cannot exchange data* with the utilizers of other standards unless specific gateways are created.	All utilizers can exchange data, unless further technical barriers are set up (e.g., firewalls).

Table 2.1: Mapping and defining coexisting and competing standards.

Legend: 'proponent' refers to developers/supporters of a standard/specification.

The fourth working statement was added when the data generation process had already started to have a supposition that was more strictly focused on

Internet fragmentation.

It must be stressed that the distinction between coexisting and competing standards is somewhat ideal-typical. For example, IP version 4 (IPv4) and IP version 6 (IPv6), the two versions of the Internet Protocol currently in used, are backward-incompatible. However, protocols have been established so that devices using one or the other can communicate seamlessly with each other. Therefore, it cannot be argued that the establishment of IPv6 constitutes Internet fragmentation, although the risk was there potentially (ICANN 2021). This makes the technical fragmentation question increasingly nuanced.

The four working statements illustrated above have been elaborated based on two pieces of secondary empirical data. The first is Chinese companies' leadership position in 5G standardisation, expressed in terms of standard contributions presented by Chinese actors-affiliated experts at 3GPP (Pohlmann, Blind, Hess 2020). In particular, Huawei Technologies emerges as the single most important proponent of 5G standard contributions in absolute quantitative terms by the beginning of 2020 (26,372 by January 2020) – notwithstanding the various ways in which standard contributions can be quantified and qualified (Pohlmann, Blind, Hess 2020, 25-26).

The second piece of empirical evidence is Chinese actors' relative growth in contribution to the IETF's activity. The number of Chinese authors contributing to RFCs and Internet Drafts sharply increased between 2007 and 2010, then remaining relatively steady at 2010 levels thereafter. Furthermore, Huawei is on aggregate the second most important actor in terms of 'active authors' (around 157), slightly behind the US company Cisco (179), in the IETF by 2020 (IETF 2021b). These two companies hold the same position when looking at RFCs (co)published by their affiliates (Arkko 2021).

The key informants participating in interviews are twenty-nine Chinese and non-Chinese (mostly Western) representatives of six Internet stakeholder communities: governments, international organisations, multinational enterprises, civil society, technical communities, and academia[7]. This

[7] More information in Appendix A and Appendix B.

categorisation is drawn from DiploFoundation (2015) and adds ‘academia’ to the five stakeholder groups often found in ICANN, Internet Society (ISOC), and UN institutional documents (UN Educational, Scientific and Cultural Organisation 2019, hereafter UNESCO), as academics do not easily fit the other categories unless they carry governmental or business roles or hold strictly technical competences.

To be sure, many taxonomies can be found in Internet governance literature (Raymond, DeNardis 2015; NetMundial 2014; WGIG 2005). Each one has undergone criticism from other literature sectors as categories of stakeholders were excluded or overlapped conceptually. For example, it is challenging to distinguish between the technical community and multinational enterprises when around 80% of the technologists participating in the Internet Engineering Task Force are employed by corporations (Belli 2015). The global multistakeholder event held by the Brazilian government in the wake of the PRISM scandal, NetMundial (2014), proposed a six-fold distinction among stakeholders: governments, the private sector, civil society, the technical community, the academic community, and users. While possibly more encompassing, this definition does not avoid conceptual overlapping since ‘users’ could arguably fall under the category ‘civil society’ – after all, the latter’s purpose is to represent citizens (Belli 2015). The UN-sponsored Working Group on Internet Governance’s 2005 definition enshrined in the Tunis Agenda provides instead a threefold distinction among stakeholders: governments; the private sector; and civil society. This categorisation, while parsimonious, leaves out academia and the members of the technical community not affiliated to any of the three categories.

The six-fold categorisation adopted in this thesis is chosen as a good compromise between inclusiveness and parsimony.

As for the involvement of mostly Western (that is, mainly from the EU and the US) non-Chinese stakeholders, it is due to the fact that the main non-Chinese actors involved in the processes under analysis are Western (Cisco, Nokia, Ericsson, and the US government among others). Interviewing non-Chinese participants helped the author to gauge their views on Chinese actors’

behaviour, stance, and policies. Interviews with Western participants were insightful as they held views on how they saw Chinese stakeholders entering into governance and standardisation venues and carry their weight in them. This way, interviews with Chinese and non-Chinese, as well as interviews with exponents of different stakeholder groups, corroborated each other. The possibility to include actors from other national/regional backgrounds systematically in the analysis to address, for instance, China's relations to Latin American and African governments and stakeholders exists and would open the way to important analytical aspects, such as the role of China's relations to developing countries within its broader foreign and digital-infrastructural policies. Nonetheless, it also risked expanding the scope of this research project beyond feasibility. It goes without saying that key informants from other geographical areas of the world have been involved when their expert position was deemed relevant within the scope and objectives of this research project.

The software QDA Miner is used to qualitatively analyse interviews. Interview texts are coded thematically through concepts found in literature: Internet fragmentation, competing/coexisting standards, and normative change are the three crosscutting topics.

2.3.2 *Thematic document analysis*

As for the second methodological approach, analysing documents allows researchers to interpret the outputs of decision-making processes and thus the influence of specific (networks of) stakeholders. In terms of norm entrepreneurship, this method helps gauge the efficacy and effectiveness of Chinese stakeholders' effort in policy- and norm-making within the analysed subsets of the Internet governance regime complex.

In this research's case, analysis has been conducted on selected documents of selected working groups within the three fora in question. As such working groups can produce several tens of documents per year, selected time references were identified as illustrated in the following section.

The analysed documents contain specifications for selected releases (standards) of 3GPP[8]; RFCs for the IETF; and bylaws and GAC minutes and meeting transcripts for ICANN.

MaxQDA is used for qualitative document analysis. Each document is coded according to four themes derived from literature (influence, fragmentation, competing standards, and East-West geopolitical divide are some of the crosscutting topics). Section 2.3.6 will illustrate the selected timespans and the targeted documents.

Through qualitative thematic document analysis, the author observes the policy impact of Chinese stakeholders in the selected multistakeholder governance fora. Document analysis provides good corroboration to interview findings, as one can observe whether interview participants' impressions and views correspond to policy outputs. Furthermore, it supports and corroborates the findings of the network analysis illustrated in the next subsection, as bodies such as GAC have closed mailing list but publicly accessible minutes and communiques.

2.3.3 *Network analysis*

Finally, this research relies on e-mail exchange-based network analysis. Network analysis contributes to clarifying some aspects related to relations of power, influence, control and/or dialectic existing between actors (Shen 2016; Wen 2020). Per se, network analysis comes attached to neither a theory nor an interpretive framework. However, it serves as an exploratory tool to map relations among nodes (individual or collective actors), their strengths, and their leadership ties (Marin, Wellman 2010). Within the theoretical framework illustrated in section 2.2, this method allows to map which Chinese actors are involved in norm-making and where, gauging their influence through centrality

[8] Releases undergo several steps of re-elaboration and transformation, which complicates the retrieval of information. When reference to the content of a release is made, it points to its related specifications, a term that refers to both Technical Reports (TRs) and Technical Specifications (TSs) as defined by 3GPP in TR21.900 (3GPP 2021c).

measures.

While network analysis can be conducted using many tools, mailing lists were chosen as they have been the main means of communication in standard development organisations (SDOs) and Internet governance bodies since the early days of the Internet. This allows researchers to potentially have a view of informal, yet work-related, exchanges among technologists and other participants at virtually any point in Internet history. Furthermore, with every working group within a SDO and every ICANN support organisation and advisory committee possessing their own mailing list(s), researchers can focus on the dynamics of specific groups and subtopics. Despite this potential, mailing lists are an understudied source of knowledge in Internet governance (Ten Oever, Milan, Beraldo 2020), which makes mail exchange-based network analysis an enticing venue for scholarly analysis.

Therefore, this method allowed the author to reconstruct connections between and among individuals and stakeholder groups within the three aforementioned bodies. Analysis was conducted through Bigbang[9], an open-source Python-based software for mailing list analysis specifically oriented to the study of Internet governance bodies. In general, Bigbang was conceived for studying open collaborative communities. The software contains scripts allowing automatised collection of mail text from public Mailman and Listserv archives. Within this research, mail exchange-based network analysis helped to interpret the extent and type of relations among actors and stakeholder groups. In particular, a contentious aspect of Chinese stakeholders' activity is the unknowns around their relation to the Chinese government (Pupillo 2019). While qualifying the ties between the Chinese government and its domestic companies is unfeasible, the quality of the relations among the latter and between them and third-country companies helped to gauge the extent to which they are allowed autonomous business action (Shen 2016; Wen 2020), an aspect further corroborated through interviews.

[9] Bigbang code retrieved from: https://github.com/datactive/bigbang (October 20, 2021).

The networks analysed in this thesis are defined on a position and relation basis (Marin, Wellman 2010). A position-based approach to networks considers members of a network all those actors who hold a formally defined position. In this sense, for example, all Huawei employees at 3GPP can be considered a network and so can all the members of a working group. However, relations within these bodies are also informal and cross-company. Observing such relations helps to make sense of the dialectic among Chinese stakeholders and between these and other stakeholder groups. In observing networks so defined, this research adopts a structuralist approach to network analysis, that is, an approach "concerned with how patterns of relations can shed light on substantive topics within […] disciplines" (Marin, Wellman 2010).

In this research, nodes are individuals who participate in ICANN, IETF or 3GPP. By computing eigenvector centrality and PageRank for every one of them, along with the quantity of emails sent and received, one can gauge their importance in the network(s). Both eigenvector centrality and PageRank aim to show which node plays a stronger leadership role within a network. However, the two can give slightly different results. Therefore, both are calculated to try and reduce potential biases embedded in one measure or the other. To complete this passage, this thesis used Gephi[10], an open-source software through which Bigbang-based network analysis can be represented graphically and statistics can be computed on the dataset.

Moving forward, it must be stressed that each individual (node) in question is affiliated to an organisation (most often a company). In such fora as the IETF, where activities are only nominally conducted on a personal capacity, one needs to gauge patterns of corporate engagement. Therefore, intra-mailing list domain entropy analyses provide a graphical hint to whether companies have a corporate strategy within a body and how it is deployed. For example, mail addresses with corporate domains (for example, 'cisco.com' and 'huawei.com') may have similar entropy degrees and their distribution within a working group

[10] Gephi code retrieved from: https://github.com/gephi/gephi (October 20, 2021).

or sub-body can suggest a certain kind of corporate strategy (Benthall 2021)[11]. This analysis is also conducted with Bigbang.

Network analysis, accompanied by intra-domain entropy analysis when relevant, is applied in this research as it seeks to gauge the extent and patterns of engagement of Chinese stakeholders with other actors within the given forum.

Entropy is a coefficient that measures the difference in engagement (that is, number of emails sent in a mailing list per individual) among individuals with the same domain, or in other words, affiliated to the same company. This helps the researcher to gauge the extent of Chinese corporate actors' engagement in the analysed bodies and observe whether and how their patterns of engagement differ from those of Western companies' affiliates. Along with the other methods illustrated, this allows the observation of the extent of Chinese stakeholders' integration in and adaptation or contestation to the normative settings of multistakeholder Internet governance.

While this is an unnecessary step in smaller working groups, it proves useful in IETF working groups where several individuals from the same corporate actor or organisation participate in the same working group in different ways.

A final disclaimer needs to be made for 3GPP. Networks in IETF and ICANN working groups are built around email senders and receivers. However, in 3GPP senders put themselves as receivers along with the general mail address of the group as a praxis. This impedes the application of the same criterion used for the IETF and ICANN in building a network. Therefore, entropy analysis and email distribution analysis will be used to gauge the same kind of exploratory information.

To summarise, a mix of entropy analysis and network analysis is adopted

[11] In this chapter, the words 'subgroup' or sub-body' should be conceived as an informal term to encompass all the organisational structures within a broader entity. For instance, it can be used to indicate the ensemble of ICANN support organisations, advisory committees and other panels and groups.

to study individual- and corporate-level interaction among Chinese stakeholders and between these and stakeholder from other countries. Through these analytical tools, in conjunction with the two qualitative methods illustrated in the previous subsections and summarised in Table 2.2, this research observes Chinese stakeholders' adaptation to and acceptance of multistakeholder normative settings.

Methods	**Research Objectives**	**Theoretical implications**
Semi-structured expert interviews	Gauging stakeholders' views, interests, and drivers.	Norm entrepreneurs' behaviour in the regime complex.
Thematic document analysis	Observing Chinese actors' impact in policy and standardisation.	Effectiveness of norm entrepreneurship.
Network analysis (and domain entropy analysis)	Gauge patterns of engagement among Chinese stakeholders and with other actors.	Norm entrepreneurs' centrality and influence in the complex.

Table 2.2: A summary of this thesis' research methods and their objectives.

2.3.4 *Building the sample of interview participants*

To summarise, the three data gathering methods illustrated in this section allow a threefold analysis of Chinese stakeholders' stance in Internet governance: their interests and drivers; their actions and strength through time within the selected fora; and their influence and impact in such fora's work. This happens through a constant interaction of the three methods: interviews findings influence and help the interpretation of document contents and vice-versa, with network analysis providing a formalised, quantitative corroboration to statements emerging from interviews.

Furthermore, each method helps to address the others' shortcomings. For example, interviews and mail exchanges in open mailing lists can feature different types of social desirability bias, potentially leaving contentious issues for discussion in more private contexts.

As analysable documents, mail exchanges, and working outputs are numerous, the author was compelled to select significant documents in given timespans for feasible analysis: analysis on 3GPP, ICANN and the IETF spans decades and therefore needs to be trimmed down to a few nodal points in history. Different criteria have been applied in identifying time references and target groups for the three data collection and analysis methods illustrated above and summarised in Table 2.2. However, the overall timespan ranges from 1998 up to the time of writing for each of them, being the founding year for both ICANN and 3GPP. These aspects are illustrated below in this chapter. Furthermore, different criteria have been adopted to sample interview participants within the six stakeholder groups identified above.

To begin with, interview participants have been selected through purposive sampling. Every participant was first contacted by email. Earliest contacts were made through senior members of the Department to which the author is affiliated, then each interview was concluded with a request for contacts with persons in key positions. Such contacts were either colleagues in the same organisation or structure as the research participants or representatives of other stakeholder groups with whom the participant was acquainted through their common activity at ICANN, the IETF or 3GPP. Chinese and Western participants were interviewed for every stakeholder group (governments, international organisations, tech companies, civil society, academia, technical communities), with the sole exceptions of governments and civil society. Only representatives of Western stakeholders could be involved from these groups, despite several attempts, arguably due to the autocratic nature of the Chinese governments and the sensitivity of the issues at stake.

Government participants were familiar with either the GAC or Internet Governance Forum (IGF) processes, as public authorities are not represented in IETF and 3GPP. However, their familiarity with these bodies was investigated.

Among academics, senior figures (assistant professors and professors) were interviewed, all of which were Internet governance experts and/or participants. For all other stakeholder groups, professional profiles engaged first-hand in ICANN, IETF or 3GPP were selected. A strong emphasis was given to technologists' views, as they are underrepresented in IR literature but possess a privileged expert view on the politics of technical governance (Tanczer, Brass, Carr 2018). In ICANN's case, Western and Chinese members of staff were also interviewed. Once again, it must be stressed that the stakeholder group categorisation is ideal-typical, and most interview participants fit more than one stakeholder group.

All interviews took place between mid-March 2020 and February 2021.

2.3.5 *Document analysis and network analysis: defining the targets*

Owing to the vast array of work conducted by ICANN, IETF and 3GPP, selected working groups or sub-bodies were targeted for network and document analyses.

For ICANN, the focus was on the Governmental Advisory Committee (GAC), the Country-Code Name Supporting Organisation (ccNSO), and the Generic Name Supporting Organisations (GNSO). These bodies allow one to see both the government and those private actors managing country-code (such as '.cn') and generic (such as '.com') Top-Level Domains (TLDs) in action. Nonetheless, the main obstacle met with ICANN is that many of its mailing lists are not freely accessible. To proficiently conduct mail exchange-based network analysis at ICANN, three open subgroups were identified: Chinese Generation Panel (chinesegp), GNSO's New gTLD Subsequent Procedure Working Group (gnso-newgtld-wg), and IANA Issues (ianaissues).

Chinesegp deals with Internationalised Domain Names (IDNs). These are domain names in non-ASCII (that is, non-Romanised) characters, which include Chinese characters, a topic on which Chinese effort has been strong since inception (Zhang 2019). These lay at the basis for the development of Chinese-character domain names, which are an important financial matter for

Chinese stakeholders in this field. Chinesegp engages in IDN-related work, which is the reason that it has been incorporated in the analysis. More precisely, Generation Panels participate in the "Procedure to Develop and Maintain the Label Generation Rules for the Root Zone in Respect of Internationalized Domain Names in Applications (IDNA) Labels" (ICANN 2021). This is a two-step process:

> *"[t]he first pass creates a set of label generation rules specific to a given script, writing system, language, or all of these; […] [t]he second pass is to review the proposal by the Generation Panels by the Integration Panel, which comprises of experts in the fields of Linguistics, Unicode, Domain Name System and the IDNs"* (ICANN 2021).

More specifically in this context, "Each generation panel works on a subset of Unicode relevant to one writing system or a set of related writing systems" (ICANN 2013).

Moving forward, the GNSO's New gTLD Subsequent Procedure Working Group was chartered by the GNSO Council to conduct a Policy Development Process (PDP) following the 2012 launch of new gTLDs (Barbaras 2020).

Finally, IANA Issues was an At-Large, that is, users' working group set up by the At-Large Advisory Committee (ALAC) of ICANN.

In summary, covering chinesegp, gnso-newgtld-wg, and ianaissues helps one to observe Chinese engagement at the civil society (users), private (GNSO), and state (chinesegp) level. While pure governmental engagement is only visible through GAC, whose mailing list is closed, chinesegp feature a prominent participation by affiliates to the state-sponsored China Internet Network Information Centre (CNNIC), manager of the '.cn' ccTLD. Furthermore, the selected groups allow researchers to observe Chinese engagement in SOs (that is, policy-making organisations) and ACs (purely advisory).

For the IETF, the focus is on three working groups (WGs): Inter-Domain Routing (idr); IPv6 maintenance (6man, which de facto took over the work conducted by the ipv6 WG); and Application-Layer Traffic Optimization (alto).

These three groups were selected as they fit into three different areas of the IETF's work: routing (rtg), Internet (int), and transport (tsv).

Finally, within 3GPP, analysis was conducted on Core Network and Terminals WG 1 (CT1), Radio Access Network WG 5's (RAN5) mailing list on New Radio (NR) work, and Service and System Aspects WG 3 (SA3) working on architecture security. As mentioned, network analysis is replaced here by observations on intra-domain entropy and email distributions.

The first selected 3GPP working group is the one currently elaborating the main specifications for the 5G core network, while the second one elaborates 5G's radio specifications. The third group works on the politically sensitive matter of architecture security. While core network-related issues are more geopolitically loaded, it is radio accessibility that affects devices' technical characteristics and therefore the final market, which is why participants in RAN working groups are significantly more numerous than in CT ones (3GPP 2020). While for ICANN choices were constrained by the public availability of mailing lists' text, in the case of 3GPP, technical constraints arose during mailing list scraping. Some mailing lists, such as that of Radio Access Network WG 1 (RAN1), can feature up to almost 200 thousand emails, which makes it difficult for the scraping to succeed. Nonetheless, the email exchanges of relevant working groups for this thesis' analysis were successfully obtained.

2.3.6 *Selected timespans for document analysis and network analysis*

As mentioned, selected historical turning points were also identified for mailing list and document analysis. First, the end of the IANA stewardship transition in 2016 was identified as a key moment for ICANN. The transition, ending the US's contentious supervision of the IANA functions, triggered reforms of ICANN's bylaws. Observing whether Chinese stakeholders had an influence on the 2016 text of the bylaws and in GAC bylaws in the three meetings (one year) preceding the end of the transition helps to gauge their normative influence on critical Internet resources governance. Coherently, network analysis is conducted on emails exchanged in the aforementioned

ICANN subgroups in 2016.

Second, the beginning of Chinese company-affiliated authors' participation to IETF work (2007) and the freezing of the first 5G specification (Release 15, mid-2019) were identified as key moments for the IETF. While the IETF is not competent for 5G standardisation, the latter has implications for the efficiency and maintenance of the Internet's basic protocols. As Huawei is the main Chinese actor in both the IETF and 5G standardisation at 3GPP (Arkko 2021; Pohlmann et al. 2020), a common interest at the basis of its activities can be assumed. Furthermore, 2007 and 2008 are key years in the roll out of IPv6: the closure of the ipv6 WG in June 2007 (IETF 2021c), de facto taken over by 6man as mentioned above, signalled an up-step in IPv6 implementation following the end of its standardisation process (ICANN 2021). For these many reasons, mail interactions and RFCs presented throughout the years in question (June 2007 to June 2008; June 2018 to June 2019) are analysed.

Applying the same criterion of relevance, the freezing of Release 15 in mid-2019 was identified as a key moment in 3GPP's history, preceded by the freezing of Release 8 on 3G Long-Term Evolution (LTE) (that is, the first 4G-related specification) in March 2009. The text of the two Releases is thematically analysed and email exchanges in the aforementioned 3GPP working groups are observed.

To be sure, further elements could be added: for instance, the contents of Releases 15, 16 and 17 could be analysed to have a full panoramic of 5G development. However, that would broaden the scope of this research beyond feasibility. Furthermore, the technical nature of standards and technical documents (IETF's RFCs and 3GPP's Releases) makes them often unintelligible to non-technical readers. Alternative ways to study actors' impact on policy and technical outputs were considered. For instance, output documents of the Internet Governance Forum could prove useful to reconstruct the public position taken by Chinese actors and stakeholder groups. However, given the authoritarian characteristics of the Chinese government, public documents from policy fora may not reveal deeper aspects of Chinese stakeholders' stance on specific topics. While this may also hold true for the

aforementioned documents and mailing list exchanges, the deeply technical nature of standards makes them less exposed to public scrutiny and therefore more likely to show dynamics and dialectics in Chinese public and private actors' relations.

2.4 *Ethical issues*

Ethical issues arose when conducting interviews and network analysis. In interviews, questions of anonymity were addressed by not naming any participant in the text and agreeing on an ad hoc basis what to quote and how. An exception was made for one interview participant who explicitly requested being quoted by full name owing to his public role at the time of the events under analysis.

Having interviewed people from both the West and China, different degrees of sensitivity arose when asking the same questions, as some respondents are nationals of democratic states while others are autocratic.

Throughout the interview process, it was generally easier for the author to access Western stakeholders for interviews than their Chinese counterparts. Arguably, this is due to the autocratic characteristics of the Chinese government, but also to matters of positionality. As the inquirer is a white European in a moment of strong East-West geopolitical divide on the subject matter in question, subconscious assumptions on the interviewer's position may have emerged, thus forcing the author to make extra effort in building rapport with interview participants. This also connects to matters of 'digital orientalism' (Mayer 2020), which is the tendency of Western observers to see China's cybersphere and digital policies in direct counter-position to an ideal view of what Western liberal cybersphere and digital policies (should) look like. Such bias may have subconsciously been perpetuated by the author when building rapport to interview participants.

Further ethical issues are present in network analysis. While the mailing

lists analysed are fully public, and display email texts and the sender's details, ethical considerations arise when conjectures are made on individuals' interactions (Ten Oever, Milan, Beraldo 2020). While full anonymity cannot be granted, the author seeks to minimise the use of persons' names, unless reference is made to people in key formal positions (for example, working group chairs). Persons' names are never displayed on graphs and tables. While this limits the descriptiveness of graphs, full details of the data collection and analysis process is provided so that the same analysis can be replicated and validated by others in the research community.

2.5 *Conclusions*

Within feasibility constraints and ethical boundaries, the threefold data gathering and analysis methodology illustrated above allows data crosschecking and a reconstruction of Chinese stakeholders' relations, intentions, and normative/policy influence, leaving space for interpreting the reasons behind their actions.

The forthcoming chapters dive deeper into Chinese stakeholders' interaction with and within ICANN, the IETF, and 3GPP, with a look at the state-to-state, business-to-business, state-to-business, down to the individual levels of interaction. This process sheds new light on Chinese stakeholders' influence, contestation, and adaptation to the norms and institutions of global Internet governance, with analytical implications for the future of the Liberal International Order in the wake of China's rise.

CHAPTER 3

EXPLORING CHINESE ENGAGEMENT IN ICANN, IETF, AND 3GPP. A NETWORK ANALYSIS

3.1. *Introduction*

Based on the theoretical and methodological frameworks described in chapters 1 and 2, this chapter maps Chinese stakeholders' engagement in different working groups of ICANN, IETF, and 3GPP at different stages in time.

The observations illustrated in this chapter are obtained through network analysis based on mailing list exchanges within the timespans illustrated in Chapter 2. An analysis of email entropy and distribution is added for the IETF given the size of the network, while for 3GPP such type of analysis replaces network analysis given the impossibility to build a network with the same criteria, as described in more breadth in Chapter 2. The tool used for analysis is Bigbang, developed by Benthall et al. (2021).

As mentioned in Chapter 1, Chinese stakeholders have grown in engagement in 3GPP and the IETF, while ICANN is more ambiguous to quantify. Huawei is the single most important corporate contributor to 5G standardisation in terms of standard contributions (Pohlmann, Blind, Hess 2020), but before reaching this leadership position China promoted and deployed a non-interoperable nationally-developed 3G standard and had lower participation in 3GPP. In the IETF, Huawei is currently the second main contributor in terms of RFCs yearly published by its affiliates (Arkko 2021), while Chinese acceptance of ICANN seems to be growing amid a strengthened role in the ITU (Negro 2020).

The policy change that brought Chinese stakeholders to engage more deeply in mobile Internet to influence the global standard is often seen as one that derives from domestic economic transformation, changes in political views

and economic strategies, changing global economic environment, as well as changes in tech companies' own strategic thinking and market positioning (Shen 2016). Zhou (2019) summarises this process as '3G chasing, 4G synchronism, 5G leadership'[1]. The whys and wherefores of China's domestic changes are outside the scope of this research. However, country-systemic elements have been born in mind all throughout the analysis and will be constantly looked at, as they influence a country's and its domestic actors' stance internationally.

Observing corporate affiliates' individual-level interactions within organisation-based networks allows one to look at how key economic actors with political salience, such as Huawei, interact within the observed organisations: ICANN, IETF, and 3GPP. Observing their numerical growth in time and their centrality in the networks (that is, their capacity to influence decision-making) provides a basis for the forthcoming chapters to qualitatively observe Chinese stakeholders' drivers and impact in the fields of standardisation and CIRs management, and the consequences of their stances and actions on Internet fragmentation and multistakeholderism.

This chapter observes Chinese stakeholders' engagement in key venues at key times as illustrated in Chapter 1. Section 3.2 observes networks and actors' patterns of engagement in the IETF. Section 3.3 does the same for ICANN. In section 3.4, patterns of engagement at 3GPP are observed based on email distribution and domain entropies. Finally, section 3.5 draws conclusions.

3.2 *Networks in the IETF*

Recalling from Chapter 2, time references for idr and 6man are mid-2007 to mid-2008 and mid-2018 to mid-2019. For alto, time references are November 2008 to November 2009, mid-2018 to mid-2019, and January to

[1] In Chinese: '3G追赶, 4G同步, 5G引领' (3G zhuigan, 4G tongbu, 5G yinling).

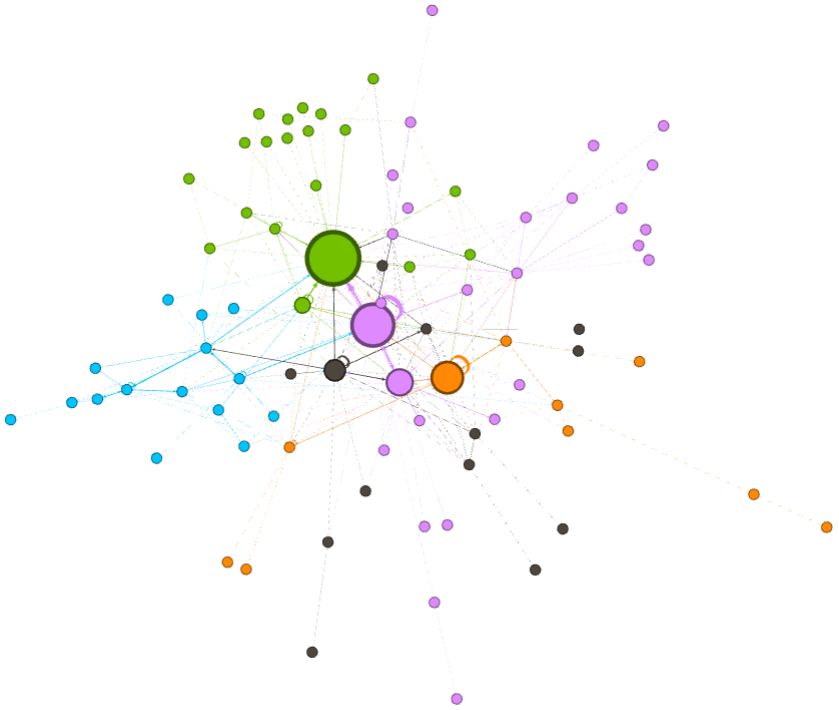
December 2020. This is due to the different patterns of engagement in this working group illustrated below.

The IETF is at the core of Internet standardisation, as the essential protocols for the Internet infrastructure to function (including TCP/IP) are elaborated here. Observing Chinese stakeholders' interactions in the IETF allows one to gauge their influence in Internet standard-making and the extent to which they have adapted to or challenged the existing normative ecosystem of the IETF and Internet standardisation more in general.

3.2.1 *Inter-domain Routing (idr)*

To start with, Graph 3.1 illustrates network connections in idr from mid-2007 to mid-2008. Nodes of the same colour belong to the same intra-network community, as detected through Blondel et al.'s (2008) modularity algorithm. It must be stressed at once that the heaviest edge in the network (weight: 10.0) connects the most central node (green) with the second most central one in terms of eigenvector centrality (pink), despite belonging to different intra-network communities. This is to clarify that such communities are not closed ensembles, but rather groups of individuals that tend to communicate with each other more often than with others.

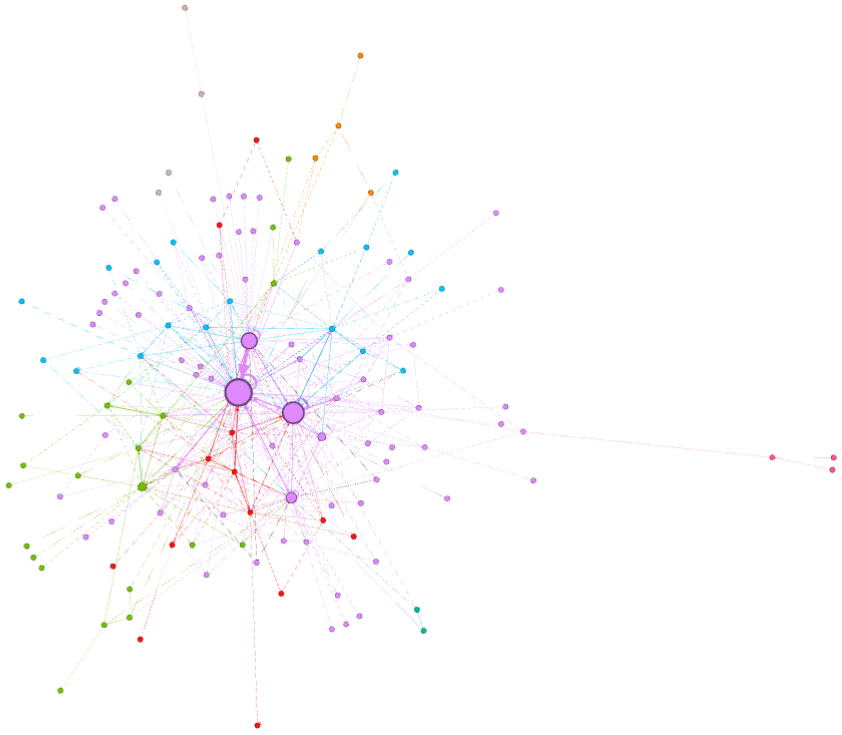
The biggest and most central node (in green) of Graph 3.1 features the highest eigenvector centrality (EC: 1.0). It is connected to other major nodes, bigger in size, each belonging to a different module with the sole exception of two pink nodes. None of these worked for Chinese companies, only Western ones such as Juniper feature among the most central nodes. The PageRank algorithm does not provide a significantly different outcome. Despite belonging to different communities, one can quickly observe that the most central nodes in Graph 3.1 do maintain contacts amongst themselves.



Graph 3.1: idr networks. 2007-2008 (Nodes: 102; Edges: 269)

By mid-2019, idr's internal network distribution changed (Graph 3.2). First, one can observe growth in number of nodes and edges. Second, there is a visibly bigger community (pink) encompassing all the most central nodes and 46.5% of the working group's members. The distribution of central positions in the networks changed from 2008 to 2019. The most central nodes in Graph 3.2 are affiliated to Cisco and Huawei, with the single most central node in terms of eigenvector centrality being a Huawei-affiliated consultant (EC: 1.0). This same person is chair of idr at the time of writing (IETF 2021c). Here, once again, PageRank shows an only slightly different centrality structure, but the aforementioned nodes remain the most central. As Arkko (2021) shows, Huawei and Cisco have been the two most active corporate actors in the IETF in the last five years (2015-2020) in terms of Request for Comments (RFCs) published yearly by their affiliates. While quantity is no guarantee of success in the IETF's consensus-based decision-making process, it shows activism from part of a corporate actor.

A peculiar aspect of the network shown in Graph 3.2 is a concentration of Chinese companies' affiliates in one specific community (blue). Several Huawei and Futurewei affiliates feature here, along with affiliates from China Mobile and China Telecom. Given the low-scale participation of the two latter state-owned Internet service providers (ISPs) to the IETF, this connection is telling considering Huawei's role as China's main network and equipment manufacturer. Nonetheless, it must be stressed that this community features members from major non-Chinese companies such as Nokia and, once again, inter-community edges exist within the network.



Graph 3.2: idr networks. 2018-2019 (Nodes: 155; Edges: 472)

To summarise, idr has seen a shift in leadership, with affiliates of the IETF's two most active corporate actors, Huawei and Cisco, taking the lead. Juniper, which is among the top-five RFC contributors for 2020 (Arkko 2021), does not feature its affiliates in idr's most prominent positions in the network.

To ensure that these figures do not simply stem from few individuals' over-

the-average engagement, domain entropy analysis has been conducted on idr email exchanges (Table 3.1). Entropy measures how dissimilar engagement in each email list is for persons with the same email domain. In other words, entropy is a tool to observe if people with the same corporate affiliation engage the same way in a working group and if the email distribution indicates a strategic pattern in a company's engagement in the working group's activities (Benthall 2021).

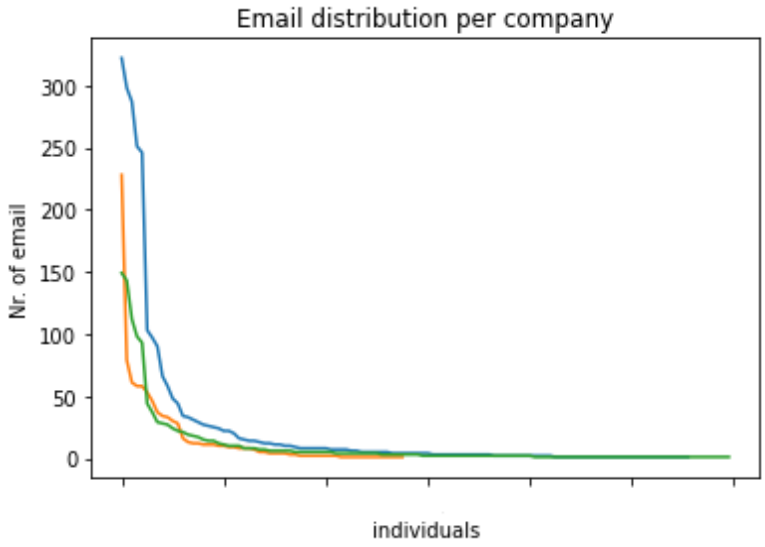
```
domain_entropies.head(20)
```

gmail.com	3.578256
cisco.com	3.307083
huawei.com	3.041566
yahoo.com	2.567374
chinatelecom.cn	2.294408
nokia.com	2.172640
msn.com	2.080648
alcatel-lucent.com	2.025163
hotmail.com	1.982090
netscape.net	1.889159
juniper.net	1.839273
tiscali.co.uk	1.747868
microsoft.com	1.667462
outlook.com	1.550846
ietf.org	1.480564
zte.com.cn	1.433495

Table 3.1: idr - domain entropy

Intra-domain entropies are calculated on the whole of the available mails for the selected mailing list (up to April 2021). Surprisingly, Table 3.1 shows that 'cisco.com' and 'huawei.com' have higher entropy than non-corporate domains like 'hotmail.com'. This is counterintuitive, as one expects corporate domains to be attributed to individuals with a common corporate strategy (Benthall 2021).

Despite this, the graphical distributions of 'huawei.com' and 'cisco.com' emails represented in Graph 3.3 are telling. The Y axis shows the number of emails sent, while every point on the X axis is an individual.



Graph 3.3: idr email distribution - mails sent per individual affiliate.

Legend. Blue: cisco.com; orange: huawei.com; green: gmail.com.

Graph 3.3 shows that one Huawei (orange line) individual is significantly more active than their colleagues in the mailing list (with over 200 emails). However, a few other Huawei affiliates participating in the mailing list are active and are graphically represented by the space under the curve between the initial spike and the long tail.

Two important limiting factors must be re-stressed: first, individuals participating with non-corporate emails do not feature in entropy analysis for a corporate domain. Second, networks represented in Graphs 3.1 and 3.2 are time-bound, whereas mail distributions in Graph 3.3 are longitudinal. This makes direct comparison unfeasible.

Moving forward, we can observe a slightly different pattern for Cisco in Graph 3.3, where the curve declines less steeply and there is no one single individual significantly more active than others. Five individuals feature in the range above the 200-emails quota. In comparison to Huawei's email distribution, it must be noted that Cisco's is on a higher scale.

Furthermore, not only is 'huawei.com' distribution different from 'cisco.com', but also from 'gmail.com' (Graph 3.3). Observing email distribution from 'gmail.com' is interesting because its users do not have

affiliations in common and may display any degree of engagement in the working group. This makes its distribution the closest to random (Benthall 2021). The different patterns displayed in Graph 3.3 suggest, unsurprisingly, that Huawei affiliates coordinate among themselves, that is, they have corporate engagement patterns. The same reasoning applies to Cisco.

In summary, Huawei gained influence in idr: a Huawei-affiliated consultant was holding a central role in idr by 2019, while the working group was strongly US-dominated by mid-2008, and one can see this being accompanied by a pattern of corporate engagement in the group's work. Higher engagement means higher interaction with competitors, too, with contacts among leading Huawei- and Cisco-affiliates being constant as per Graph 3.2.

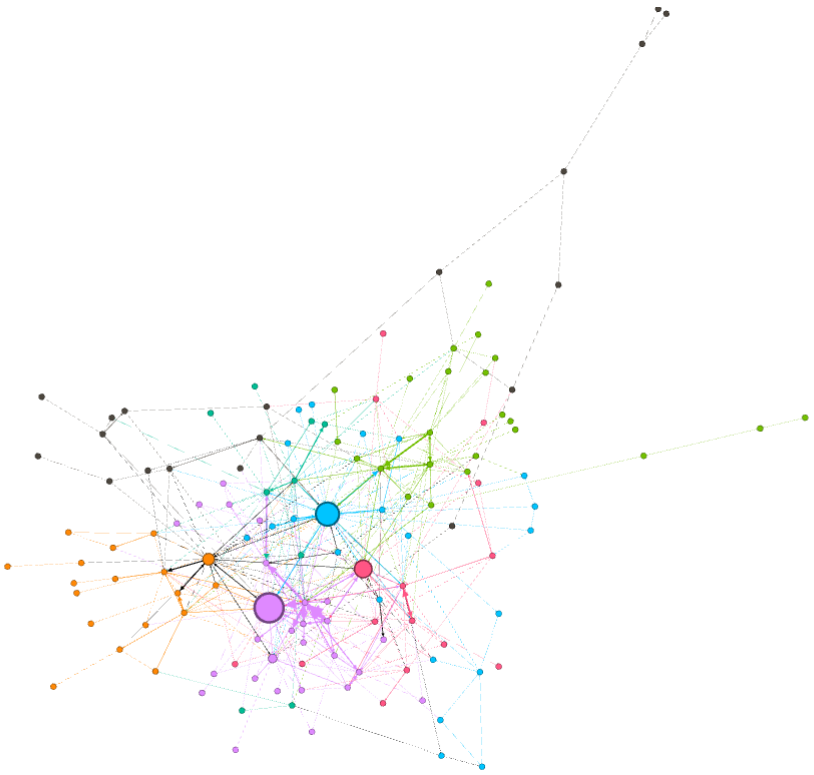
3.2.2 *IPv6 Maintenance (ipv6/6man)*

The second IETF WG under analysis in this chapter is IPv6 Maintenance (6man). This group has taken over work from the ipv6 WG, which was in charge for developing and standardising IPv6. Therefore, the denominations '6man' and 'ipv6' might be used interchangeably. 'IPv6' stands for Internet Protocol version 6, currently the newest version of the Internet Protocol in use (IETF 2021c).

First, the 6man mailing list (Graph 3.4) was more 'crowded' between 2007 and 2008 than the idr one in the same period (Graph 3.1). Arguably, this is due to the up-step in IPv6 development and implementation experienced in those years, amid the exhaustion of IPv4 at the ICANN level (Durand et al. 2011). Tellingly, ipv6 working group's rechartering to 6man took place in the second half of 2007, signalling a transition in the working group's activity from developing IPv6 to maintaining it (IETF 2021c).

The graphically biggest node in Graph 3.4 (pink) (EC: 1.0) is a long-time IBM affiliate. Here, again, major nodes belong to different intra-network communities. Among the most central nodes between 2007 and 2008 one can detect FUNET, IBM, Nokia, and Cisco affiliates. In term of PageRank, the ranking order changes but the most central nodes remain the same. In

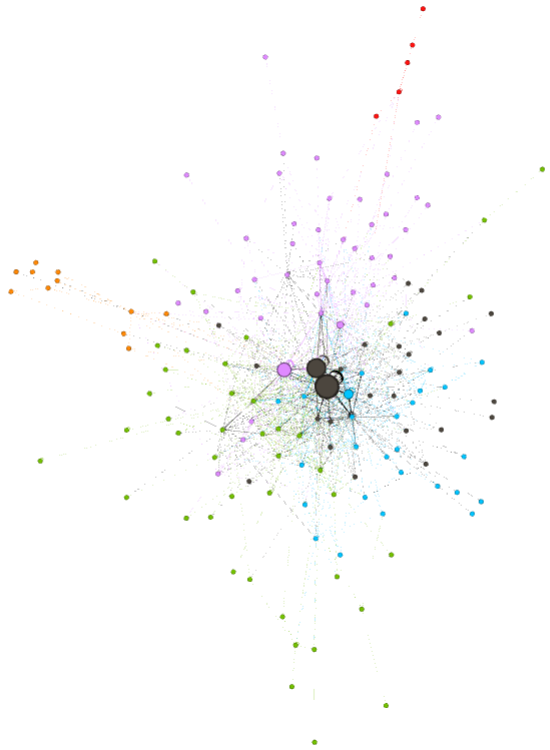
analytical terms, a certain proactiveness from and centrality of IBM affiliates can be inferred, although in terms of RFCs the company has never been among the most outstanding ones (Arkko 2021). Once again, cross-community ties are present, and the same disclaimer raised for idr modularity applies here. Furthermore, no affiliate from Chinese companies features among the most central nodes in the mid-2007 to mid-2008 timespan.



Graph 3.4: ipv6/6man network. 2007-2008 (Nodes: 145; Edges: 509)

Differently from idr, 6man had not experienced outstanding Chinese growth within its intra-mailing list networks by mid-2019. The main node (EC: 1.0) in Graph 3.5 (bigger in black) was among the most central ones in 2008, too, although the affiliation changed. Among the five most central nodes in terms of eigenvector centrality, we find a Cisco affiliate, featuring along a SI6Network affiliate and a non-affiliated participant. Observing centrality in terms of PageRank, no major difference appears. While one can observe new corporate actors coming into play in central roles in the network, no increasing

centrality from Chinese companies is detected.



Graph 3.5: ipv6/6man network. 2018-2019 (Nodes: 177; Edges: 1255)

Interestingly, while no central mailing list activity is found by Chinese actors, a quick look at the IETF Datatracker shows that many of the leading members of 6man co-authored RFCs with Huawei affiliates during the timespan in question. However, such RFCs are all within other WGs (IETF 2021b). This hints at a lower interest from Huawei affiliates in 6man work at this stage.

Beyond individual behaviour, four communities emerge as particularly big, coloured black, green, pink, and blue in Graph 3.5. Three out of four such communities feature Chinese companies' affiliates and all of them feature at least one of the ten most central individuals in the network. Once again, Chinese companies' affiliates interact within and across intra-network community like the affiliates of any other major organisation participating in the IETF.

Looking at intra-domain entropies to check for patterns of corporate

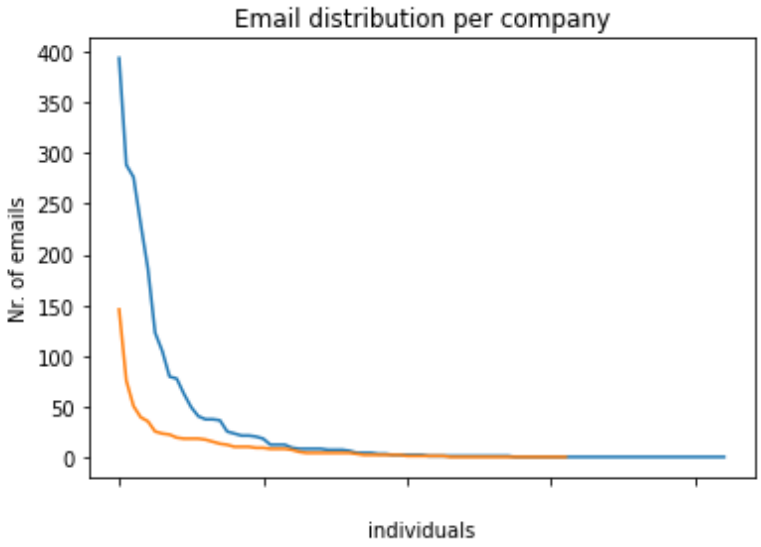
engagement in 6man, Huawei and Cisco display the highest entropy (Table 3.2).

```
domain_entropies.head(20)
```

huawei.com	3.277980
cisco.com	3.000626
gmail.com	2.910444
yahoo.com	2.470394
u-1.phicoh.com	1.912986
nokia.com	1.858399
hotmail.com	1.717361
samsung.com	1.660817
chinamobile.com	1.660015
ietf.org	1.569438
zte.com.cn	1.565129
motorola.com	1.554238
isc.org	1.418576
cable.comcast.com	1.336058
francetelecom.com	1.332179
jp.yokogawa.com	1.313864
nist.gov	1.310784
hp.com	1.309533
sun.com	1.308972

Table 3.2: 6man domain entropy

However, Huawei's engagement since ipv6/6man's inception is significantly lower than Cisco's in purely quantitative terms: 2368 mails sent from the cisco.com domain against 740 from Huawei affiliates by March 2021. It must be noticed that these figures might be skewed because Huawei's participation became active in 2007 and prominent in the following year, while Cisco's engagement is longer-standing (Arkko 2021).



Graph 3.6: 6man/ipv6 email distribution - mails sent per individual. Legend. Blue: cisco.com; orange: huawei.com.

In Graph 3.6 it can be noted that Huawei's activity in the mailing list is more strictly dominated by one person responsible for around 150 mails, while Cisco's distribution is more spread out among its affiliates, several of which authored more than 250 emails. This resembles the patterns seen in idr (Graph 3.3).

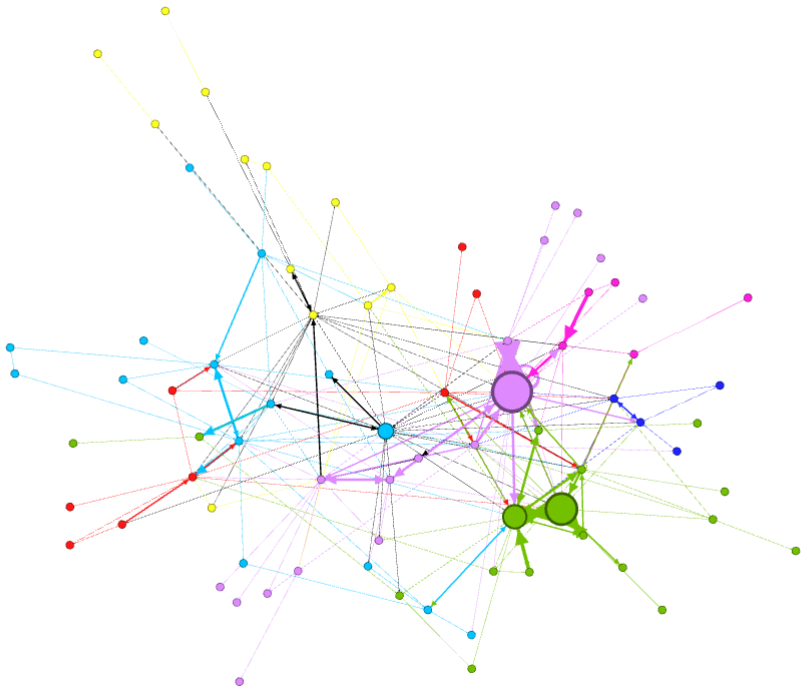
In 6man, again, Huawei's patterns of engagement in the mailing list are different from those displayed by Chinese state-owned companies - China Mobile and ZTE in this case. Their domain entropies are lower than Huawei's (Table 3.2), and their engagement is too: all China Mobile and ZTE affiliates are responsible for less than ten emails each, except for one ZTE affiliate. None of the RFCs published between 2008 and 2019 feature authorship(s) from these companies (IETF 2021b).

In summary, no major growth from Huawei's part can be detected in participation and influence in 6man, not even in terms of published RFCs. Once again, Chinese SOEs participate at a much lower level but are present. However, Huawei affiliates grew in participation and featured in many of the most numerous intra-network community by mid-2019.

3.2.3 *Application Layer Traffic Optimisation (alto)*

The third and last working group in this analysis is alto. As mentioned before, its timespans are different: November 2008 to November 2009, that is to say the WG's inception year; June 2018 to June 2019; and January to December 2020. This third timespan has been added as between mid-2018 and mid-2019 the group was dormant in terms of published RFCs.

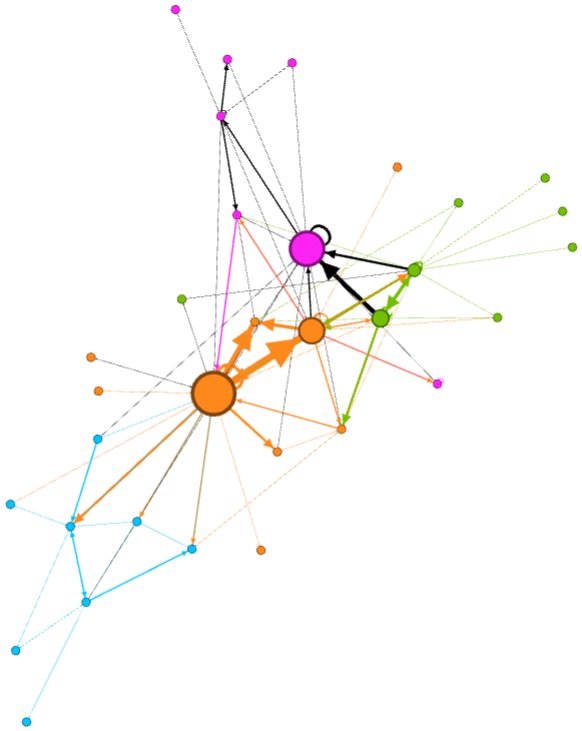
To begin with, probably the most striking difference between the first two timespans, represented in Graphs 3.7 and 3.8 respectively, is the de-growth in participation. While participation in the IETF generally increased in the last decade and a half (Arkko 2021), participation in alto decreased. Graph 3.7 features 86 nodes, while Graph 3.8 has 40.



Graph 3.7: alto network. 2008-2009 (Nodes: 86; Edges: 271)

Chinese companies' affiliates' participation in alto is visible since its inception. In Graph 3.7 (November 2008 and November 2009), the most

central nodes belong to Western companies. However, Chinese companies' affiliates, including Huawei and ZTE, feature in the communities with the most central nodes (pink, green, and light blue), signalling participation and interaction in working group discussions. This is peculiar, as Chinese companies' presence in other working groups at this early stage was less visible.

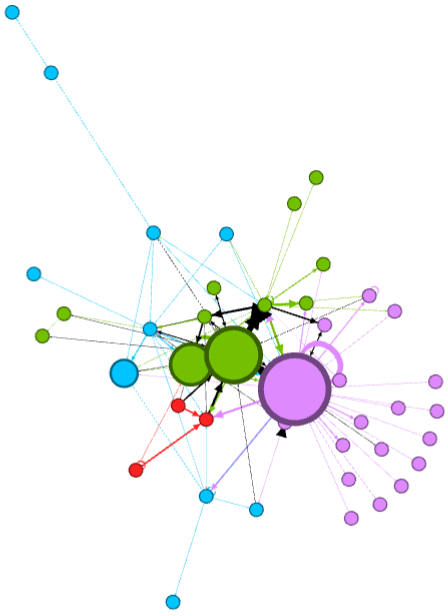


Graph 3.8: alto network. 2018-2019 (Nodes: 40; Edges: 105)

While participation in alto has declined by June 2019, Chinese presence is still relevant. While the most central nodes are from Nokia and Yale University, affiliates from Chinese entities, including a university, are active and are encompassed in the same communities as the most central nodes (Graph 3.8). However, edges connecting Chinese companies' affiliates to the most central nodes from Nokia and Yale are constantly lighter, hinting at a less intense participation in the mailing list.

This stage in alto's work is a peculiar one, as no alto-related published RFC is retrievable from the IETF's website (IETF 2021b). Nonetheless, Graph

3.9 shows a slight increase in participation and activity in 2020 (January-December), whereas three Standards-Track RFCs have been published within the year (IETF 2021b). While only one such RFC has been co-authored by affiliates of Chinese companies (Randriamasy et al. 2020), eigenvector centrality in the network increased for some individuals affiliated to Chinese private and public entities – including a Sichuan University affiliate. This runs along high centrality from Yale and Nokia affiliates as far as Western entities are concerned. This time, it must be acknowledged that PageRank appears to display higher centrality from Nokia-affiliated individuals and a lower one for Huawei participants.



Graph 3.9: alto network. 2020 (Nodes: 48; Edges: 116)

Again, Chinese and Western entities' affiliates are distributed among intra-network communities (Graph 3.9): the most central nodes (bigger in size) are coloured pink, green, and blue, signalling membership to three different communities within alto.

As Table 3.3 shows, 'huawei.com' is once again among the most entropic

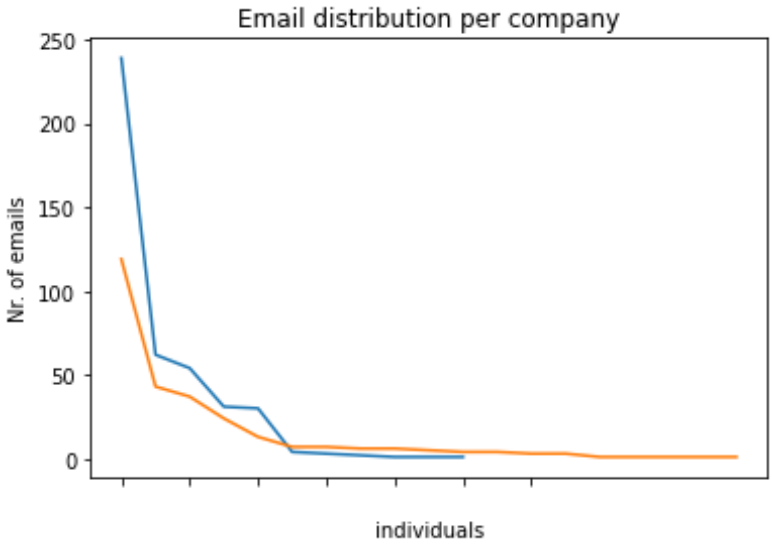
organisational domains, but so are ‘alcatel-lucent.com’ and ‘yale.edu’.

```
domain_entropies.head(20)
```

gmail.com	2.541374
huawei.com	1.991160
yale.edu	1.444534
ietf.org	1.409546
alcatel-lucent.com	1.388845
cisco.com	1.333706
nokia.com	1.333636
chinamobile.com	1.197980
net.t-labs.tu-berlin.de	1.098612
neclab.eu	1.075241
nw.neclab.eu	1.065027
verizon.com	1.039721
juniper.net	1.032691
nsn.com	1.011404
outlook.com	1.005467
zte.com.cn	0.974315
nokia-bell-labs.com	0.706373
hushmail.com	0.693147

Table 3.3: alto domain entropy

As a matter of fact, both domains’ email distribution is graphically different from the close-to-random one represented in Graph 3.3 for gmail.com. Once again, one can see in Graph 3.10 that a single individual dominates Huawei’s engagement in alto (around 120 emails), while several others display a lower but consistent participation in the email list. This is in line with the presence of at least one Huawei affiliate among alto’s most central individuals in 2020.



Graph 3.10: alto email distribution - mails sent per individual affiliate. Legend. Blue: alcatel-lucent.com; orange: huawei.com.

This pattern is similarly found, albeit on a higher scale, in the same graph for Alcatel-Lucent, which by 2021 is owned by Nokia (Alcatel-Lucent 2021). As one can see, a single individual is responsible for around 240 email communications since the working group's inception up to April 2021, while a smaller group of affiliates is responsible for circa 30 to 55 emails each.

To conclude on alto, patterns of engagement from Huawei are similar to those found for other major participants. While some Huawei- and Sichuan University-affiliated individuals are particularly central in the network, such centrality is 'shared' with Western entities' affiliates, mainly Nokia by 2020, and the identified communities within alto's network are cross-national in terms of affiliation. This is in line with the patterns found in the two working groups described above, despite different fluctuations in overall working group participation through time.

3.2.4 *Networks in the IETF: final remarks on Chinese engagement*

To draw some common lines among the three IETF working group analysed, three main statements can be made. First, while intra-working group

networks display a subdivision in communities (modules), such subdivision is loose and does not run along national lines. Second, similar longitudinal patterns of engagement are detected from Huawei and major non-Chinese actors in different working groups, with an individual (or up to five, for Cisco) affiliate(s) dominating the company's communication in the mailing list and a group of lower-profile, but still active, colleagues displaying their presence. Third, while Huawei and Chinese state-owned enterprises do work together (for example, in publishing RFCs), especially as far as ISPs are concerned, this relation is by no means exclusionary. Huawei affiliates publish RFCs with Western companies' affiliates too and are visibly more active than Chinese SOEs.

In other words, patterns of coordination among Chinese actors in the IETF are present, but there emerges no visible outside control. Companies act differently and engage with Western counterparts in different ways depending on their economic sector and market needs. On the one hand, Chinese manufacturers like Huawei do work along with their homologues from the West. On the other hand, they retain coordination with other Chinese companies involved in the domestic value chain (for example, ISPs) (Negro 2017; Zhang, Liang 2007).

To be sure, network analysis is not a tool to uncover relations of external political control, reason for which these observations will be corroborated in the forthcoming chapters through qualitative methods. What one can observe is the growth of Huawei and other Chinese actors in centrality in selected working groups, one that follows their global economic growth and the new prominence of China as a political and economic state actor.

No peculiarities are visible in Huawei's patterns of interaction with Western counterparts. Huawei's collaboration with Western companies in publishing RFCs is in line with the need for widespread consensus in the IETF community for standards to be recognised as such. Should Huawei's growth be strictly connected to external political control from the Chinese government, its exponential growth and influence within the IETF could indicate the growth of state influence in private-based governance settings. This is better addressed in

the forthcoming chapters through qualitative analysis.

3.3 *Networks in ICANN*

Recalling from the methods section of Chapter 1, the three groups under analysis for ICANN are the Chinese Generation Panel (chinesegp), the Generic Names Supporting Organization's New Generic Top-level Domains Subsequent Procedures Working Group (gnso-newgtld-wg) and IANA Issues (ianaissues). The whole of 2016 email exchanges are analysed. 2016 was chosen as a key point in ICANN's history as the year when the IANA stewardship transition was completed.

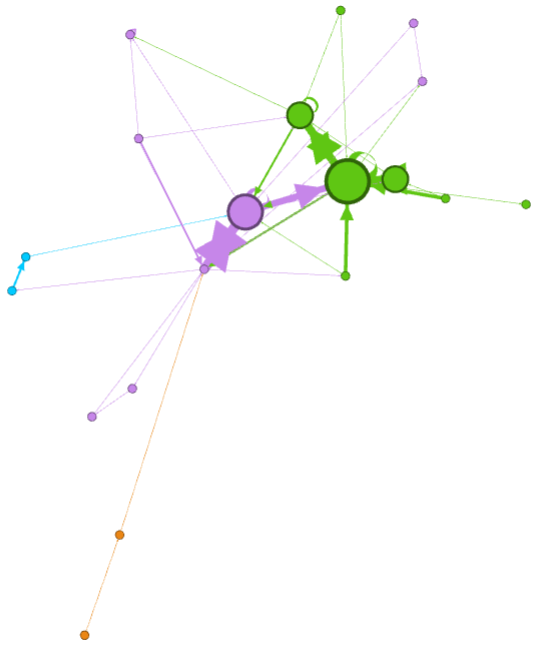
Observing Chinese stakeholders' interaction within ICANN helps one to gauge their position and role at the core of critical Internet resources management and distribution. In other words, one can observe their acceptance of or contestation to the existing normative architecture of Internet governance and build interpretations to corroborate through qualitative means, as per the forthcoming chapters.

3.3.1 *Chinese Generation Panel (chinesegp)*

The first group under analysis is chinesegp. As anticipated in Chapter 2, Generation Panels work on Internationalised Domain Names (IDNs) for specific languages – in this case, Chinese. The general work on the establishment and maintenance of IDNs is subdivided among various subgroups within Advisory Committees (ACs) and Support Organisations (SOs). This is due to the need to incorporate many stakeholders in the process, such as registries, registrars, users' communities, and different sets of expertise, such as linguists, other than technologists (ICANN 2015).

To begin with, groups in ICANN display different characteristics compared to the IETF. First, stronger participation from members of staff is

visible. Second, nodes and edges are generally fewer, possibly due to many topics being related to specific interest groups rather than the broader community. Furthermore, many potentially sensitive mailing lists, such as GAC's, are not publicly readable – a problem already identified in Chapter 2.



Graph 3.11: chinesegp network. 2016 (Nodes: 21; Edges: 45)

Observing the work of chinesegp in 2016 in Graph 3.11, one can see that only 21 individuals (nodes) were active in the mailing list throughout the year. There are six detected communities, but only two feature more than two nodes (in green and pink), all featuring some of the most central nodes. These feature the GP's most active members. Interestingly, affiliates from several country-code Top-level Domains (ccTLD) registries from the Asia-Pacific feature here, including JPRS (Japan) and NIDA (Korea). Along with them, there is a top representative from the Hong Kong-based DotAsia Organisation. After launching the '.asia' sponsored TLD, the organisation engaged in launching IDNs in Chinese, Korean, and Japanese (DotAsia 2021). Through time, DotAsia had a conflictual relation to PRC authorities. According to DotAsia

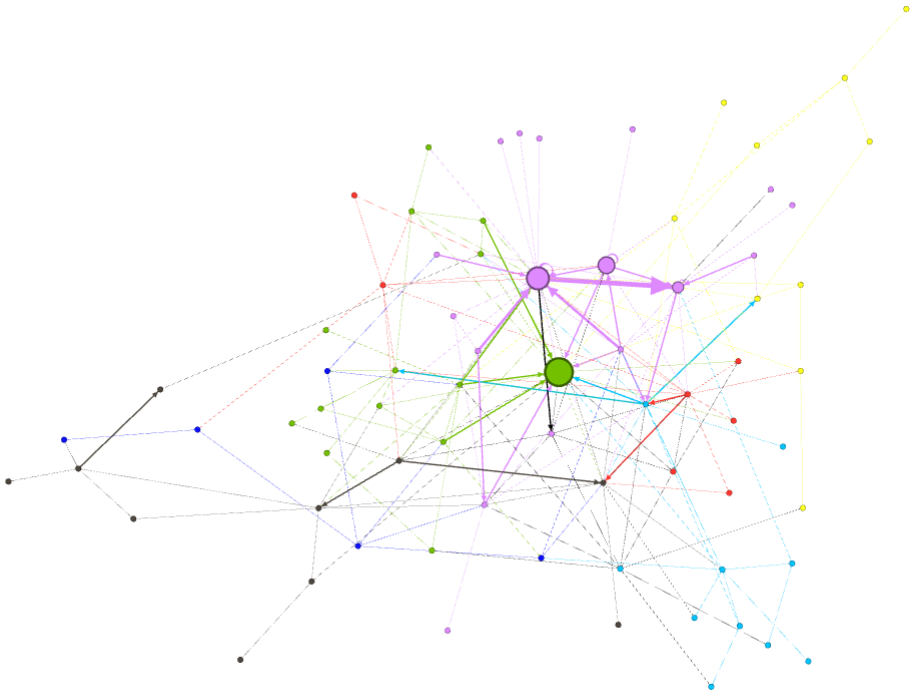
itself (2019), it is only since 2019 that the '.asia' domain is marketable in mainland China again, after having lost MIIT licensing in 2017. The five most central nodes also feature an affiliate of the China Internet Network Information Centre (CNNIC), registry of the '.cn' ccTLD.

In summary, by 2016 chinesegp attracted participants from some of the main ccTLD registries in the region, with Korean participation both from NIDA and universities. In China's case, one single CNNIC affiliate features prominently, along with an affiliate from the Hong Kong-based '.asia' domain registry, on which the aforementioned qualifications must be made. Other CNNIC affiliates feature among the least active members of the GP.

The three biggest nodes in Graph 3.11 (in pink and green) are from JPRS (EC: 1.0), a Korean university (EC: 0.96) and DotAsia (EC: 0.79), although the most active CNNIC affiliate follows closely in EC terms. PageRank does not change the distribution of central roles in the nodes, other than featuring a Pakistani university affiliate among the five most central nodes. This is to say that, perhaps unsurprisingly, the establishment of LGRs related to Chinese character IDNs was not dominated by Chinese actors. On the contrary, several registries from the Asia-Pacific area showed interest and participated.

3.3.2 *GNSO's New gTLDs Subsequent Procedures Working Group*

Interestingly, while Chinese commitment, including at the state level, towards IDNs has been documented also within the ICANN community itself (Zhang 2019), the GNSO's New gTLDs Subsequent Procedures Working Group did not feature much Chinese presence in 2016 (Graph 3.12). It is worth recalling that gTLDs are the main target activity for commercial stakeholders and that the New gTLDs process was launched in 2012 to increase competition in the domain market and avoid domain scarcity (Lipton 2016).



Graph 3.12: gnso-newgtld-wg network. 2016 (Nodes: 78; Edges: 217)

The absence of a prominent Chinese presence is surprising if one takes the starting point of Chinese industry's need for increasing presence in the domain name market demonstrated by activeness in IDNs rule-making. Perhaps Chinese-characters IDNs carry a stronger political weight compared to new ASCII gTLDs (Swartz 2006), notwithstanding the economic salience of both (Lipton 2016).

Since the inception of IDN-related talk in the early 2000s, the Chinese government and the Chinese state-controlled CNNIC restated their interest in controlling the distribution of domain names in Chinese. In 2000, Verisign announced it would launch non-ASCII domain names, including Chinese ones, trying to anticipate IETF standardisation on the matter. At this stage, the Chinese government and CNNIC pressured ICANN to prevent Verisign from taking this step by having a GAC communiqué approved that sought to establish principles for IDN approval (Ermert, Hughes 2003). While ICANN proved reluctant to prevent Verisign from taking this step, Chinese-script

domain names under the '.com', '.cn', and '.net' TLDs had been launched by CNNIC by 2006 (Swartz 2006). This generated fear of fragmentation as it looked like a separate DNS root would be created. Confusion was created by the fact that Chinese-character TLDs operated in China run in parallel to the DNS supervised by ICANN, while Chinese-character second-level domains were resolved under the '.cn' domain operated by CNNIC and recognised by ICANN.

This complex system allowed China to pre-emptively occupy the Chinese IDN space, thus forcing ICANN to accept the status quo when it came to regulating the distribution of IDNs (Arsène 2015). Otherwise, domain names obtained through the ICANN-supervised DNS could have overlapped with those already established in China under CNNIC. If the same domain name can point to different websites (and contents) on two different roots, it is as if a single phone number pointed to two different households' landlines (Swartz 2006). This could have increased the chance of creating a split DNS.

While this generated frictions between ICANN and China, the DNS split did not take place and ICANN embarked on an ongoing work for IDNs distribution and regulation under IETF-established common standards (ICANN 2015). In this, China partially run its own DNS in parallel for some time while making technical efforts to maintain interoperability with the ICANN-supervised one. While this is no longer the case, the MIIT maintains strict regulations on who can register IDNs in China and how, thus granting both China's participation in the global DNS and domestic control on contents (Arsène 2015).

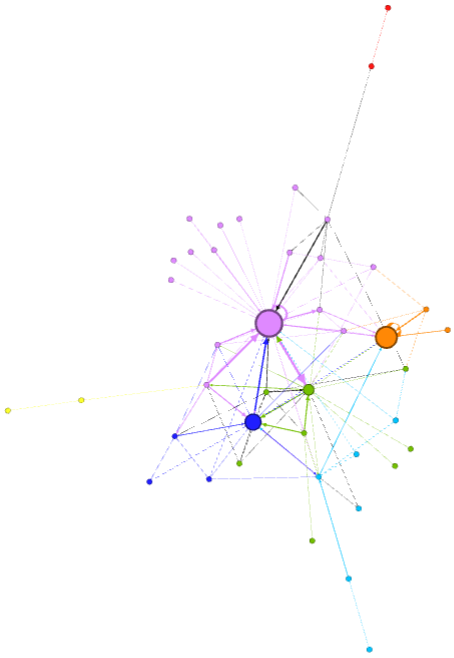
This historical excursus may help to interpret why Chinese attention on IDNs was much higher than on New gTLDs. However, these aspects have been better corroborated through interviews, the interpretation of which is illustrated in the forthcoming chapters.

3.3.3 *IANA Issues*

The third and last mailing list in analysis for ICANN is ianaissues (Graph

3.13). This mailing list brought together At-Large Advisory Committee's (ALAC) members to discuss matters related to the IANA stewardship transition from a users' perspective. ICANN's At-Large community is made of users' associations at the regional level, some openly allowing individual membership, some allowing individual membership through national users' associations (ICANN At-Large 2021).

Along with the two lists observed above, the ianaissues mailing list completes a panoramic on Chinese actors' engagement in the gTLD and ccTLD management sectors and the user's level.



Graph 3.13: ianaissues network. 2016 (Nodes: 44; Edges: 110)

Strikingly, little Chinese user participation is found in 2016 in the mailing list in question, apart from one Chinese ICANN employee and an affiliate of Beijing University, long-time participant in ICANN. Yet, they both feature eigenvector centrality and PageRank close to zero. On the other hand, most central roles in the network in eigenvector centrality (and page ranks) terms are

played by Western ALAC members, mostly from Europe, by an African academic technologist, and by an ALAC member of staff. All the most central individuals belong to different communities within the group's mailing list, as identified through the modularity algorithm (pink, orange, blue, green in Graph 3.13).

3.3.4 *Final lines on Chinese stakeholders' engagement in ICANN*

Overall, Graphs 3.11 through 3.13 show Chinese engagement in IDNs through CNNIC, a state-sponsored ccTLD manager. However, no strong Chinese participation is found at the users' level nor at the commercial or non-commercial one in the GNSO. GNSO, in general, does feature Chinese participation among contracted parties. Eminently, at the time of writing a member of the GNSO Council, Pam Little, is affiliated to Alibaba, which is member to GNSO as a registrar. Her mandate is still on-going at the time of writing but will expire in Autumn 2021 after having started in 2017 (GNSO 2021).

However, other major participants are not visible in terms of formal role or activeness in the selected mailing list in the key turning point of 2016, despite the importance of the New gTLD round and despite several Chinese companies feature as contracted parties (registries and registrars) among GNSO members.

This low-profile presence of Chinese stakeholders in ICANN, compared to their pre-eminence in the IETF, will be better interpreted through interviews and document analysis. However, it is surprising to see such difference in engagement, especially compared to common expectations of China's proactiveness in contesting multistakeholderism and reshaping the rules of Internet governance. Furthermore, China's rapprochement to ICANN in the phase after the approval of the Tunis Agenda and the agreement on Taiwan's participation would have suggested increasing participation from Beijing's part. While presence has increased, policy proactiveness and impact is not as visible in network analysis.

Whether this is due to engagement in other forms of contestation, such as

forum shopping towards multilateral venues, or other reasons will be better explored in the forthcoming chapters. This would help assessing the extent to which China's contestation and adaptation to ICANN norms are in place (Negro 2020).

3.4 *Chinese stakeholders' interactions in 3GPP*

Before moving to observing interactions in 3GPP, a caveat needs to be restressed. The peculiar functioning of 3GPP mailing list exchanges make the network analysis criteria applied above unworkable. Briefly, when a participant sends an email, they put themselves as receivers along with the collective email list address. In network-analytical jargon, this creates a graph with all nodes but no edges, as senders and receivers are the same persons. This forces one to look for other ways to make similar observations.

As anticipated above and in Chapter 2, the intra-domain entropy analysis applied to 3GPP working groups proves useful, as it shows the different size of corporate engagement in a given mailing list. This peculiar type of analysis follows the same objectives as those illustrated in the previous sections of this chapter. In particular, it aims to observe the influence and extent of adaptation of Chinese stakeholders to standard-making norms in 3GPP. While 3GPP has no direct competence on the Internet infrastructure, its work on 5G makes it a venue of utmost technical and political importance. First, influence in 3GPP means influence in what the 5G standard looks like in security terms. Second, a company that has its patents incorporated in the standard gains strong economic and strategic weight. Third, 5G connectivity is IP-based and increases the interdependence between telephony and Internet infrastructures, as anticipated in the previous chapter and better discussed in the concluding one.

These aspects, together with the economic competition between the US and China, led to the securitisation of 5G. Observing Chinese stakeholders in

3GPP, to recap, allows one to gauge their influence in, adaptation, and contestation to the rules and norms of mobile connectivity standardisation.

3.4.1 *Core Network and Terminals Working Group 1* (CT1)

NOKIA.COM	741
ERICSSON.COM	574
HUAWEI.COM	533
QTI.QUALCOMM.COM	480
ETSI.ORG	222
ZTE.COM.CN	200
SAMSUNG.COM	172
VIVO.COM	102
LGE.COM	97
MEDIATEK.COM	94
INTERDIGITAL.COM	91
OPPO.COM	90
BLACKBERRY.COM	78
MOTOROLA.COM	73
PARTNER.SAMSUNG.COM	66

Table 3.4: 3GPP-CT1 Emails per domain.

Table 3.4 displays the number of emails sent in the CT1 mailing list per corporate domain. CT1 is short for Core Network and Terminals (CT) Working Group 1 (WG1). As expected, Nokia, Ericsson, and Huawei feature as the most active domain names (that is, companies) followed by Qualcomm, ZTE, and Samsung – leaving aside the institutional domain ETSI.ORG.

While the US is a major national actor in the IETF with Cisco, its role is relatively marginal in 3GPP, where the main competition is between European and Chinese companies, with South Korean ones playing a major role. Other than being visible in Graph 3.18, this also appears in Pohlmann, Blind and Hess (2020), who indicate Huawei and Ericsson as the main proponents of 5G standardisation proposals and Samsung as the main owner of 5G-related patent families by the beginning of 2020. As illustrated in Chapter 1, 3GPP was initially a Europe-led project. This less central role of US companies helps interpret the US's positioning towards the 5G question amid the emergence of Chinese companies, Huawei in particular, as major players. However, this is

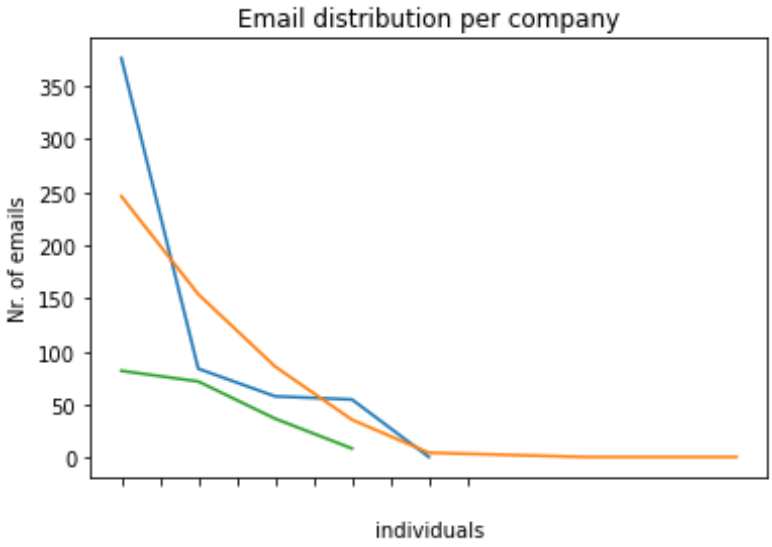
better corroborated through qualitative analysis in the forthcoming chapters.

```
domain_entropies.head(20)
```

SAMSUNG.COM	1.614434
APPLE.COM	1.470132
QTI.QUALCOMM.COM	1.318756
HUAWEI.COM	1.300237
ZTE.COM.CN	1.185068
NOKIA.COM	1.178618
ATT.COM	1.059385
ERICSSON.COM	1.025760
MEDIATEK.COM	1.013745
INTERDIGITAL.COM	0.782998
VIVO.COM	0.717865
INTEL.COM	0.686962
OPPO.COM	0.626103
ORANGE.COM	0.595400
ETSI.ORG	0.576147
CHINAMOBILE.COM	0.450561
THALESGROUP.COM	0.410116
LGE.COM	0.374255

Table 3.5: 3GPP-CT1 domain entropies.

Moving forward, from the content of Table 3.5 one can easily gauge that in CT1, like in IETF working groups, the most active companies feature the highest intra-domain entropy, although Ericsson is fairly low compared to Apple, who does not feature among the most active companies in Table 3.4.



Graph 3.14: 3GPP-CT1 email distribution.

Legend: blue: Ericsson; orange: Huawei; green: ZTE

Observing email distributions, Graph 3.14 shows three different patterns of engagement between Ericsson, Huawei, and ZTE. Ericsson has been chosen as a comparison owing to its leading position, along with Huawei, in terms of 5G standardisation contributions (Pohlmann, Blind, Hess 2020), while ZTE has been chosen as China's main SOE in this sector.

In Graph 3.14, one can see Huawei has a leading affiliate who authored almost 250 emails, followed by one who authored around 150. Then the graph features a long tail of low-profile Huawei affiliates. The same graph shows instead that Ericsson's affiliates are also led by a single highly active participant who authored more than 350 emails but have a bigger group of lower-profile but active (between 50 and 100 emails each) affiliates. ZTE's participation is instead much more low-profile, with no affiliates having authored more than 100 emails and much fewer affiliates being active at all.

In short, Huawei and Ericsson have different patterns of engagement, but their activeness in the mailing list of the present WG on core technology reflects their prominence in 5G standardisation proposals as illustrated by Pohlmann, Blind and Hess (2020).

3.4.2 *Radio Access Network Working Group 5 – New Radio (WG5_NR)*

The second working group under analysis is Radio Access Network (RAN) working group 5, and in particular their mailing list on 5G's New Radio (NR). As mentioned in Chapter 1, 5G's New Radio refers to the portion of radio frequency between the device and the active base station. This specification is key for 5G connectivity function as radio access remains the most prominent architectural aspect in 5G standardisation as it affects devices' specification.

ERICSSON.COM	192
QTI.QUALCOMM.COM	149
CHINAMOBILE.COM	59
HUAWEI.COM	59
ROHDE-SCHWARZ.COM	56
ETSI.ORG	55
MOTOROLA.COM	44
KEYSIGHT.COM	43
ANRITSU.COM	40
NTTDOCOMO.COM	29
CATT.CN	23
HISILICON.COM	22
CAICT.AC.CN	20
PARTNER.SAMSUNG.COM	19
ATT.COM	15

Table 3.6: 3GPP-RAN5_NR Emails per domain.

To begin with, in Table 3.6 one can see that up to the end of June 2021 conversation in the mailing list was mainly participated by Ericsson and Qualcomm affiliates. Huawei's affiliates follow right after in terms of number of emails sent by its affiliates since the list's inception (in June 2017), but the quantitative distance is visible. What is striking in terms of Chinese participation in this email list is the presence of Chinese state-owned ISPs like China Mobile and public academic entities such as the China Academy of Telecommunications Technology (CATT) and the China Academy of Information and Communication Technologies (CAICT). While these actors are usually less prominent than Huawei in participation, they emerge as active participants in this list. To be sure, Huawei's participation is still more prominent. The emails sent by its affiliates are more than CATT's and CAICT's

put together, while the 59 emails registered by China Mobile affiliates have all been authored by the same person, signalling lower engagement in number of participants. Furthermore, to the emails sent from huawei.com domains, one should add those sent by HiSilicon affiliates. HiSilicon is a semiconductor manufacturer fully owned by Huawei and based in Shenzhen, China. This shows a high variety of Chinese participation in the work of this group, although one should not be surprised by the presence of semiconductor makers.

As mentioned, RAN work has the strongest impact on the device market in that it affects devices' technical specifications. Coherently, it can be argued that chipmakers strive to have their patented technologies in the international telecommunication standard, so that they gain royalties and technological advantage on the semiconductors market, which is essential in devices' manufacturing (Mahon 2017; Yu et al. 2017). This could also explain the strong presence of another globally important semiconductor maker, Qualcomm, whose affiliates are overall active but often less central in other 3GPP settings.

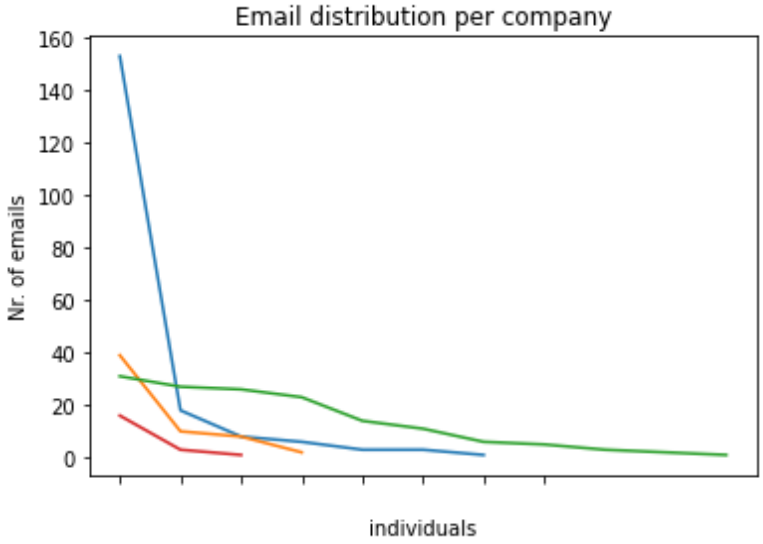
```
domain_entropies.head(20)
```

QTI.QUALCOMM.COM	2.057157
ROHDE-SCHWARZ.COM	1.332180
KEYSIGHT.COM	1.217890
ANRITSU.COM	1.130274
HUAWEI.COM	0.960138
ERICSSON.COM	0.800925
SGS.COM	0.693147
APPLE.COM	0.693147
SAMSUNG.COM	0.693147
MOTOROLA.COM	0.689009
HISILICON.COM	0.655482
CAICT.AC.CN	0.612869
ETSI.ORG	0.587179
NTTDOCOMO.COM	0.575730
INTERTEK.COM	0.562335

Table 3.7: 3GPP-RAN5_NR domain entropies.

Observing domain entropies in this email list in Table 3.7, one finds once again that the most engaged corporate actors have higher entropy. When comparing corporate email domains, this is perhaps unsurprising. After all, one

can expect that the higher the number of people involved for an organisation, the higher the number of emails sent, the higher the difference in engagement among individuals with the same affiliation (entropy). However, the entropy of ericsson.com is lower than that of huawei.com, despite the different number of authored emails highlighted in Table 3.6. In this, qualcomm.com's entropy is much higher than everyone else's despite the number of emails sent being similar to Ericsson's. This suggests different patterns of engagement for different companies.



Graph 3.15: 3GPP-RAN5_NR email distribution.
Legend: blue: Ericsson; green: Qualcomm; orange: Huawei; red: CAICT.

Observing email distribution in Graph 3.15, one can note that this holds true. While Ericsson and Qualcomm affiliates authored a similar number of emails in the list, they adopted different engagement strategies. Ericsson displays fewer participants (X axis) than Qualcomm, but one of them alone authored more than 150 emails (Y axis). On the contrary, Qualcomm affiliates are more numerous, but authored fewer emails each. The Chinese stakeholders represented in Graph 3.15 feature an email distribution per affiliate similar to Ericsson's, although smaller in scale: one prominent individual followed by a few less active affiliates.

To summarise, Huawei is a prominent corporate actor in the RAN5 mailing list on 5G's NR, although not as active as Ericsson and Qualcomm. Arguably, given the economically strategic importance of radio access, this group features a stronger participation from 'chip' makers, including the Huawei-owned HiSilicon.

3.4.3 *Service and System Aspects Working Group 3 (SA3)*

The third and last working group under analysis in this chapter for 3GPP is Service and System Aspects working group 3 (SA3). The main declared objective of SA3 is "defining the requirements and specifying the architectures and protocols for security and privacy in 3GPP systems" (3GPP 2020). Therefore, this group plays a key role in the making of the architecture.

ERICSSON.COM	6146
HUAWEI.COM	6108
NOKIA.COM	3174
QTI.QUALCOMM.COM	2319
CHINAMOBILE.COM	1152
INTERDIGITAL.COM	1071
ETSI.ORG	1012
SAMSUNG.COM	923
LENOVO.COM	868
APPLE.COM	746
HM.EDU	698
VODAFONE.COM	622
LGE.COM	599
ZTE.COM.CN	498
THALESGROUP.COM	489

Table 3.8: 3GPP-SA3 Emails per domain.

The number of emails per domain in SA3 mailing list reflects expected distributions based on Pohlmann, Blind and Hess (2020) figures on standardisation contributions to 5G (Table 3.8). Ericsson and Huawei are by far the main corporate contributors to the mailing list, followed distantly by Nokia, Qualcomm and only later China Mobile and Samsung. Overall, this group is strongly Europe- and China-dominated in purely quantitative terms, looking at

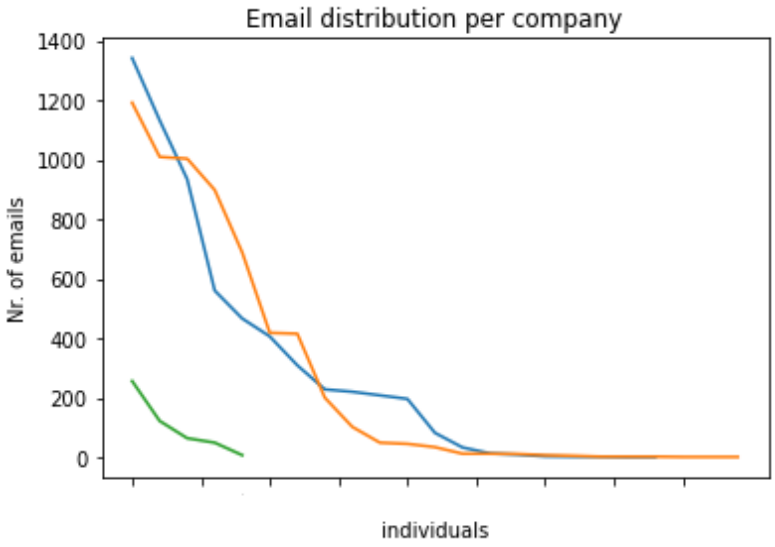
the mailing list. Arguably, this is due to the growing politicisation of infrastructural security amid the concerns raised by the then Trump administration over the potential for backdoors being inbuilt in the infrastructure (Ciuriak 2019). Therefore, the main network manufacturers may see an interest in setting international network security standards and have their patents incorporated there.

```
domain_entropies.head(20)
```

ERICSSON.COM	2.259691
HUAWEI.COM	2.152640
CHINAMOBILE.COM	1.477291
NOKIA.COM	1.372103
ALCATEL-LUCENT.COM	1.341003
ZTE.COM.CN	1.238421
QTI.QUALCOMM.COM	1.228122
SAMSUNG.COM	1.148102
OUTLOOK.COM	1.098612
CHARTER.COM	1.039721
GMAIL.COM	0.983281
VODAFONE.COM	0.859340
BT.COM	0.822600
PHILIPS.COM	0.812599
TNO.NL	0.805370
TELEKOM.DE	0.758932
HPE.COM	0.737508

Table 3.9: 3GPP-SA3 domain entropies.

Once again, the most active companies have the highest degrees of entropy, although one can see that there is no straightforward correspondence. Graph 3.16 shows the different patterns of engagement of Ericsson, Huawei and ZTE. Again, Huawei and ZTE are compared to look for different patterns of engagement between state-owned and private-owned Chinese actors. As per above, Ericsson and Huawei are the dominant actors in SA3 mailing list and one can see that their pattern of engagement is similar: few individuals dominating participation in the list on the company's behalf and a 'long tail' of less active affiliates.



Graph 3.16: 3GPP-SA3 email distribution.
Legend: blue: Ericsson; orange: Huawei; green: ZTE.

To summarise, the two most active corporate actors in terms of 5G standard contributions dominate conversations in the SA3 mailing list in quantitative terms, coherently with expectations based on Pohlmann, Blind and Hess' (2020) data.

3.4.4 *Chinese engagement in 3GPP: final remarks*

The selected working groups observed in 3GPP allow a series of observation. First, different areas of work attract different kinds of actors, with specialisation increasing in more strictly focused groups – such as RAN5's subgroup on New Radio. Second, Chinese companies – mainly Huawei – carry a leading position, directly in line with that of major European and South Korean players, as expected observing secondary data by Pohlman, Blind and Hess (2020). Third, given the strongly securitised media discourse on 5G, it is interesting to look at Chinese companies' engagement in the elaboration of architectural security features in SA3, where Huawei has a strong position as much as in other 3GPP working groups.

On the one hand, one can reiterate observations similar to those valid for

the IETF: should Chinese stakeholders be politically controlled, the Chinese government would have a strong indirect weight within industry-based standard-making activities affecting usership all over the globe. This would have a strong normative impact on the private-based nature of standardisation activities in turn. Nevertheless, no such form of tight control and overlap in activities is visible from Chinese stakeholders in 3GPP, an aspect that has been addressed in expert interviews and will be illustrated in the forthcoming chapters.

3.5 *Concluding remarks*

The computational analysis illustrated above is exploratory and serves as a basis for the interpretive, qualitative analysis addressed in chapters 4 and 5. What can be observed in this chapter is an analysis of mailing lists of working groups belonging to the three different organisations object of this thesis: IETF, ICANN, and 3GPP. Three working groups have been analysed for the IETF, representing different areas of work of the organisation; three have been analysed for ICANN, shedding light on three different stakeholder groups; and three have been analysed for 3GPP per as many areas of work, or Technical Standardisation Groups (TSG).

Patterns of engagement are different for different companies in each mailing list and this hints at different interests playing out in the given working group. In theoretical terms, it means the way Chinese actors display norm entrepreneurship changes across the Internet governance regime complex. In the IETF, different patterns of growth of Chinese stakeholders' participation were found in the three different working groups and the same applies for Huawei, despite being the second biggest corporate contributor to RFCs publication. In ICANN, Chinese participation is visibly low-profile and while CNNIC plays an active role in IDNs, it is not central in the Chinese Generation Panel during the analysed timespan. This strengthens the qualitative findings

that will be illustrated in Chapter 4. Moving to 3GPP, it was mentioned in the previous section that the prominence of semiconductor makers in the work on New Radio may be connected to the fact that radio access standards affect the device market. As semiconductors are an essential tool for the functioning of devices and networks (IEEE 2013), semiconductor makers see an interest in having their patents included in the international standard.

Overall, the evidence emerged from computational analysis produced a mixed picture of Chinese engagement in the selected subsets of Internet governance. While Chinese presence is strong in 3GPP, it is much less so in ICANN, where Chinese stakeholders are present but not prominent despite contestation has slowly faded away in the last decade. As for the IETF, Huawei is prominent in RFC publications, but Chinese stakeholders' centrality is not constant across all working groups. Despite overall growth in the private-based and multistakeholder Internet governance ecosystem, evidence of Chinese influence is mixed and, much as claims of political control on private actors are widespread, mailing list patterns show different forms of engagement from different actors.

This evidence hints at the complexity of the question of Chinese engagement in multistakeholder and private-based Internet governance and their involvement in the making of (new) Internet standards. In IR-related terms, one can observe that Chinese stakeholders are growing stronger and more participatory and influential in the existing private-based, multistakeholder (that is, liberal-informed) Internet governance ecosystem. However, these patterns are not homogeneous throughout ICANN, the IETF and 3GPP. Furthermore, extents of contestation to multistakeholderism from China's part are still found in literature (Negro 2020). In other words, the Chinese actors' norm entrepreneurship is exercised in different ways in different subsets of the Internet governance regime complex depending on a variety of aspects, with such actors gaining centrality in some contexts and maintaining a low profile in others. These aspects will be better corroborated qualitatively in chapters 4 through 6.

The findings illustrated in this chapter will help the interpretive processes

on these aspects conducted in the two forthcoming chapters, subdivided in critical Internet resources (Chapter 4) and mobile Internet standards (Chapter 5).

CHAPTER 4

ON THE NORMATIVE IMPACT OF CHINESE STAKEHOLDERS IN THE GOVERNANCE OF CRITICAL INTERNET RESOURCES. A DOCUMENT- AND INTERVIEW-BASED ANALYSIS

4.1 *Introduction*

A key takeaway from the computational analysis illustrated in Chapter 3 when it comes to critical Internet resources (CIRs) is the great disparity in Chinese stakeholders' engagement in the IETF and ICANN.

In the IETF, where CIRs are standardised, Huawei plays a major role and minor state-owned actors such as ZTE and the two main national Internet Service Providers (ISPs), China Mobile and China Telecom, are more peripheral but do feature in the work. In sporadic occasions, Chinese universities also feature in the work of IETF working groups (WGs). While the centrality of Chinese stakeholders is different in different WGs, Huawei is overall the second most active corporate actor in terms of Request for Comments (RFCs) published or co-published by its affiliates per year (Arkko 2021).

Conversely, in ICANN, where CIRs are managed within the framework of the IANA functions, Chinese stakeholders keep a low profile. To be sure, some Chinese actors do cover key positions. It is the case of the Alibaba-affiliated member of the Generic Name Supporting Organisation (GNSO) Council and the Chinese government's representative who formerly covered the role of Governmental Advisory Committee (GAC) vicechair in the wake of the IANA stewardship transition, the latter aspect being better discussed below. However, the mailing lists analysed in Chapter 3 do not show prominent Chinese participation and Chinese membership in many ICANN bodies is relatively low.

Matters of Chinese engagement and impact in Internet governance are explored throughout interviews and documents analysis in the forthcoming

sections.

In section 4.2, this chapter explores the relation between public and private Chinese actors and how they are displayed in core Internet governance activities. The following section contextualises it in the framework of ICANN, whereas section 4.4 sets it in the framework of the IETF. Section 4.5 analyses the implications of the aspects explored in sections 4.2 through 4.4, while the concluding section 4.6 reconnects findings to theory.

4.2 *Chinese stakeholders' actions at the core of Internet governance*

Recalling from Chapter 1, a few turning points can be identified in the history of China's engagement in Internet governance since the foundation of ICANN in 1998. These can be summarised as the foundation of ICANN (1998), the WSIS process (2003-2005), WCIT-12 (2012), and the IANA stewardship transition (2014-2016). It is through the historical passage among these four milestones that the strengthening and weakening of multilateralist quests can be observed. While the extent to which WCIT-12 has been impactful on Internet governance history is debated, it is still referred to in literature as a key moment in which the multilateralist-multistakeholderist debate re-emerged (Palladino, Santaniello 2021).

To begin with, it can be noted that, despite constant growth of Chinese private stakeholders in the global market (Drahokoupil et al. 2017), China's governmental role has not faded away. After all, suspicions of party-political control on Chinese businesses, whether warranted or not, is a key element in the US-China trade war (Ciuriak 2019; Pupillo 2019). To be sure, the government is recognised to retain a strong regulatory and coordination role in China's domestic Internet market and its industrial policies influence companies' growth and development (Negro 2017; Shen 2016; Wen 2020; Zhang, Liang 2007). While the development of Internet infrastructure and policies has been strongly state-driven also through political control and

accountability of Internet Service Providers (ISPs) among other aspects, different layers of Chinese bureaucracy clashed throughout the 1994-1998 telecommunications market reform and after as they held different interests on the nascent Internet market. In turn, state-owned operators as well as private manufacturers displayed their own peculiar interests in the market (Negro 2017; Zhang, Liang 2007). While disquisitions on China's domestic dynamics fall outside the scope of this thesis, it is essential to pinpoint that, despite governmental multilateralist stances and suspicions over governmental control on private stakeholders, China cannot be considered a monolithic whole.

In the earliest stages of ICANN-based Internet governance, whereas China's government engaged in a boycott of ICANN meetings, which was gradually suspended between 2006 and 2009 (Creemers 2020a), commercial and other Chinese stakeholders kept participating in ICANN's activities. This was confirmed time and again by research participants involved in or familiar with ICANN, both from China, Europe, and North America. Many participants also confirmed a dialectical relation among the Chinese government and its domestic stakeholders in this phase. In an interview with a Chinese academic, discussing the relationship between the Chinese government and Huawei, it emerged that:

> *"In the dialectic, the government sometimes definitely has more power, [especially during Huawei's] early development. But on the other hand, Huawei became more and more powerful. As you can notice, Huawei's international revenue at one point [around 2010] was actually higher than its revenue in domestic China. So, Huawei has to balance its position as well, it certainly doesn't want to [forfeit] its people in the US, in Europe. It will try its best to make that market open to itself. So, sometimes Huawei will push back a little bit on state initiative to keep that market open."*

This interview statement finds confirmation in literature and publicly available data. Huawei's profits have increased despite the Trump administration's restrictions also thanks to the big size of China's domestic market, where it achieved a 37% share of the smartphone market in 2020

(Buchholz 2021). However, Huawei's presence in the global network and device market has historically been high, especially compared to other major Chinese actors, such as its direct domestic competitor, the state-owned ZTE. In 2013, Huawei's market share based on declared global LTE (4G) contracts was 39%, compared to ZTE's 2%. Huawei's share at that stage was higher than Ericsson's (31%) (Pawlicki 2017). Nevertheless, since 2017 US sanctions pushed Huawei to invert this trend, with its domestic revenues becoming higher and higher with respect to those deriving from the international market (Brown 2021).

In short, the power relation between Huawei and the Chinese government is likely transforming. While Huawei is only one key Chinese actor, albeit an economically and politically important one, these figures help to confirm the aforementioned statement. Aspects of such dialectic relation between public (including government and SOEs) and private actors in China will keep emerging throughout this chapter and the forthcoming ones. More recently, Chinese authorities clamped down on domestic big techs, arguably to strengthen political control on otherwise too powerful actors. While no action against Huawei has been taken at the time of writing, sanctions have been imposed on Alibaba, who participates as a registrar in ICANN's GNSO, and Didi (Zhong 2021). This situation is developing at the time of writing and falls outside the scope of this thesis. However, it must be acknowledged as it affects the aforementioned trend of growing domestic reliance for such companies as Huawei.

4.3 *Chinese stakeholders and multistakeholder governance at ICANN*

While full of unknowns, the dialectic among public and private actors described in the previous section must be acknowledged as it makes China's country-level stance towards multistakeholderism more nuanced and ambiguous than often depicted. However, the role of the central government

remains powerful. Observations on this will be further illustrated in the forthcoming sections.

To begin with, following the establishment of the WSIS process, China accepted the consolidation of multistakeholderism. Such consolidation came from three elements that characterised the conclusion of the 2003 and 2005 rounds of WSIS. First, this UN-sponsored initiative incorporated in its final document, the Tunis Agenda, a multistakeholder definition of Internet governance as provided by WGIG (2005); second, it launched a UN-sponsored non-decisional multistakeholder process called Internet Governance Forum (IGF); third, it did not replace ICANN, which on the contrary maintained its role and characteristics, including its formal link to the US DOC at this stage (Mueller 2017; Palladino, Santaniello 2021).

While China's re-accession to GAC following the consolidation of multistakeholderism in the WSIS process could be read as a (partial) acknowledgement of the latter principle from China's part, observers hinted at China as a 'repressive multilateralist' following WCIT-12 (Glen 2014). Concerns over the increasing (geo)politicisation of the Internet grew in this context, but some scholars warned against the excessive militarisation of Internet governance that could derive from framing it in terms of 'digital cold war' and cybersecurity (Mueller 2013). True, the Chinese government was among the supporters of the new ITRs, which were ostracised by the US-led bloc as too 'government-empowering'. However, the approval of the new ITR happened through majority vote rather than consensus and made the regulations inapplicable as supporting countries were too few and too economically weak (Palladino, Santaniello 2021).

Furthermore, the forecasted geopolitical divided did not materialised in the form of a new 'Cold war' as the following year, 2013, China hosted in Beijing the biggest ICANN meeting ever recorded until then, with the Chinese government participating in it. While this was the second China-hosted ICANN meeting, the first one did not record the Chinese government's participation. Held in Shanghai in 2002, this first China-hosted ICANN meeting took place at the beginning of China's ICANN boycott on the recognition of Taiwan's status

in the GAC. Therefore, the meeting was planned, held, but not participated in by Chinese governmental representatives as the boycott had meanwhile commenced. However, Chinese non-governmental stakeholders, including the state-sponsored NGO Internet Society of China (Negro 2017) and future ICANN Board member Qian Hualin, were present (ICANN 2002).

Furthermore, Chinese authorities coordinated with ICANN amid China's pre-emptive actions on the IDN space that led to the running of a system of Chinese-character domain names parallel to the ICANN-supervised DNS – an aspect solved at a later stage with a mix of domestic regulation and acceptance of the *fait accompli* on the ICANN side that acted accordingly (Arsène 2015). While this is described in more depth in Chapter 3, what matters in this context is that the 2002 and 2013 ICANN meetings held in China show that Chinese stakeholders' engagement with ICANN was always in place, even in times of major strain. The presence of state-sponsored stakeholders at the 2002 meeting despite China's government's boycott showcases China's will to retain links to ICANN despite diplomatic issues. In an interview with the author, Paul Twomey, ICANN's President from 2003 to 2009, confirms that dialogues between ICANN and Beijing and ICANN and Taipei were always on-going and officials on both sides of the strait kept contacts. Indeed, this research participant maintains there never was such thing as a fully-fledged break with ICANN on China's part, contrary to what is often found in literature (Creemers 2020a). As recalled above, the Chinese government's leadership finally re-accessed the GAC, after agreement was found on naming Taiwan 'Chinese Taipei' (中华台北, zhonghua taibei). Furthermore, agreement was achieved on referring to territorial entities in the Asia-Pacific region as 'economies', rather than 'states' or 'countries', to avoid sensitivities on territorial disputes (Scholte 2017).

A similar dynamic was in place following WCIT-12 in ICANN-China relations. This time, despite militaristic claims on the future of cyber-geopolitics, the Chinese government continued in its engagement with ICANN and the multistakeholder model. After the 2013 Beijing meeting, China

participated in NetMundial in 2014, the multistakeholder forum sponsored by the Brazilian government in the wake of the PRISM scandal. NetMundial represented a peculiar phenomenon: while declaredly multistakeholder, it was aimed at calling for a non-US centric form of Internet governance (Belli 2015; Hurel, Santoro Rocha 2018). In the same year, Lu Wei, then director of the Cyberspace Administration of China (CAC, 国家互联网信息办公室 guojia hulianwang xinxi bangongshi), a regulatory authority, participated in ICANN's fiftieth public meeting (ICANN50), publicly endorsing multistakeholderism in his speech. While these commitments are rhetorical, research participants familiar with the process believe they resulted from and represented a deeper engagement of China with ICANN and multistakeholderism. While Lu Wei's speech and China's participation in NetMundial took place at the outset of the IANA stewardship transition, short after the end of the transition that took place on 30 September 2016, China's governmental representative obtained GAC's vice-presidency (Negro 2020).

Nonetheless, this has thus far not translated into more influential Chinese policy engagement in ICANN. While this is difficult to quantify as GAC is a purely advisory body working on a consensual basis (Galloway 2015), thematic document analysis provided insight on it.

Between ICANN 54 and ICANN 56 (autumn 2015 to summer 2016), a key moment in the IANA stewardship transition, GAC Communiqués and meeting transcripts show Chinese input in post-transition ICANN reform has been welcomed by various parts, including Latin American and European countries such as Argentina, Brazil, Norway, and France. In particular, these countries' governments opposed the so-called 'Stress Test 18' and pushed for a two-third majority of the ICANN Board vote to be needed for the latter to reject GAC Consensus Advice. Stress Test 18 was a major point of discussion for GAC during the IANA stewardship transition and the subsequent reform of ICANN Bylaws. Stress Test 18 was based on the following working hypothesis:

> *"Stress Test 18 is related to a scenario where ICANN's GAC would amend its operating procedures to change from consensus decisions to*

> *majority voting for advice to the ICANN Board. Since the Board must seek a mutually acceptable solution if it rejects GAC advice, concerns were raised that the ICANN Board could be forced to arbitrate among sovereign governments if they were divided in their support for the GAC advice. In addition, if the GAC lowered its decision threshold while also participating in the Empowered Community, some stakeholders believe this could inappropriately increase government influence over ICANN"* (Cross Community Working Group on Accountability 2016, hereafter CCWG-Accountability).

Based on this, the CCWG-Accountability proposed that the threshold for the Board to reject GAC Consensus Advice be 60%, which in the sixteen-voting-member ICANN Board translates as one less vote than requested by China and the other opponents of Stress Test 18.

China was particularly vocal on this topic at ICANN 54 (October 2015), when the issue was debated in a GAC meeting with the Board. Here, France tabled a question on the rationale for the Board supporting the CCWG-Accountability bylaw reform proposal based on Stress Test 18. The Board's response received the following reaction from Russia:

> *"We believe the conditions under which accountability is enhanced but the role of governments is diminished, that condition is not acceptable. We had been talking about it from the very beginning. And so we can't support stress test 18 and we don't think that it has a place here"* (Governmental Advisory Committee 2015a, 33, hereafter GAC).

Russia's reaction was backed by China, who shared "the same viewpoint made by Argentina, Brazil, Russia, and many other countries", including France, who restressed unsatisfaction over the Board's arguments in favour of Stress Test 18 (GAC 2015a, 33-35). Despite concern being raised by governments cutting across the usual geopolitical lines, the reformed ICANN Bylaws as entered into force in October 2016, following the completion of the IANA stewardship transition, featured the 60% threshold proposed by the CCWG-Accountability.

These aspects confirm the low-profile presence of China in the GAC as

reported by interview participants, which has grown to obtain formal and active roles, but has not necessarily become influential. A similarly low profile is found elsewhere in ICANN for Chinese stakeholders. An interview conducted with a Chinese ICANN staff member confirmed that, while China's increasingly active participation in ICANN can be observed, Chinese stakeholders' activities have not become particularly prominent with regard to policy-making. According to this research participant, this probably results from China's more complex ecosystem and its later involvement in ICANN. Furthermore, an academic familiar with the internal work of ICANN restressed in an interview with the author specific rhetorical aspects that hint at China's growing engagement and acceptance of ICANN at the apex of the IP and DNS governance ecosystem: while China maintained a relatively low profile throughout the IANA stewardship transition, this interview participant stressed the importance of the aforementioned speech by the then-head of CAC Lu Wei at ICANN 50 in 2014 and the appointment of China's representative GAC Vicechair right after the completion of the IANA stewardship transition. While observing no major growth in terms of strength of Chinese actors in ICANN in recent years, this participant finds that these episodes signal growing acceptance of the forum by the ICANN-involved Chinese Internet governance community. This is further demonstrated in literature: Jongen and Scholte (2021) found that ICANN is mostly perceived as a legitimate within the ICANN community and this involves Chinese participants.

Finally, it must be stressed that Chinese participation being mostly low-key does not entail inactiveness. While Chinese participation is not numerous and a group of participants finds that Chinese impact on ICANN policy-making is relatively low, in an interview an ICANN staff members stressed Lu Wei's constant activeness in informal settings during the IANA stewardship transition on behalf of the Chinese government. In this participant's words:

> *"In those years there was a strong diplomatic action with the Chinese government: bilateral meetings, including high-level and ministry-level ones. […] [Lu Wei] met with the then ICANN president to stress China's interest that ICANN go on with this independence process:*

ending the [IANA] contract and restructuring the governance model by changing ICANN's Bylaws."

In short, this participant stresses that China's government did engage in the IANA stewardship transition and carried an influence, while not being necessarily prominent in GAC.

To conclude on this aspect, China's relationship to ICANN has surely improved throughout time, evolving from straightforward confrontation in the early 2000s to Lu Wei's endorsement of ICANN and Guo Feng's vice-presidency of GAC. To this, growing engagement on selected policy issues, such as internationalised domain names (IDNs), must be added (Zhang, 2019).

However, a degree of ambiguity in relation to ICANN and multistakeholderism remained. For example, Negro (2020) finds China's multilateralist challenge to ICANN has not faded away. Research participants confirm Chinese presence has grown in the ITU, as demonstrated by the appointment of Zhao Houlin as ITU Secretary. In an interview with the author an ICANN staff member stresses that this is not to be read necessarily as a confrontational move towards ICANN. In a way, China is simply leveraging one forum against the other to put pressure for reform, but on the other hand ICANN-ITU relations improved under Zhao Houlin as ICANN has become a member to the ITU-D and the two started joint capacity-building initiatives. Nevertheless, initiatives such as the 'New IP' project, which is better discussed below, periodically cast ambiguities on China's stances on multistakeholderism.

Briefly, ambiguity remains, but overall Chinese stakeholders do not aim to replace a governance model that allows them to participate and 'forum-shop' to enhance their influence.

4.4 *Chinese actors and the IETF: public-private relations in standard-making*

Contrary to ICANN, the IETF allows for assumptions to be made based on publicly available quantitative data. As Arkko (2021) shows, Huawei is

currently the second main contributor to the IETF in terms of RFCs yearly authored by its affiliates, right behind Cisco. However, the former does not have the latter's longstanding experience in the IETF. Instead, Huawei started featuring increasingly prominently in RFC-related figures in 2007. Meanwhile, between 2007 and 2010, Chinese nationals' participation in the IETF spiked in terms of number of RFCs and Internet Drafts authors, remaining relatively steady at the 2010 level thereafter (Arkko 2021). On a clarification note, Chinese nationals' participation and Chinese companies' participation do not go hand in hand. It goes without saying that Chinese nationals may work for non-Chinese companies and Chinese companies may employ non-Chinese nationals. Notwithstanding this, the synchronism of Huawei's escalation in IETF participation and the increasing number of Chinese RFC and Internet Drafts authors is an interesting aspect.

As research participants often pointed out, initially Chinese companies participated in such technical bodies as the IETF through their Western technologists, often hired in consultant positions. This was deemed helpful to overcome both linguistic and cultural barriers that could have posed obstacles to engineers' work. However, as Chinese companies' participation increased, so did the participation of Chinese engineers employed by domestic Chinese companies. Many research participants familiar with the work of the IETF, whether technologists or not, see it as symptomatic of a growing socialisation of Chinese companies and their engineers into the rules and modi operandi of the IETF and other technical bodies. A similar process was in fact observed in 3GPP.

Therefore, 2007 represents a turning point. While identifying the drivers of such timing is complicated, hints can be found in the business orientation of Huawei as a device and mobile network manufacturer. To begin with, by 2007 China had not rolled out 3G yet (Stewart et al. 2011; Zhang, Liang 2007). This posed the country in a condition of backwardness compared to Europe and the US, with the then Europe-led 3GPP setting the scene for 4G standardisation already in 2008 (3GPP 2021a). While this displayed a strong role of the central government, which slowed down the process of implementation in order to

protect the home-grown 3G standard, it also gave private manufacturers a push towards penetrating foreign markets. Accordingly, this is seen as one reason behind Huawei's timings in the global market (Zhang, Liang 2007), and arguably in global standardisation fora, too. Huawei's first infrastructural contract in Europe was signed in 2005 (Huawei 2021) and the beginning of its participation in the IETF was in 2007, right when the deployment of the new version of the Internet Protocol (IPv6) began stepping up and work on 4G standardisation was about to begin at 3GPP (3GPP 2021a; Internet Society 2017; Wen 2020). Right in the same year, Huawei deployed its first all-IP mobile network in Germany (Huawei 2021).

To be sure, mobile Internet is not a central topic in this chapter, as it will be addressed in Chapter 5. Nonetheless, being Huawei a network manufacturer as well as China's 'giant' within the IETF, observing developments in the mobile infrastructure and device market helps to interpret its policy choices and those of the stakeholders it relates to.

Briefly, in this phase both the market needs of Huawei and state policies played a role in Huawei's internationalisation. In Wen's (2020) account, Huawei's internationalisation push was both state policy and a market need. In terms of state policy, Huawei was identified as a strategic company in a 2005 national funding plans for internationalising Chinese ICT industry, while in terms of market needs the aforementioned domestic 3G impasse pushed Huawei to seek international markets along with the high domestic competition with SOEs and foreign competitors. US and European manufacturers and carriers had in fact gained a strong position in China's domestic market before Chinese companies such as Huawei and ZTE gained their current size and position.

In other words, the historical phase between the end of the WSIS process reaffirming multistakeholderism as a governance principle in 2005 and the reawakening of the multistakeholderist divide in 2012 sees an increased presence of Chinese stakeholders, mainly Huawei, in the European market and in standardisation bodies like the IETF. The main drivers behind Huawei's choices appear to be market-based, as illustrated in the previous paragraph,

despite important doubts remaining about the central government's effective control on domestic actors (Pupillo 2019). While Chinese corporate actors were growing active in the IETF, China's government rebuilt relations to ICANN and became more participatory in GAC. Meanwhile, further Chinese stakeholders engaged in ICANN too, albeit maintaining a relatively low profile. Indeed, a governmental role in Internet policies is acknowledged by the literature and was confirmed by most research participants (Negro 2017; Tang 2020). Nonetheless, evidence of direct control allowing government and private companies to be treated as a monolithic whole did not emerge in conversations with technologists familiar with 3GPP and the IETF. The more Chinese companies globalise and gain a leadership role, the more the state-company dialectic evolves (Shen 2016), with instances of strong coordination and instances of reciprocal criticism (Shih 2015). However, this is a rapidly evolving situation. As mentioned above, sanctions related to the technological competition between the US and China forced Huawei to redirect its effort towards the Chinese domestic market, which after 2017 became its main source of revenues, whereas before Huawei mainly earned income overseas. The difference between the increased reliance of Huawei on China's domestic market and its decreased revenues overseas became prominent since 2019, with the Covid-19 pandemic potentially playing a role (Brown 2021).

Going back to Chinese stakeholders' role in the IETF, the phase following WCIT-12 and the PRISM scandal, up to the IANA stewardship transition, did not have a direct influence on the IETF according to most research participants. The mode in which IETF work is conducted remained similar. To be sure, the IANA Stewardship Transition Coordination Group (ICG) was established, followed by a working group called IANAPLAN. However, their role was mainly to ensure that the transition affected IETF work and IETF's relation to ICANN as little as possible. At the time of IANAPLAN's launch, an email communication by the working group's chair retrievable from the IETF's public mail archive stated that

> *"[t]he system in place today for oversight of the IETF protocol registries component of the IANA function works well. As a result,*

> *minimal change in the oversight of the IETF protocol parameters registries is preferred in all cases and no change is preferred when possible. […] This working group is chartered solely with respect to the planning needed for the transition, and is not meant to cover other topics related to IANA. Possible improvements outside that scope will be set aside for future consideration. However, the mechanisms required to address the removal of the overarching NTIA contract may require additional documentation or agreements. The WG will identify, but not create such required agreements"* (Internet Engineering Steering Group 2014, hereafter IESG).

To summarise, while the IETF did follow the IANA stewardship transition owing to its ties to ICANN in the regime complex, the transition itself did not influence the IETF's modus operandi nor the internal relations among actors.

Difference, however, is visible in the influential role played by Chinese stakeholders in IETF work. The three IETF working groups analysed in Chapter 3 show increased Chinese presence and even centrality and pre-eminence of affiliates of Chinese corporations in the working groups. Observing the RFCs authored within idr, 6man, and alto in the same timespans analysed in Chapter 3[1], further observations can be made. Strikingly, no single RFC was co-authored by Chinese actors' affiliates in idr for the 2007-2008 timespan, but two of the four RFCs published within the same WG between 2018 and 2019 are co-authored by Huawei and Cisco affiliates, along with affiliates from smaller companies (Ginsberg et al. 2019; Previdi et al. 2019). A third RFC, authored by Arrcus and Cisco affiliates, has been reviewed by the Huawei-affiliated idr chair Susan Hares, among others (Bush, Patel, Ward 2019). As illustrated in Chapter 3, Huawei's activeness in the mailing list has grown and Huawei affiliates hold central positions in the network, including

[1] Recalling from Chapter 2, the selected timespans are June 2007 to June 2008 and June 2018 to June 2019 for idr and 6man. For alto, the selected timespans are November 2008 to November 2009, June 2018 to June 2019, and January 2020 to December 2020.

formal responsibility roles in the WG. Along with this, authorship in RFCs shows growing activeness in standard-making from Huawei's part. This is not homogeneous, however. In 6man, no RFC has been authored by Chinese companies' affiliates in the given timespans. Furthermore, the 2018-2019 timespan saw only two RFCs coming from the 6man WG, one of which is a Best Current Practice (BCP) RFC. This signals a general pattern of lower engagement in 6man from the broader IETF community. Conversely, alto represents a peculiar case, as illustrated in Chapter 3. Dormant in terms of produced documents between mid-2018 and mid-2019, it saw three standards-track RFCs published in 2020. One of these was co-authored by affiliates from Chinese companies, namely Huawei and China Mobile, along with affiliates from Thales Deutschland, Yale University, and Nokia (Randriamasy et al. 2020). Another one was authored by affiliates of Nokia and Yale University, but reviewed by Yale and Tongji universities' affiliates. Once again, cooperation among Western, including US, and Chinese actors emerges in the IETF despite East-West geopolitical divisions.

This is relevant because the then Trump administration impeded cooperation between Chinese companies and companies doing business with the US, as well as cooperation between Chinese and US companies in strategic research and development (R&D). This led other private US-based standard-making organisations to question the handling of Chinese companies' participation, with the Institute of Electrical and Electronics Engineers (IEEE) suspending Huawei's participation to certain activities for a short while in 2019 (IEEE 2019). Such difficulties seem not to have affected the IETF, where Chinese participation and co-drafting of RFCs between US and Chinese companies has continued.

Briefly, documents' authorship confirms the hints provided by network analysis in Chapter 3 on Chinese actors' growing centrality and presence in the network. While this is not constant and equal in every WG, Chinese RFC (co)authors are present and Huawei is the second main organisational RFC contributor after Cisco on a yearly basis (Arkko 2021), by far the most influential Chinese actor in the IETF. Many of the RFCs analysed here, as

presented within the selected WGs, have not made it to official standard status yet. As described in previous chapters, the basic reference for standard-making procedure in the IETF is RFC 2026 (Bradner 1996). It can take years before a Standard-Track RFC develops into a fully-fledged Internet standard and technology can remain in use without becoming a recognised standard in full.

In other words, Chinese stakeholders participate in the IETF conscious that the need for consensus makes cooperation with industry and technologists across geopolitical lines is a must. What instead reopened the multilateralist vs. multistakeholderist divide in the current historical phase is the presentation of the so-called 'New IP' proposal to the ITU's Telecommunication Standardization Sector (ITU-T). This proposal, then renamed 'Future Vertical Communications Network' (FVCN), was put forward in late 2019 by a group of actors including the MIIT, Huawei and two ISPs (Hogewoning 2020; Li 2020). Beyond media concern (Murgia, Gross 2020), the technical proposal has been subjected to criticism on a normative and technical level (Durand 2020; Hogewoning 2020; Mueller 2020a; Sharp, Kolkman 2020).

On a normative level, the question relates to the competence of the ITU and its state-based conformation in contrast to the private-based characteristics of the IETF, traditional 'home' of TCP/IP. The IETF being a private- and consensus-based decision-making body clashes normatively with the ITU's more state-centric characteristics (Flonk, Jachtenfuchs, Obendiek 2020; Sharp, Kolkman 2020). On a technical level, the proposal still lacks clarity (Mueller 2020a). While this is a new topic subject to constant evolution and lack of public information, this view was confirmed in interviews with the author as late as December 2020. Richard Li (2020, also in Mueller 2020b), one of the leading engineers behind the FVCN/New IP idea, did engage in public relations to promote and explain the rationale behind this technical project. While this helped to bring an extent of clarity, a common understanding among research participants from various backgrounds is that the New IP proposal is not meant to replace the existing IP versions, but rather to create an Internet architecture aimed at tackling specific technical problems emerged with new Internet-enabled technologies.

The final details and results of this technical initiative are beyond the scope of this thesis. What matters here is the debate on the nature of the Internet and the role of actors and institutions at the core of standard-making. According to an interview participant, the New IP/FVCN raises further normative questions related to the philosophy upon which the Internet has been built: one of building blocks rather than a fully-determined architecture, which instead reflects the way in which the telecom market, including mobile Internet technologies, has evolved. In other words, despite its initial name, the New IP is not a new proposed version of the Internet Protocol, at least in its current form given the available information (Durand 2020; Mueller 2020a, 2020b). Furthermore, the New IP proposal must be observed in the broader context of technical debates over the suitability of TCP/IP for new Internet-of-Things (IOT) technologies that need ultra-reliable connections and low latency, such as medical IOT. In this view, work on new forms of IP and non-IP networking is on-going at the IETF and the European Telecommunications Standards Institute (ETSI), too (Petrescu 2021).

As far as the potential replacement of TCP/IP in the near future is concerned, it must also be added that the existence of different, technically incompatible basic protocols is not new to the Internet ecosystem. The introduction of IP version 6 (IPv6) is exemplary: its elaboration started in the 1995 amid concerns that IP version 4 (IPv4) would exhaust its address space (IANA 2019). As DeNardis (2014) illustrates, IPv4 encompassed a total of 2^(32) IP addresses, that is, around 4.3 billion. Instead, IPv6 has a total of 2^(128) (undecillions) addresses. The assignation of the last addresses available in the IPv4 space by ICANN to a Regional Internet Registry (RIR) took place in 2011 (ICANN 2020). A few years before that, the development and implementation of IPv6 was accelerated, with a strong Chinese contribution as well (Negro 2020). Even though the complete replacement of IPv4 with full-IPv6 networks is nowhere in sight, the two IP versions have been made fully interoperable through ad hoc technical specifications (RIPE Network Coordination Centre 2020, hereafter RIPE NCC). Users seldom know what IP version is attributed to their network-connected devices and to the

devices they are interacting with.

Notwithstanding this, a number of research participants with technical, academic and public-institutional backgrounds raised normative questions related to the New IP. Two of these emerged as particularly eminent: first, if this new technology is conceived for fulfilling an 'IP-like' role, it should be standardised at the IETF rather than the ITU. The former, other than being the traditional 'IP home', is a private- and consensus-based body, whereas the latter is a state- and majority-based one (Sharp, Kolkman 2020). Second, in an interview with the author, a senior technologist maintained that "there are clear indications that the New IP architecture would include controls to impede or redirect 'unwanted' traffic - as a security measure. Technical details about the design of those controls lack but we should be careful [to] make sure that they will not become censorship tools." Third, as mentioned above in this section, doubts were raised concerning architectural characteristics.

Notwithstanding these normative concerns, few research participants find it likely that the New IP (if implemented) will constitute an infrastructure unable to communicate with IP-enabled network-connected devices. The dominant position Huawei (and by extension China as a state) has achieved in 5G technology at the global level would suggest it is not in its interest to promote a non-interoperable basic protocol, as it would create major transaction costs on the device market: devices aimed at different markets would need to be developed to work through different protocols in different countries or areas of the world. In line with Mueller (2017), it is more beneficial for Chinese stakeholders to retain scale economies and enjoy network benefits by adopting universal standards, shaping them through IETF activity. This point of view was raised by most research participants and finds theoretical support in economic and regime-theoretic literature on transaction costs (Alter, Raustiala 2018).

In other words, the potential for the 'New IP' to be more disruptive than IPv6, in normative terms as well as in terms of technical fragmentation, has been pinpointed by some research participants from academia, the technical community, and governmental institutions. However, the lack of technical

detail as well as the interest of major Chinese stakeholders in keeping global scale economies in the device market make IP-related initiatives unlikely to technically fragment the Internet. To be sure, other normative aspects such as the choice to present a technical proposal containing 'IP' in its name to a multilateral body, as well as the unknowns around New IP's capacity to enhance online censorship, remain unaddressed.

As mentioned, the New IP/FVCN question is an ongoing one, detail lacks, and there is no guarantee it will become an implemented technology at the time of writing. What matters in this is the role this proposal plays in portraying the ambiguity of Chinese actors' engagement in multistakeholderism.

4.5 *What is at stake?*

What is at stake for the future of the Internet given the conditions discussed above in this section? A key takeaway is that China has little interest in fragmenting the Internet at the technical level. This is strengthened by Chinese stakeholders' increasing integration in the multistakeholder model: it would go against their self-interest to disrupt a governance architecture that allows them to grow influential on a global scale. To be sure, there may be groups within the Chinese Communist Party (CCP) or smaller private or state-owned actors with an interest in a more closed 'national' Internet. Nonetheless, with Huawei becoming a major player in 3GPP and the IETF, technical fragmentation would go against China's economic and Huawei's business interests. In literature, this is confirmed by Mueller (2017), who stresses the centrality of network benefits of a technically unified Internet.

While China has progressively integrated into multistakeholder governance (ambiguities notwithstanding) and is not pushing for a technical fragmentation, the question of alignment is at stake. By 'alignment', Mueller (2017) refers to the process undertaken by governments to control 'what goes on' on the Internet, that is, the data and information fluxes to which citizens

and organisations have access from within the territory. In other words, Mueller (2017) sees a general trend from governments to 'align' the Internet to domestic regulation. Examples of this are not only found in China or autocratic states, but also in liberal democracies. The US's 'Clean Path' initiative has been identified as a fully-fledged attempt to splinter the global Internet. In Mueller's (2020c) words, it aims "to leverage US information services providers to force the rest of the digital economy to indiscriminately exclude Chinese businesses". Two important aspects emerge from this. First, fragmentation is not an 'East vs. West' question. Second, a commonly accepted threshold of what constitutes 'fragmentation' is not set (DeNardis 2016; Drake, Cerf, Kleinwächter 2016; Mueller 2017). Mueller's (2017) account of alignment adds to and anticipates a growing corpus of literature on digital sovereignty and the return of state in Internet governance (Haggart, Scholte, Tusikov 2021).

Analytically, it emerges from interviews that Chinese authorities are more prone to controlling the domestic Internet ecosystem at the regulatory level, while allowing for network benefits to be enjoyed at the technical one, empowering market actors to 'go global'. The Golden Shield Project (金盾工程 jindun gongcheng), also known as the 'Great Firewall of China', is a good example of it (Negro 2017), as it makes sets of information inaccessible without adopting separate basic protocols. What is interesting in the Golden Shield Project is its scalar implementation as China became more integrated in the global market and the world's digital economy. Launched in 1998, the project was completed ten years later (Negro 2017), that is, when China's 3G network was rolled out, granting expanded Internet access to at least a portion of the population (Stewart et al. 2011). Furthermore, it is at this stage that Huawei started enhancing its active participation in the IETF (Arkko, 2021), amid delays in domestic 3G rollout (Zhang, Liang 2007). This was followed by the Facebook and Google bans in 2009 and 2012 respectively (Quinn 2012; Wouters 2009). In the latter case, it was only the browsing service that was banned, while the company maintains offices in mainland China at the time of

writing and redirected its servers to Hong Kong (Google 2021). When China banned WhatsApp in 2017 (B. Haas 2017), the development of 5G was already launched, with Huawei poised to become one of the main contributors to the global 5G specification (Pohlmann, Blind, Hess 2020). In this context, Chinese companies developed alternative platforms, with WeChat playing the role of both WhatsApp and Facebook in its being a mobile and desktop app performing platform and private messaging functions – other than a set of further services such as payments.

This aspect was addressed in interviews. Research participants familiar with the Chinese Internet ecosystem pinpoint that WeChat's success in domestic China (where it is known as 微信 weixin) was already higher than WhatsApp's earlier than 2017. This suggests that, censorship notwithstanding, WeChat created a business model more successful in intercepting the taste of Chinese users. After all, Shen (2021) stresses that the Golden Shield Project, other than having political objectives, plays an economically protectionist role to shield the domestic platform industry from competition with Silicon Valley giants. While this falls outside the scope of this thesis, it is worth underlining that forms of geographical or linguistic content 'fragmentation' (definition notwithstanding) can take place autonomously in cyberspace. These can be leveraged for political reasons and reinforced through acts of censorship such as those described above in this paragraph, but they do not constitute fragmentation inasmuch as they remain accessible to users elsewhere.

A further, technical element need be added when talking about political control on the Internet in China and its influence globally. While it is true that censorship takes place domestically through technical tools working at a higher layer than such universal standards such as TCP/IP and the DNS, which are still in place, it must be stressed that the physical Internet infrastructure of China is strongly built within China's geographical borders (Allen 2019). This adds to strong data localisation policies that are constantly developing (Liu 2020).

These elements complicate the debate on fragmentation further. To what

extent can a strongly censored online environment, built upon an 'almost-domestic' Internet infrastructure, be considered part of the global Internet, although it deploys the same basic standards? This thesis argues that keeping the infrastructure as much as possible within the country's geographical border is part of the process of controlling conducts on the Internet rather than a form of technical split. In fact, such platforms and services as Google and Facebook are technically accessible with a Virtual Private Network (VPN). This confirms that the Chinese government sees an advantage in letting its domestic industry benefit from scale economies and network benefits by deploying global standards for devices to function, while maintaining strong control on societal activities over the Internet. Further elaboration on the meaning of fragmentation and its conceptual borders will be provided in Chapter 6 based on this empirical research.

To conclude, the stronger China and Chinese stakeholders have grown, the more they have become involved in the existing multistakeholder Internet governance ecosystem, as the presence of major domestic actors among the biggest competitors in the digital market, including sensitive sectors such as mobile Internet architecture, makes it disadvantageous to create technical splinters. At the same time, to cast control over what takes place in the domestic cyber-sphere, China opted for forms of information and regulatory control, while maintaining the Internet intact at the technical level. In other words, the more China grew involved in technical Internet governance at the global stage, accepting existing organisations and institutions such as the multistakeholder principle, ICANN and the IETF, the more it strengthened control on online activities domestically: from the implementation of the Golden Shield Project to banning Google, Facebook, and later WhatsApp in 2017 as illustrated above (B. Haas 2017).

While the author found little disagreement among research participants on Chinese stakeholders' interest not to technically split the Internet, phenomena at the societal, informational level yielded more disagreement. First and foremost, there is no agreement on what constitutes fragmentation. At the user level, many believe the Internet was born fragmented, though not along

national boundaries, as different user constituencies use different platforms and information sources. Furthermore, other maintain an extent of separation is to be expected, censorship notwithstanding, as different linguistic groups will access sources, platforms, and contents in different languages, creating separate user bases. Second, it could be argued that that governmental control in terms of information and data movement is also enforced through technical tools: for example, by detecting and rerouting data packets with particular forms of encryption. However, this principle is similar to the Golden Shield's and entails no fragmentation of the basic protocols. In Mueller's (2017) account, this constitutes alignment inasmuch as it entails control on Internet-related activities through state regulation.

4.6 *Conclusion: back to theory*

From the perspective of norm entrepreneurship, Chinese actors are maintaining a degree of ambiguity in their engagement in Internet governance which allows them to be influential in a wider variety of fora (Negro 2020). For example, presenting the 'New IP' project at the ITU in a context of increased influence in that venue can be read as forum-shopping, that is, the practice of taking topics off the competence of a given forum and shift it to another as a technique of policy or norm negotiation (Hofmann 2019). In regime-complex terms, while different bodies have different competences, their loose interdependence allows corporate and state actors to turn to other venues to try and push one's technology into the global standard. This increases actors' capacity for political contestation, thus allowing different actors to act as norm entrepreneurs. In the 'New IP' case, presenting a technical proposal carrying 'IP' in the name to a multilateral body that had been protagonist of anti-ICANN contestation in the past can be read as a political signal. Notwithstanding the normative element of this, many interview participants hinted at Chinese actors' strategizing: a reason for presenting the 'New IP'

proposal at the ITU is that it resembles much more a telephony infrastructure than the Internet one as illustrated above. In this case, the ITU would be an adequate standardisation forum for a technology that would not replace IP as we know it but would build a form of non-IP connectivity for IOT.

However, 'New IP' represents an ongoing project and a shifting target at the time of writing, thus not allowing strong theory-building. What matters here is the interest element behind the choice. On a more cognitivist ground, it emerges that Chinese stakeholders' interests have transformed in light not only of domestic public-private relations, but also through interaction with other actors within ICANN, the IETF, and the ITU itself. As it became apparent that ICANN was there to stay and that IETF norms and rules are rigid due to consensus being needed for standard-making, Chinese actors stepped up their participation in such venues. As illustrated above in this chapter, it is not just the consolidation of the (ICANN-centred) multistakeholder global Internet governance mechanism in the wake of WSIS that triggered Chinese actors' acceptance of such fora, but also contemporary technological innovations such as the beginning of 4G development internationally, 3G deployment in China, and an up-step in IPv6 implementation. In this process, many interview participants pinpoint Chinese actors initially hired Western technologists to participate in such fora as the IETF. As the IETF was founded in the US and was historically US- and Western-dominated, this way Chinese companies hired technologists who were already culturally and professionally aware of IETF practices. Therefore, Chinese actors (mainly companies, in this context) internalised and reproduced working practices so to be more effective within the IETF, to the point that nowadays they participate through Chinese-born and Chinese-educated technologists who are fully-fledged, effective IETF participants.

Briefly, as made explicit in Chapter 2, rational interest and cognitive dynamics go hand in hand, the latter complementing the former by providing a theoretical ground for interest formation. In this, however, Chinese actors see an interest in participating and carrying weight in as many governance fora as possible, maintaining a degree of ambiguity that allows them to forum-shop

(Negro 2020), but see interest in maintaining the existing fora in place as they can influence decision-making through the existing rules. In other words, the norm-entrepreneurial effort of Chinese stakeholders features instances of contestation through such practices as forum shopping, but also instances of adaptation to the existing normative architecture. This bases on matters of incentive and constraints at the market and political levels, but also on a learning process of socialisation through which Chinese stakeholders have familiarised with the governance processes in question and the way to influence rule- and standard-making.

Interpretively, one can see elements of continuity in China's government-led contestation against ICANN. However, the straightforward contestation experienced in the early 2000s has faded and what remains now is that form of ambiguity illustrated above. Conversely, elements of continuity are found in Chinese stakeholders' participation in ICANN, too. Even the years of China's strain and non-participation in GAC saw Chinese public, private, and state-sponsored groups and subjects participating in ICANN. In the IETF, Chinese actors became active participants in 2007, when Huawei's participation started growing until becoming the second most prominent corporate actor per RFCs published by its affiliates (Arkko 2021). The mix of policy and market drivers (and constraints) that pushed Huawei's action in its early years in the IETF has been illustrated above in this chapter. They entail market constrictions domestically, but also an economic and political need for stronger influence in standard-making both in the Internet standard-making and in telephony, with Chinese stakeholders' role in 3GPP being analysed in the next chapter.

Overall, what matters in this theoretical section is that ICANN and IETF rules and norms are rigid. Consensus (or supermajority, in many ICANN SOs cases) is needed in decision-making, which makes it difficult to influence an organisation's policies without forms of compromise. This is also due to the voluntary and scalable nature of the technologies in question. This creates forms of regime resilience, strengthened by elements of technological path dependence. In this context, Chinese stakeholders preferred to carry influence within the existing fora following existing rules rather than pushing for

normative shifts. As Chinese stakeholders grew more economically powerful, they found it more advantageous to step up participation and influence decision-making in such fora as ICANN and IETF, while retaining presence and influence in the ITU, where the current Secretary General is a Chinese national at the time of writing.

Amid normative rigidity and the institutionalisation of the ICANN-centred multistakeholder Internet governance model that followed WSIS, Chinese stakeholders adapted to the existing norms and rules of Internet governance at ICANN and the IETF rather than adapting such rules to their interest. This happened amid market and policy pushes as illustrated above and involved a learning process by Chinese stakeholders, who internalised expertise on the working culture and mechanisms of such bodies as the IETF by hiring experienced Western personnel from other companies before enhancing their participation through Chinese-born staff members educated in China and/or in the West. Chinese stakeholders' adaptation to the existing rules and norms was visible during the IANA stewardship transition, too. Rather than pushing for the outright replacement of ICANN, which would have been the expected stance given China's government's historical support for multilateralism (Flonk, Jachtenfuchs, Obendiek 2020), the Chinese government played a key – albeit low-profile – role in pushing for the transition, rendering ICANN as autonomous as possible from the US government.

To be sure, some interview participants believe that the transition is still insufficient for China, who is still on a challenging position with regards to ICANN. This is also found in literature and confirmed above in light of China's ambiguity at the ITU. Nonetheless, the historical process of China's engagement in the ICANN-centred multistakeholder governance model is one of further acceptance and adaptation the more China and its domestic stakeholders grew capable of influencing decision-making.

On the 'fragmentation' side of this thesis' research questions, a few statements can be made. First, conceiving fragmentation as a technical split that creates two separate and non-communicable networks, this chapter shows that Chinese actors have interest in maintaining the Internet universal.

Producing different devices for different markets using different protocols to connect to the Internet hampers technological scalability and Chapter 4 shows that a convergence in standard is present elsewhere, too, not only in critical Internet resources. Applying Mueller's (2017) definition of fragmentation, Chinese stakeholders maintain an interest in pursuing network benefits. To maintain political and social control on the Internet, the Chinese government opts for censorship tools acting at a higher level than basic Internet protocols, along with regulatory instruments. In other words, China engaged in a process of alignment of the Internet to domestic regulation that dates back at least to the implementation of the Golden Shield Project and allowed it to control information fluxes and promote the growth of domestic platforms alternative to the Western ones, which played both a political and economically protectionist role (Shen 2021). This aspect of domestic regulatory alignment is addressed to a deeper extent in Chapter 6.

To summarise and conclude, the rigidity due to the need for consensus in Internet standard- and policy-making, along with the need for scale economies and network benefits, pushed Chinese stakeholders to adapt to the existing rules and increase their influence within the given institutional and normative settings. The more Chinese actors became capable of influencing ICANN and IETF work, the more they became participatory in it. At the same time, the more Chinese public- and private-owned actors became influential globally, the more the Chinese government pushed for a process of alignment domestically (Mueller 2017). The Golden Shield Project, carrying out both a political task and a protectionist one to shield Chinese companies from Silicon Valley competition (Shen 2021), has been enhanced to censor Facebook, Google, and then WhatsApp in three different moments as China became more prominent globally and more present in standard-making and Internet governance. This shows a process of adaptation of Chinese companies to existing norms.

To be sure, this cannot be taken as to entail full normative acceptance. Ambiguities persist both in China's behaviour among ICANN, the IETF, and the ITU (Negro 2020), and in official documents. In its 2017 International Strategy of Cooperation on Cyberspace, China expresses support for a

multilateral governance with multi-party (multistakeholder) participation, an important ambiguity in the formulation. At the same time, it must be stressed that this document refers to a broader scope of governance than critical Internet resources strictly speaking, and it endorses the push for ICANN reform without ever rejecting its role (Ministry of Foreign Affairs of the PRC 2017).

Nonetheless, there is a general acceptance of the persistence of such bodies as ICANN and the IETF in their existing form and recognition of the advantage of participating in them.

CHAPTER 5

ON THE NORMATIVE IMPACT OF CHINESE STAKEHOLDERS IN MOBILE INTERNET STANDARD-MAKING. A DOCUMENT- AND INTERVIEW-BASED ANALYSIS[1]

5.1 *Introduction*

The question of mobile Internet connectivity has been increasingly politicised and reached high media coverage amid the US-China technological competition that peaked under the Trump administration (Ciuriak 2019). Such hype contributed to confusion over the topic, with outcry for the risk of Internet fragmentation (Tayal 2021). True, the development of 5G, the latest generation of mobile Internet connectivity, imposed new pressure on the functioning of core Internet protocols. By allowing increasing IoT-related connectivity, new problems of latency have emerged in relation to TCP/IP-based data transport, affecting critical IoT services such as those for remote surgery, requiring reliable connectivity and low latency. This has pushed standardisation bodies and companies to work on connectivity mechanisms alternative to IP, with geopolitical conundrums attached when it comes to such things as Huawei's 'New IP' proposal illustrated in Chapter 4 (Hogewoning 2020). Furthermore, these same developments are yielding overlaps and interdependency between telephony and Internet infrastructures inasmuch as the former are all-IP and allow Internet-based connectivity of new devices, with further implications for the configurability and security of the network according to sectors of the literature (Ten Oever 2020).

As illustrated in Chapter 1, the work of 3GPP does not fit the

[1] Part of the content of this chapter has been published as: Nanni, R. 2021. "The 'China' question in mobile Internet standard-making: Insights from expert interviews", *Telecommunications Policy*. 45 (6): http://dx.doi.org/10.1016%2Fj.telpol.2021.102151.

multistakeholder framework in a straightforward manner, although it goes along the same pattern of private-based governance of technological resources and standard-making related to scalable technologies. What is more strictly connected to the geopolitics of 5G amid growing restrictions against Huawei is a form of market fragmentation, whereby some countries may open markets to Western or Chinese companies exclusively along geopolitical lines (Poggetti 2021). Conversely, a trend towards harmonised mobile Internet standards is visible.

These aspects will be explored within this chapter proceeding in historical order. Sections 5.2 through 5.4 explore the drivers and dynamics of Chinese stakeholders' engagement in mobile connectivity standard-making in 3G, 4G, and 5G respectively. Section 5.5 builds on the empirical analysis in the previous sections to address the normative implications of Chinese stakeholders' transformation in their engagement with standardisation. Finally, section 5.6 draws conclusions.

5.2 *Road to 3G: domestic constraints, market drivers, and Chinese stakeholders' early engagement in 3GPP*

A few aspects related to the market conditions in China, as well as the relationship between Chinese state and companies, have been illustrated in chapters 3 and 4, hinting at the connection between Chinese stakeholders' international engagement in Internet standard-making and in 3GPP. After all, the main Chinese companies in terms of contributions to standardisation in both fields are Huawei and ZTE followed by others (Arkko 2021; Pohlmann, Blind, Hess 2020), which shows a connection between the two areas when it comes to companies' strategies and interests.

Negro (2017) provides a powerful hint on this by stressing the strong connection between telecommunications policy and the Internet ecosystem in China, in light of the aforementioned interdependence between the two. He

underlines how the four years preceding the establishment of ICANN and 3GPP constituted a major period of reform in the Chinese telecommunications market and in the layers of public bureaucracy in charge of its management. Details notwithstanding, it is worth underlining that the central state maintained a strong political and administrative control. After all, the then Jiang Zemin presidency was adamant on both the necessity to engage in digital development and the need to govern its social implications. On the administrative hand, as far as mobile Internet connectivity is concerned, it was the government who granted operators the use of one mobile Internet standard or the other. On the political hand, up until nowadays Internet Service Providers (ISPs) are bound to control the information exchanged by user and are made politically accountable. To be sure, what was here dubbed 'administrative' has politico-economic implications. Decisions on what standard to implement nationally affect the device market since incompatible standards force device manufacturers to produce devices with different technical characteristics for different national markets. This is most often read as a protectionist move (Shen 2021; Stewart et al. 2011).

Powerful governmental role notwithstanding, public and private stakeholders, as well as different layers of the Chinese public bureaucracy (for example, ministries and authorities), held separate interests. In this view, Zhang and Liang (2007) provide an insightful reconstruction. By 2007, that is, the year before 3GPP set the basis for 4G equipment roll out in Release 8, China had not rolled out 3G nationally yet. Three different 3G standards had been approved by the ITU-R, one of which (known as TD-SCDMA[2]) was elaborated in China and was incompatible with the other two. Governmental delays have been attributed to political concerns and the need to protect China's domestic market, still strongly SOE-dominated and potentially incapable to withstand global competition. Political concerns derived from the government's need to control the social implications of a more widespread Internet access. It is worth recalling from Chapter 4 that the Golden Shield Project, the so-called 'Great

[2] TD-SCDMA: Time-Division Synchronous Code-Division Multiple Access.

Firewall of China', was not fully implemented until 2008 (Negro 2017). In this context, private device and network manufacturers like Huawei had, in Zhang and Liang's (2007) account, an incentive to penetrate foreign markets amid China's domestic 3G standby. To this, Wen (2020) adds that China's domestic market was strongly dominated by foreign manufacturers, as China relied on foreign companies before building its own 'national champions'.

Therefore, a market push for internationalisation was among the drivers of Huawei in the mid-2000s. At the same time, Wen (2020) stresses that at that stage Huawei had been identified, along with other private and state-owned enterprises, among the strategic companies for which special funds for internationalisation were allocated.

In interviews with Huawei-affiliated participants, the company's need to internationalise amid domestic competition with SOEs emerges as a topic and is corroborated by other participants not affiliated to Chinese stakeholders. This provides ground for interpreting Huawei's drive towards internationalisation from a market, other than government-led, perspective. To be sure, industrial policy played a role, but this does not necessarily point towards extents of political control. Rather, it shows Huawei plays a strategic role in China's government's technological growth strategy. Given the latter authoritarian characteristics, the government's growing presence in business affairs within companies, and Huawei's growing dependence on China's domestic market, doubts about political control remain in place (Pupillo 2019). Once again, however, this thesis seeks to acknowledge the complex relation between the Chinese government and Chinese private companies, which is made of cooperation and control as well as dialectics as per chapters 3 and 4.

In short, the timing of Huawei's first contract for network manufacturing in Europe (in 2005) and the beginning of its engagement (and rapid growth) in the IETF (from 2007) allow to argue for the existence of a market incentive for Huawei to internationalise along with the Chinese government's existing industrial policy (Arkko 2020; Huawei 2021; Wen 2020; Zhang, Liang 2007). In interviews, some research participants do attribute Huawei's mid-2000s internationalisation spur to development in mobile technology and the device

market.

These elements are telling on the development of public-private relations in China, the transformation of the dialectic between the two, and the impact this had on Chinese actors' stances in standard-making. As stated above, governmental role in China's 3G policy proved central: it was the government who dictated the schedule for 3G rollout, even at the cost of major delays, and led to the deployment of the Chinese-elaborated TD-SCDMA in an effort to protect the Chinese mobile market. In this context, private actors found an incentive to internationalise and became active network manufacturers abroad.

Briefly, in this phase, a Chinese-elaborated mobile Internet standard was coexisting with those elaborated mainly by Western actors (Stewart et al. 2011). The role of the central government was a protectionist one. However, private actors (Huawei, in particular) began their internationalisation as network manufacturers, enhancing their role in the European market and in the IETF. Stewart et al. (2011) confirm this view: while the MIIT (which in 2008 subsumed the Ministry of Information Industry, MII 信息产业部 xinxi changye bu) was a major promoter of the TD-SCDMA standard, the then major national mobile operator, China Mobile, was testing the implementation of other international standards amid scepticism over TD-SCDMA's real potential for success. Nonetheless, despite its incompatibility with the other internationally developed 3G standards, TD-SCDMA attracted foreign investments, with such companies as Nokia, Alcatel, and Ericsson participating in its elaboration along with Chinese private and state-owned enterprises. At the same time, it must be noted that the Chinese SDO (CCSA, then called CWTS) had entered 3GPP already in 1999 (CCSA 2021). According to Stewart et al. (2011), ZTE became the second-biggest patent holder in TD-SCDMA as it invested in it despite uncertainty.

However, it is worth mentioning that both ZTE and the sceptical China Mobile are SOEs, suggesting that, despite state-ownership, a coherent 3G strategy did not emerge until 2008, when China Telecom, China's main telecom operator, was granted TD-SCDMA licence while China Mobile and

China Unicom were allowed to deploy the other ITU-accepted standards. This happened in a bid to protect the domestic market and the home-grown technology TD-SCDMA while respecting WTO commitments on technological neutrality (Stewart et al. 2011). As recalled in Chapter 1, TD-SCDMA was a 'Chinese' standard inasmuch as it was elaborated in China and deployed there. However, it was recognised as a 3G standard by ITU-R and the standardisation process saw strong cooperation between Chinese and Western companies, who saw an advantage in holding patents on different 3G technologies (Stewart et al. 2011). Moreover, 3G deployment in China was not capillary. In this context, private manufacturers like Huawei chose a strategy of internationalisation and 'tech agnosticism', whereby they produced technologies for every market (that is, for every standard) without prominently participating in the standardisation process.

The scattered characterisation of 3G standard-making does not only affect China. US and Asian actors launched a standardisation initiative called 3GPP2 in this phase. More specifically, 3GPP2 was established by the US, Korean, Japanese, and Chinese institutional partners of 3GPP to elaborate CDMA-2000, a 3G standard separate from the mainly Europe-made UMTS, also referred to as WCDMA with reference to its radio access technology[3].

As for this thesis' focus, what are the implications of this aspects for multistakeholder governance and technological (Internet) fragmentation? Briefly, government-company relations in China are dialectic ones, albeit ones in which the government plays a powerful role, which suggests private actors have a space for manoeuvre when acting internationally in standard-making. In 3G, in particular, the role of the central government was a powerful one in that it imposed a delayed implementation schedule and regulated the distribution of licences in favour of the home-grown standard.

In this view, a Chinese academic research participant based in the US underlines that Chinese stakeholders' participation in 3G standardisation, even though not fully internationalised, can be read as a Chinese effort to build a

[3] WCDMA: Wideband Code Division Multiple Access.

domestic mobile Internet value chain in order to better participate in standardisation and rollout processes when it came to future generations (4G and 5G). This participant maintained it is complicated to evaluate the positive or negative impact of Chinese activity in 3G standardisation given this technology's relatively small presence within the Chinese territory. However, it is deemed to have created a domestic ecosystem enabling tech stakeholders to enhance their participation in 4G and 5G standardisation processes. This allowed Chinese stakeholders to gain capacity in the global standardisation ecosystem.

As Wen (2020) recalls, the early 2000s were years of major market reforms in China amid the country's accession to the World Trade Organisation (WTO). The market saturation in the then 2G infrastructure and the strong presence of SOEs provided a strong incentive for Huawei to internationalise amid oscillating relations with the government and other major SOEs in its sector, such as ZTE. Only towards the end of the first decade of the twenty-first century did Huawei change its position in the Chinese market. However, at that stage the 4G rush had already started.

5.3 *A change in strategy: drivers and implications of China's approach to 4G*

In the run towards 4G standardisation, China's national strategy changed. According to some research participants, including telecommunication engineers familiar with the work of 3GPP, this derived from the 3G strategy's unsuccessfulness in promoting Chinese technology abroad. At this stage, it must be noted that Chinese participation is consolidating both in 3GPP and the IETF. Furthermore, between 2006 and 2009 the Chinese government suspended its boycott of ICANN's activities. While Chinese stakeholders' IETF and ICANN engagement is analysed in Chapter 3, it is worth mentioning their growing engagement in globally established governance institutions at this time in history.

However, this did not change China's protectionist attitude towards domestic-made mobile connectivity standards. Its home-grown 4G standard, known as LTE-TDD (also referred to TD-LTE)[4], was licenced in China in December 2013, while other global standards were only licenced by the Beijing government starting from 2015 (Wen 2020). Once again, all the aforementioned standards are ITU-approved, in compliance with the requirements set forth by ITU-R.

This time, deployment was broader and quicker than with 3G. Furthermore, the government is known to have endeavoured more proactively to promote TD-LTE in other developing countries, whereas TD-SCDMA was mainly deployed in China (Wen 2020). According to Yu Jiang (2011), Chinese actors' newly found competitiveness is due to the path dependences that exist in mobile Internet technologies. In this account, path dependences allowed Chinese actors to plan for future generations' developments by basing on the available 3G-related knowledge. Such path dependence is also visible in 5G: the initial phase of its development foresaw the deployment of radio standards on the LTE core network. In this, while being a standard-maker gives one a short-term advantage, being a standard-taker allows one to partially free ride on the earlier standards towards the development of the new one. This, of course, needs to be followed by economic and financial conditions, as well as a favourable public system of incentives.

As for the dialectic between public and private actors mentioned above, this stage also features relevant elements. According to Wen (2020), Huawei, poised to achieve a leading position in the domestic and international mobile Internet market, launched a 'price war' on ZTE and major foreign equipment sellers in 2007, rising from a 2% share in China Telecom's CDMA[5] equipment market share to a 30% share the following year. ZTE declined from the leading position in this market (32% in 2007) to 15% the following year. While China

[4] LTE-TDD: Long-Term Evolution Time-Division Duplex.

[5] CDMA: Code-Division Multiple Access, a telecommunications standard mainly related to 2G and built upon in 3G technology.

Telecom's three other major equipment suppliers (the Western companies Alcatel, Motorola, and Nortel) suffered minor losses in percentage terms, ZTE fell by more than half its 2007 percentage points. Once again, these aspects show that, despite an active governmental role in promoting home-grown technologies, relations among Chinese companies (whether state-owned or private) are not necessarily one of market sharing under state supervision. On the contrary, the Huawei-ZTE 'love-and-hate relationship', as it was dubbed by a research participant, emerges in most interviews with experts active in or familiar with 3GPP. This includes members of staff of Western companies, who observe the dynamics between Chinese private enterprises and SOEs as third parties. Nonetheless, in this dialectic the role of the Chinese government has remained powerful. By 2008, when 3G rollout had just started in China, the State Council had licenced a three-billion US dollar plan for 4G-oriented research and development (R&D). While this does not add information on governmental control on companies' activities in global standardisation bodies, it suggests a strong stance from the government in promoting a profitable home-grown 4G technology (Ming, Ouyang 2008; Yu Jiang 2011).

At this stage in history, Chinese corporations such as Huawei and ZTE increased their international market share. Meanwhile, 4G development continued. After beginning work on Release 8 in 2008, by 2012 3GPP had already frozen Release 10, paving the way for the deployment of LTE-Advanced (Wannstrom 2013)[6]. The growth of Huawei and ZTE, China's two main network manufacturers, has partially been addressed in Chapter 3. As mentioned, by 2013 Huawei's share of LTE contracts worldwide competed directly with Ericsson's, while ZTE was more reliant on the domestic market (Drahokoupil et al. 2017). At this stage, around two thirds of Huawei's global

[6] The all-encompassing terms indicating generations, such as '4G', are generally catchphrases for a set of technologies each being a development on top of the previous one, improving performances. Releases 8 through 10 are fully-fledged 4G-related releases, referring to technologies called LTE, LTE-Advanced and LTE-Advanced Pro, which set the basis for 5G.

revenues were from foreign markets, only one third were domestic.

In hindsight, it is possible to see that revenues had been declining since 2011, a tendency that now sees Huawei being strongly dependent on China's domestic market, which accounted for around two thirds of its revenues in 2020 (Brown 2021). However, by 2013 Huawei was establishing itself as a global player, with a strong market presence in Europe, Middle East, Latin America, and Africa, although in terms of Chinese industrial policy there still was a protectionist tendency towards participating in 3GPP while developing a non-interoperable 4G standard domestically. This phase was dubbed 'synchronism' by Zhou (2019), as China deployed 4G at the same pace as the world's other major powers and participated in 3GPP work while also standardising its home-grown TD-LTE standard.

Observing the text of specifications related to Release 8, 3GPP's first LTE-related release, frozen in 2009, one can see the widespread participation of Huawei, whose affiliates also obtained rapporteur positions on some working items. The two other most prominent Chinese actors within Release 8-related specifications are ZTE and China Mobile, the main-featuring Chinese ISP. These companies are listed either as supporting members to a feature or work item or as rapporteurs' affiliation on work items (3GPP 2009). Another important characteristic of Release 8 is that it aims in many points to integrate work from individual organisational partners and from 3GPP2, as well as subsuming the work of ETSI on Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), a move that allows better coordination on the elaboration of specifications for New Generation Networks (NGN) (Vidal et al. 2007).

In Release 8, several specifications and features address the integration of 3GPP2-elaborated standards to allow for greater technological compatibility worldwide (3GPP 2009). Many such integrations were supported by Chinese stakeholders, especially Huawei, hinting at an interest towards creating a 3GPP-elaborated 4G standard as broadly applicable as possible. While this could also have other drivers and objectives that fall outside the scope of this article, it is interesting to see that such patterns of behaviour of Chinese

companies in Release 8 are coherent with interview findings. As anticipated, research participants pinpointed both Chinese stakeholders' growth in presence in 3GPP during the 4G standardisation phase (2008-2013, roughly) and China's increased deployment of the 3GPP-elaborated 4G standard.

Following 2013, 3GPP2 remained dormant while its members have been increasingly active in 3GPP. Pohlmann, Blind and Hess (2020) find for example that South Korean actors like Samsung were the main owners of 5G-related patent families by the beginning of 2020, while Huawei was the main standard contributor in absolute terms. Furthermore, UMTS was also implemented in China, Japan, and South Korea, although it runs along other standards operated by different ISPs. It must also be underlined that Release 8-related specification stress 3GPP's work to integrate LTE and WiMAX technologies, a radio standard alternative to LTE in the 4G run (3GPP 2009). This signals once again a trend towards convergence in standards, an aspect that is further illustrated below and that returns in interviews.

In short, 4G set the basis for the situation illustrated by Pohlmann, Blind and Hess (2020) and summarised in Chapter 1, whereby Huawei represents one of the main standard-makers in 5G.

5.4 *5G: from 'chasing' to 'leadership'*

A key takeaway from the previous section is that 3G and 4G paved the way for Chinese industry to increase its strength towards a leadership position in mobile Internet standard-making while starting from a position of backwardness. In the words of Zhou (2019) already cited in Chapter 1, China went from 'chasing' in 3G development to 'synchronism' in 4G development to 'leadership' in 5G.

What emerges from most interviews on this topic is an increasing interest for Chinese actors to act as standard-makers at the global level instead of engaging in smaller-scale elaboration and implementation of technical

standards that, despite formal ITU recognition, are conceived to become coexisting to the globally deployed ones. In terms of public policy, Huawei reinforces this view by stressing its activeness in global standard-making.

In an interview with the author, a senior Huawei-affiliated telecommunication engineer underlined that around 14% of Huawei's capital and 50% of the company's human resources are invested in research and development (R&D). To this research participant, this strategy is aimed at enhancing the company's capacity to create and promote global standards, a fundamental element to gain a strong position in the market. Furthermore, this research participant agrees that the existence of multiple, coexisting, 3G mobile Internet standards was detrimental to the development of the global market and thus to companies' – including Huawei's – interests, reason why they are now striving to elaborate a global 5G standard. Telecommunication engineers not affiliated to Huawei tend to confirm this view. Among them, a former chair of a 3GPP working group and a 5G application expert add that no tendency towards fragmenting the work of 3GPP has come from China, where Huawei has been the top 5G standardisation contributor in quantitative terms, followed by Ericsson (Pohlmann, Blind, Hess 2020).

In November 2020, few months after these interviews, these interpretations have been corroborated by ITU-T's approval of two 3GPP-elaborated 5G radio interface standards. While no separate technical proposal came from China, the only locally elaborated 5G standard that met ITU-R's IMT-2020 criteria was from Telecommunications Standards Development Society India (TSDSI). At the time of writing, however, the ITU has stated that global interoperability has been reached (ITU 2020c). It must be stressed however that a few further 5G-related releases are expected to come from 3GPP at the time of writing (Ten Oever 2021). Furthermore, it must be specified that among the two 3GPP-promoted 5G radio interface standards recognised by the ITU, one was promoted by Chinese companies among others, albeit still within the 3GPP realm. However, this simply featured an extra IOT-related specification and is interoperable with the other one (ITU 2020c).

Observing the specifications related to Release 15, one can see

engagement on the side of Huawei, ZTE and the three state-owned ISPs. Huawei is often sided by HiSilicon, its fully owned chip-making division. Compared to specifications related to Release 8, there are fewer references to the integration of specifications elaborated by different bodies. Conversely, the effort visible in Release 8 to harmonise 3GPP2 and WiMAX provisions within 3GPP work seem to be replaced in Release 15 by measures to interoperate LTE and 5G infrastructure, coherently with the objective to build a non-standalone 5G connectivity in this phase, allowing 5G's New Radio to operate on top of the LTE core network. As mentioned above in this chapter, this is done in anticipation of the standalone specifications provided in Release 16. The fact that less harmonisation work was needed at this stage signals once again the trend towards harmonised mobile Internet standards that emerged in interviews, which brought about an operationally compatible 5G landscape on a global scale.

On a different note, 5G rollout has only just began and geopolitics is deeply entrenched with market policies. Long-standing debates in Europe about whether or not to include Huawei in the construction of core networks and in auctions for the radio spectrum are exemplary (Ciuriak 2019; Economist 2020; Poggetti 2021). Therefore, a deeper insight below the surface of public policy shows not only that Huawei is a major rule-maker in 5G standardisation, but also that there is no intention from Chinese stakeholders to elaborate a separate, incompatible national 5G standard. However, geopolitical divides remain visible within the network and device markets, as better discussed in the next section.

To summarise, the three 5G radio interface standards approved by the ITU at the end of 2020 ensure compatibility, confirming the views expressed by most interview participants throughout the research process and the aforementioned process of convergence in standards. This entails that Chinese companies' activities in mobile Internet standardisation processes grew in time and became more influential. Participation and influence grew together: as the capacity of Chinese stakeholders to influence decision-making grew, so did their interest in shaping global standards and avoid local incompatible

specifications. It goes without saying that the need for a growing company to expand its market is an essential driver of the aforementioned actions, as it emerged throughout interviews.

5.5 *The rise of China (and Chinese industry) in telecommunications: normative implications*

A key finding illustrated in the previous section is that it is mainly through private actors – above all, Huawei (Pohlmann, Blind, Hess 2020) – that China is becoming stronger in mobile connectivity standard-making. Research participants knowledgeable about 3GPP's work usually observe a governmental role in standards-related policy-making, but generally limited to matters of policy coordination. As it emerges in literature, governmental support and government policies do play a role in Chinese companies' 'going out' that is acknowledged in both Western and Chinese literature, although the extent to which its role is dominant is not apparent (Cai 2018a; Segal 2018; Shen 2016; Tang 2020). In addition, the threshold between influence and coordination, on the one hand, and control, on the other, is blurred (Zhong 2019; Pupillo 2019).

Particularly relevant is the contribution of a US-based Chinese academic, who underlined in an interview with the author the dynamicity of the relationship between China's government and Chinese companies. This research participant stressed the strong role of the state in the early 2000s, when China opted for the adoption of a nationwide 3G standard incompatible with the one deployed in Europe and elaborated within 3GPP. Significantly, the image of China's inner politics emerging from this interview is not a monolithic one, although a strong, albeit evolving, state-business tie is visible:

> *Probably you should view it as a longer historical process: China's participation in shaping the mobile communication standards started very early with 3G and there was a very big debate in China on*

whether [Chinese actors should have participated] in this game or just follow[ed] the US's or Europe's standard. So, […] even today, you can't say [Chinese participation in 3G was] a success or failure because it has only very, very limited presence within Chinese borders, [but currently] I think almost the majority would agree that [without] China's participation in shaping this early standard, Huawei today would not be able to reach standards in 5G. In 3G, China basically built its whole production chain, so now Huawei can take advantage of this huge [value] chain to shape this technical standard.

Generally speaking, research participants knowledgeable about 3GPP could not identify instances in which forms of governmental control on Chinese companies was visible beyond matters of coordination and policy direction.

In other words, ambiguities in public-private relations persist and it is difficult to assess the normative impact of Chinese actors on multistakeholderism. On a formal level, China's engagement in 3GPP is strongly business-driven. Huawei is a private actor, whereas other state-owned enterprises such as ZTE are much less active and influential in 3GPP. However, the extent to which China's government controls companies' business process is unknown. Nonetheless, most research participants familiar with 3GPP's work, independently of their affiliation, tend to confirm state-business ties but see governmental coordination, rather than governmental control, behind Chinese companies. In this, the Chinese state leadership remains ambiguous. For instance, China's president Xi Jinping called for efforts "to unite people from the private sector around the Communist Party of China (CPC) to better promote the healthy development of the private sector" (Xinhua 2020a; Xinhua 2020b; Buckley, Bradsher 2020). While he did not elaborate on what this means in practical terms, practices for stricter governmental control on companies' activities have been implemented through antitrust measures (Zhong 2021). Briefly, whether and to what extent China may increase states' influence in multistakeholder Internet governance through de facto state-controlled, but formally private, actors remain open questions.

Ambiguity notwithstanding, patterns of behaviour similar to those found in the IETF emerge among Chinese actors in 3GPP. According to interview participants active within 3GPP, Chinese stakeholders went from a numerically and technologically marginal position to one of prominence under both perspectives. Besides Chinese stakeholders' quantitative prominence illustrated in Chapter 3 and systematised by Pohlmann, Blind and Hess (2020), interview participants underline that Chinese growth in 3GPP started with Chinese companies hiring Western consultants familiar with the forum's working culture and environment. Progressively, Chinese companies grew their numerical presence within and across 3GPP working groups with an increasing presence of Chinese-born and Chinese-educated engineers. This follows the pattern illustrated for Chinese engagement in the IETF in Chapters 3 and 4. In the words of an interview participant affiliated to a European telco and active within 3GPP,

> *it is an evolving topic: the first step taken by Chinese companies was to hire American and English colleagues – even some colleagues from [my company] have been hired by Huawei, in particular, and they took on Huawei's standardisation activities. So, there was a quite big 'trading season', alternatively through consultants, to bring [to 3GPP] the company's position through people who had no linguistic barriers and were in the – so to say – 'European or American mindset' to interact in standard-making organisations, which is different from the Chinese one. From this point of view, I must say it is impressive to see [how] cultural backgrounds influence participation in standard-making organisations. […] The second step was to [strongly increase their presence in] 3GPP, by which I mean that Huawei in particular has very sizeable delegations in working groups. I mean, if I look at the RAN plenary, which is the one I follow, where normally there are around 300 people following face-to-face meetings, Huawei has 30 to 40 people present: that is, more than 10% of the physical participants are from Huawei. ZTE has lower figures, but they are always present and there are other strong Chinese actors: I'm thinking of Oppo.*

As emerges in interviews, the growth of Chinese stakeholders in 3GPP, much like in the IETF, was a process of learning and adaptation to the body's standard-making norms. The adaptation process went along Chinese companies' market growth, especially in Huawei's case, while domestically China was launching different deployment strategies: from protectionism, with the promotion of the home-grown 3G standard TD-SCDMA, to a global stance with their participation in an industrial leadership position in a fully interoperable 5G environment. Such process was also followed by a faster deployment policy at the domestic level: while 3G deployment in China was not ready until 2008, 4G and 5G deployments were synchronic with Europe and the US.

Summarising, mobile Internet connectivity has experienced a convergence in standards: three major non-interoperable 3G standards were deployed in three major markets, with CDMA-2000 being the dominant standard in the US, UMTS being dominant in the EU, and TD-SCDMA in China. Nowadays, the three 5G radio interface standards recognised by the ITU – two from 3GPP (3GPP 5G-SRIT and 3GPP 5G-RIT) and one from TSDSI (5Gi) – grant a wide extent of interoperability. In the ITU's own words, "these technologies were deemed to be sufficiently detailed to enable worldwide compatibility of operation and equipment, including roaming" (ITU 2020c). To put it briefly, mobile Internet connectivity is experiencing a trend towards competing, rather than coexisting, standards as defined in Chapter 1. Chinese stakeholders such as Huawei are supportive and fully participatory in this trend as their global market reach requires globally scalable technological solutions. However, such convergence in standards is confronted by a growing market divide, whereby countries tend to (or are pushed to) choose between network manufacturers from Western(-leaning) countries or China. In the context of the growing US-China trade competition, many US allies within and outside the EU adopted some extent of restrictions towards Huawei and other Chinese manufacturers (Poggetti 2021). Despite centrality in the media (Ciuriak 2019), in terms of standardisation politics this is a separate matter. While it can and does affect the speed and characteristics of deployment policies, it falls outside the scope

of this thesis.

5.6 *Conclusion: back to theory*

At the theoretical level, similar considerations can be advanced as per the analysis on critical Internet resources presented in Chapter 4.

From a regime-theoretic perspective, Chinese actors maintained an extent of ambiguity in time towards mobile connectivity standards, too. While having accessed 3GPP at an early stage in 1999, they participated in 3GPP2 and elaborated domestic 3G and 4G standards along the other internationally recognised ones. However, such ambiguity appears to have faded with 5G development, as Chinese stakeholders became capable of contributing to global 5G specifications. Therefore, Chinese actors have grown within the existing governance complex, transformed the balance of power within it by growing to a standard-maker position within 3GPP but did not change its institutional rules, norms, and principles so far. Indeed, no new regimes, organisations, nor separate technical standards have been established. In several interview participants' accounts, informal rules within 3GPP and other bodies involved in the making of 5G-based technologies have transformed amid changes in the balance among different stakeholder groups. For example, the surge of the so-called 'Over the Top' (OTT) service providers is seen as a factor. However, no normative change is seen coming from a group of stakeholders on national lines. On the contrary, as illustrated above in this chapter, Chinese stakeholders have progressively become prominent within 3GPP's work and participate through a growing number of engineers who were born and educated in China, signalling a growing acceptance and familiarity with 3GPP's institutional environment.

This matter can be observed in terms of norm entrepreneurship. The findings illustrated in this chapter show that the more Chinese state- and non-state stakeholders have grown capable to influence decision-making, the more

they have accepted norms and rules and adopted them to promote their national and/or business interest. The historical perspective of their progressive engagement with the existing mobile Internet standardisation architecture is telling: from partial isolation on 3G, to a form of partial engagement on 4G, to a leadership role in 3GPP work on 5G (mostly as far as Huawei is concerned). Recalling from Chapter 4, it can be noted that this was accompanied by a contemporary shift from multilateralist stances in global Internet governance towards increased, albeit ambiguous, acceptance of multistakeholderism. As illustrated above, in the early 2000s, when separate 3G standards were deployed, China stood as a staunch multilateralist, which confirms its role of defiant outsider to the institutional arrangement. In the run towards 2010, when 4G started being deployed, and short after, China alternated further engagement in the multistakeholder system (with Huawei's presence at the IETF increasing steadily since 2007) but contributed to reawakening multilateralist conundrums at WCIT in 2012 (Glen 2014). This is also reflected in China's ambiguous stance in mobile Internet standards, as it deployed nationally both the LTE and LTE-TDD standards.

In the years preceding 2020, that is, the deployment of 5G, Chinese actors were fully engaged in 3GPP work as illustrated above and expressed increasing support for and involvement in the multistakeholder system (Shen 2016; Mueller 2017), especially in the wake of the IANA stewardship transition (Jongen, Scholte 2021; Mueller 2017). In summary, Chinese stakeholders display all the interest in accepting the norms and institutional architectures that allow them to participate fully and cast their power globally. As mentioned, Huawei has become the most influential actor in 5G standardisation within the European-born 3GPP without establishing or seeking to establish any alternative standardisation body but following a path of progressive involvement in and engagement with the existing governance mechanisms that followed – to a broad extent – a wider national strategy where the Chinese state played, at least, a role of financial supporter and political coordinator.

As anticipated elsewhere in this thesis, technologists participating first-hand in 3GPP work raised qualitatively different interpretations of Chinese

stakeholders' engagement in mobile connectivity standard-making compared to policy experts. Many interview participants familiar with the work of 3GPP stressed the process of adaptation of Chinese stakeholders not only in terms of political norms applying to collective actors (governments, companies, or other organisations), but also at the individual level. Contrary to widespread media debates on technological and Internet fragmentation along geopolitical lines, Chinese stakeholders are in a process of growth within the Internet governance regime complex. As far as mobile connectivity standards are concerned, a convergence in standards from 3G to 5G is visible as illustrated in this chapter.

In conclusion, it emerges that, despite ambiguities arose in time, China and its domestic actors have become increasingly involved in the existing standardisation venues: they have increasingly acknowledged and adopted universal standards and contributed to their making. This happened through a market and policy push that provided growth incentives to Chinese actors and made them capable of influencing standard-making, but also through a learning process as illustrated above in this Chapter. Drawing from chapters 3 and 4, one can see that this trend from Chinese stakeholders is valid both in critical Internet resources governance and in mobile Internet standard-making. This carries broader implications for China's engagement in and with the Liberal International Order, inasmuch as multistakeholder, private-based Internet governance is a facet of it as per Chapter 1.

In strictly theoretical terms, this proves the normative rigidity of the Internet governance regime complex recalled in Chapter 2: as promoting alternative standards through alternative fora proved to be economically untenable given the geographically narrow deployment of TD-SCDMA, Chinese stakeholders scalarly adapted and integrated within 3GPP's work. Furthermore, this happened through patterns of competition and collaboration among Chinese actors, signalling non-overlapping interests at play among them despite common nationality.

Certainly, conclusions drawn from the field of mobile Internet standards do not allow straightforward generalisation to a systemic level. For example, scholars and policy-makers are divided on the meaning of China establishing

financial institutions parallel to the global ones, such as the Asian Infrastructure Investment Bank (AIIB) (Gabusi 2019). Furthermore, China has certainly not transformed domestically to accept liberal norms (Economy 2018). While these topics go beyond the scope of this research, they are illustrated to stress that what applies to China in global Internet governance or its subsets may not be universally applicable to Chinese action in other policy fields. Furthermore, it must be re-stressed that ambiguities in the Internet governance context remains from China's part (Negro 2020).

Open debates notwithstanding, evidence from such a strongly politicised field as mobile Internet technology standards, which carries heavy economic and geopolitical weight, provides helpful insight on broader issues. Being the subset of Internet governance in question interrelated with great power dynamics, being technological supremacy historically linked to US hegemony (Winseck 2019), it can be safely argued that the findings hereby presented are transferable to other fields of inquiry involving superpower dynamics, public-private power relations, issues of private authority in global governance, as well as systemic analyses on the future of the Liberal International Order. This aspect is addressed in the next chapter, on top of essential questions on Internet fragmentation, alignment, and the future of multistakeholderism.

CHAPTER 6

THE RISE OF CHINA, INTERNET FRAGMENTATION, AND THE FUTURE OF MULTISTAKEHOLDERISM: IMPLICATIONS FOR THE LIBERAL INTERNATIONAL ORDER. A GENERAL CONCLUSION

6.1 *Introduction*

Chapters 3 through 5 portray a complex scenario for the rise of China and Chinese public and private stakeholders. Contrary to the dualist conception of the multilateralist challenge to multistakeholderism of the early 2000s, and contrary to the dichotomous views on the future of Internet governance emerged amid the US-China technological competition, the rise of Chinese stakeholders featured a mix of contestation of and adaptation to the existing multistakeholder Internet governance regime complex. Inasmuch as such regime complex is a facet of Liberal International Order as illustrated in Chapter 1, these aspects have implications on the future of the order and its capacity to integrate emerging actors and withstand revisionist attempts (Ikenberry 2018).

ICANN and the IETF feature different characteristics, and they are in turn different from 3GPP. As per Chapter 1, 3GPP does not directly fit the multistakeholder definition that is valid for ICANN. It is more similar to the IETF in its strongly private-based and technically oriented organisation. However, on paper the IETF is based on individual participation, while 3GPP has formal membership through its seven partner Standards Development Organisations (SDOs). Furthermore, the IETF elaborates standards essential for the Internet to function. In other words, it builds the logical architecture of the Internet. 3GPP is the main standardiser of new generations of mobile Internet connectivity, that is, such technologies from 3G thereafter. While allowing Internet connectivity on mobile devices, these technologies entail a telephonic

infrastructure. True, the infrastructural integration and interdependence between Internet and telephony has always existed, but while the former follows a building-block approach, the latter is a fully determined infrastructure. Furthermore, functionalities are different: IETF standards allow the Internet to function the way it does, while 3GPP standards allow a form of radio access to the Internet. Despite such differences among the three bodies, common patterns of growing engagement of Chinese stakeholders can be found. They are partially visible through the computational analysis presented in Chapter 3 but tend to emerge systematically in interviews with experts.

This chapter observes the implications of the findings outlined in chapters 3 through 5 for multistakeholderism and Internet fragmentation. Building on these observations, it addresses the consequences of such implications for the Liberal International Order.

The next section will illustrate the implications of Chinese stakeholders' involvement in 3GPP for multistakeholderism and Internet fragmentation, while section 6.3 will address the same issues for the critical Internet resources. Finally, section 6.4 draws conclusions connecting the two debates to the global one on China's rise and the Liberal International Order.

6.2 *Chinese actors in 3GPP: what consequences for multistakeholderism, interoperability, and Internet fragmentation?*

The interview working statements elaborated in Chapter 2 formed a basis to assess the influence of Chinese stakeholders on 3GPP work and mobile Internet standards and the consequences of their actions for the questions at stake in this thesis. As far as mobile Internet standards are concerned, the two statements read as follows: first, *Chinese-elaborated mobile Internet standards are competing (that is, not coexisting) with EU and US ones*. Second, *governments and government-controlled actors' influence in global technical standardisation processes has increased and China has contributed to it*.

Recalling from Chapter 5, China aims at being a 5G standard-shaper, not at creating alternative, incompatible (that is, coexisting) specifications – in line with the working statement in question. However, this has not always been the case. In short, China adopted an incompatible, domestic-oriented 3G standard in the early 2000s, while licensing UMTS to a minor operator. When it came to 4G technologies, China adopted both the universal standard and an incompatible locally-oriented one, with the government choosing which operator was allowed to deploy which standard. Now, Chinese stakeholders are one of the key standard-setters in 5G and, as emerged from interviews, they show no intention of elaborating local specifications which are incompatible with global ones (Pohlmann, Blind, Hess 2020). Both Huawei-affiliated engineers and technologists affiliated to Western companies confirmed in interviews that no tendency towards fragmenting the work of 3GPP appeared to come from Chinese stakeholders, where Huawei is currently the top 5G standardisation contributor in quantitative terms, followed by Ericsson (Pohlmann, Blind, Hess 2020).

In brief, Huawei is a major standard-maker in 5G standardisation and there is no intention from Chinese stakeholders to elaborate a separate, incompatible national 5G specification. On the contrary, they aim at being major players in 5G at the global level. However, beyond network infrastructure standardisation, questions remain open about Huawei's device- and application-level capacity to grant interoperability. The US ban on Huawei's use of Google services makes this issue increasingly relevant. To be clear, this falls partially outside the scope of this thesis. Furthermore, academic analysis on this aspect is sparse and mostly speculative, arguably due to the novelty of the issue at stake, which emerged powerfully in 2018 with the US-China trade war. Nonetheless, it is worth spending a few words to clarify.

To start with, it must be underlined that Android is an open-source operating system, which entails that the US government could only ban the use of Google's Mobile Services (GMS) core part (Sin 2020). As Sin (2020) explains,

[GMS] are a collection of services with special APIs (application

programme interfaces) designed by Google to allow for easy adoption by third-party developers. The services mostly cover Google's cloud ecosystem, such as Google Drive and Docs, as well as YouTube and the Google Play Store. Other Google apps that fall outside this umbrella, such as Google Maps and Chrome, work perfectly fine on a Huawei device. In fact, Gmail and Google Calendar work too, but only through third-party apps such as Microsoft's Outlook.

Furthermore, with the launch of Huawei's GMS equivalent, that is, Huawei Mobile Services (HMS), and the operating system HarmonyOS, Huawei seeks to provide a fully-fledged alternative to Android and the GMS's core part while allowing its users and customers to use the same services and platforms available through Google services (Doffman 2020). For services and platforms present on GMS but still not accessible from Huawei devices, the block seems to be porous, as several mirroring systems have been made available to access them (Sin 2020).

To summarise, Chinese companies' activities in mobile Internet standardisation processes grew over time and became more influential. Participation and influence increased together: as the capacity of Chinese stakeholders to influence decision-making grew, so did their interest in shaping global standards and avoid local incompatible specifications. It goes without saying that the need for a growing company to expand its market is an essential driver of the aforementioned actions, as it emerged throughout interviews.

This can be better analysed when framed within the broader context of China's participation to Internet governance, illustrated in Chapter 4. To recap, Chinese authors of Internet Drafts and Requests for Comments (RFCs) at the IETF increased sharply between 2007 and 2010 amid a relative decline of the number of Western authors (IETF 2020) and Huawei was second only to Cisco in terms of affiliated RFC and Internet Draft authors by 2020. In this, China is the second major contributing country, although it slides down to third position if contributions from EU countries' nationals are totalled (Arkko 2021).

Based on these figures, it can be observed that Chinese actors' presence and weight is growing throughout the Internet governance regime complex at

large. In other words, China has grown more powerful in 3GPP and more participatory in other Internet governance fora, too. While literature underlines China's ambiguous behaviour towards the key organisations of the multistakeholder system, namely ICANN with respect to the role of the ITU, what generally emerges through interviews is that China and Chinese stakeholders have sought to substantially increase their presence in every subset of the Internet governance regime.

Moving back to mobile connectivity standards, no incompatible local Chinese specifications are under elaboration according to research participants, while Huawei is the single most important contributor to 5G standardisation within 3GPP. The approval of three globally interoperable 5G radio interface standards by the ITU confirms it (ITU 2020c), notwithstanding concerns by part of the technical and business community. Significantly, no new organisation or fora has been established by China in parallel or replacing the existing ones under consideration. This provides a rather straightforward corroboration of the first working statement. The convergence in standards, however, is accompanied by a fragmentation of the market along national lines (Poggetti 2021). Despite this, standards convergence remained a trend after the 3G and 4G experiences in limited global interoperability.

As for the second working statement (on state-centricity in mobile connectivity standard-making), China is becoming stronger in mobile Internet standard-making mainly through private actors – primarily Huawei (Pohlmann, Blind, Hess 2020). Research participants with a good understanding of 3GPP's work usually observe a governmental role in standards-related policymaking, but generally limited to matters of policy coordination. As previously underlined, governmental support and government policies do play a role in Chinese companies' 'going out' that is acknowledged in both Western and Chinese literature, although the extent to which its role is dominant is not apparent (Cai 2018a; Segal 2018; Shen 2016; Tang 2019). In addition, the threshold between influence and coordination, on the one hand, and control, on the other, is blurred (Zhong 2019; Pupillo 2019). Interviews in Chapter 4 underlined the dynamicity of state-company relationships in China in the run

from 3G to 5G development. Generally speaking, research participants with a good understanding of 3GPP could not identify instances in which forms of governmental control on Chinese companies were visible beyond matters of coordination and policy direction.

To summarise, the second working statement is more difficult to corroborate. China's engagement in 3GPP is strongly business-driven, as Huawei is a private actor, whereas the state-owned enterprise ZTE is much less active and influential in 3GPP. However, the extent of state-company ties in China is still unknown. Despite this, most research participants familiar with 3GPP's work, independently of their affiliation, tend to confirm such ties in terms of governmental coordination, rather than governmental control. In this, the Chinese state leadership remains ambiguous. For instance, Chinese authorities are currently conducting antitrust crackdowns on several big tech providers under the Maoist banner of 'common prosperity' (Nanni 2022), which in the context of the US-China trade competition goes hand in hands with Huawei's increasing reliance on the domestic market (Brown 2021). In other words, whether and to what extent China may increase states' influence in multistakeholder Internet governance through state-controlled, but formally private, actors remains to be seen.

To conclude, the more China's private sector and state-owned enterprises grew capable of influencing 3GPP standardisation processes, the more they integrated into the mainstream of the aforementioned process. This convergence in standards was accompanied by a fragmentation of the market, rather than the infrastructure, in the wake of the US-China trade competition, whereby a number of EU states followed the US in restricting market access to Chinese market actors (Poggetti 2021).

6.3 *Multistakeholderism and fragmentation at the core: Chinese actors in the IETF and ICANN*

At times, the prominence of one type of actor or another can be prevalent and the power balance in multistakeholder relations is most often skewed towards more economically powerful stakeholder groups (Santaniello 2021). Internet fragmentation has instead received a multitude of definitions. While Mueller (2017) sees it as a technical compatibility matter and leaves political forms of control to the realm of 'alignment', Drake, Cerf and Kleinwächter (2016) conceptualise it as a broader phenomenon that can stem from political, commercial, as well as technical actions. Further discussion on these definitions is elaborated at the end of the present chapter.

As far as critical Internet resources are concerned, the following working statements were elaborated and corroborated throughout the interview process: first, *China's re-accession to ICANN GAC has increased governmental influence on IPs and DNS root zone management*. Second, *China's increased participation in the IETF has enhanced the likelihood of separate (that is, coexisting, not competing) Internet standards being created*.

To assess the first working statement, it is necessary to draw from Chapter 4. The re-accession of China to GAC has a manifold explanation. The institutionalisation of multistakeholderism as a governance principle, the permanence of ICANN (Mueller 2010), and a compromise on Taiwan's membership are all reasons for China to normalise its troubled relation to ICANN (Scholte 2017). As observed throughout the interview process, China has grown as a national group within ICANN, both in terms of its government's participation in it and in terms of stakeholders' presence. However, apart from the notable presence of an Alibaba affiliate in the GNSO Council and the vicechair of GAC obtained by the Chinese representative in the wake of the IANA stewardship transition, no visible influence was brought by Chinese stakeholders.

To be sure, many interview participants find state influence has increased in Internet governance independently of China's role. China's growing

influence in the ITU, along with a more globally generalised push for increased governmental role on such aspects as data protection, data localisation, and Internet and 5G infrastructures create ground for increased state presence and influence (Haggart, Tusikov, Scholte 2021), a push that comes also from Western governments (Santaniello 2021). Despite this, Chinese stakeholders have become increasingly present and participatory in multistakeholder Internet governance at ICANN and the IETF, as per Chapter 3, and something similar happened in 3GPP as assessed in Chapter 4. This interpretation resonates with several interview participants and with previous literature findings. Arsène (2018) confirms that, despite pushes for ICANN reforms and multilateralist quests, the Chinese government chose to find a way into the ICANN-based multistakeholder governance model to be able to influence decision-making in the existing regime complex. Furthermore, she hypothesises that with the global economic growth of Chinese non-state stakeholders, participation in multistakeholder fora is more profitable for them in terms of the influence they can exert in multiple existing governance venues.

This is confirmed throughout the interview process conducted for this research. Despite ambiguities and attempts at forum shopping (Negro 2020), most research participants confirm Chinese participation in ICANN and acceptance of norms thereof has increased, as also found by Jongen and Scholte (2021). Once again, it would be simplistic to address the ensemble of Chinese stakeholders as a monolithic whole and dialectic among actors needs to be accounted. When addressing this matter in relation to Chinese stakeholders' acceptance of the norms of ICANN-based governance, a research participant stressed that

> *the so-called 'multistakeholder community' [is] a kind of transnational elite whose identity is more that of a transnational elite network than of a particular, individual national component. In other words, […] these people are seeing each other and interacting with each other constantly, so they're not only working at the main ICANN meetings - and one should say also the Regional Internet Registries […]. So, what I want to say is: between the ICANN meetings; the conference calls*

that are going sometimes weekly, sometimes – depending on the policy processes – even every couple of days… there's a constant interaction among these people and they see each other over a long period of time. And so when they meet at these meetings it's all hugs and kisses and, you know, best friends… it's [as if] they worked for a supranational company, a supranational regulatory community, if you like. I wouldn't say that the representatives of China are as integrated as many of the others, but I think they are recognised, they're part of the show, they're at the cocktail parties, they are doing everything, […] they're absorbed into all of that. I remember the head of CNNIC (at one point, during the IANA transition) got up, took the microphone and said: "well, I can't think of any better arrangement than ICANN for the oversight system". Meaning, by implication: not the ITU, ICANN is the place.

This participant continued to emphasise how this applies to the members of the ICANN community, that is to say those people who participate in it on a regular basis. Conversely, this does not apply outside that pool, implying that different political circles within China have different interests and points of view when it comes to participating in Internet governance and regulating the Internet. This has powerful implications when it comes to the questions of fragmentation and alignment.

To summarise, as far as the first working statement on CIRs governance is concerned, ICANN and IETF maintained their strongly private-led governance form. True, governments can carry weight through GAC in ICANN and attempts at state influence in standard-making have been identified in the media and by some research participants. Furthermore, the debate on digital sovereignty and the return of states in Internet governance is growing (Haggart, Scholte, Tusikov 2021). Nonetheless, ICANN and the IETF have retained their private-based functioning.

Moving to the second working statement related to CIRs governance, fragmentation has received a myriad of definitions. This thesis bases its arguments on Mueller's (2017) narrow focus on technical fragmentation,

whereby a fragmented Internet is one in which separate incompatible network protocols are adopted, hampering the transfer of data between devices adopting different protocols. It is worth recalling that this technical aspect would have direct geopolitical implications: different incompatible standards would be implemented along national lines, thus rendering devices produced and sold in or for one territory incommunicable with those produced and sold in another.

To the extent that the global, open Internet is a facet of the Liberal International Order in its global spatial dimension, technical Internet fragmentation along geopolitical lines would be a threat to it. Findings illustrated in Chapter 4 point towards a growing acceptance of multistakeholder Internet governance from Chinese stakeholders as illustrated above in this chapter. This is valid not only for Chinese stakeholders in ICANN, but also for their homologues in the IETF, where the standardisation of the essential Internet standards takes place. As illustrated in Chapter 4 and building on the network analysis presented in Chapter 3, Chinese stakeholders' presence and influence in the IETF has grown constantly and Huawei is currently the second most prominent organisation in terms of RFCs published by its affiliates (Arkko 2021). This has a direct tie to the Internet fragmentation debate.

Despite concerns over fragmentation, China has not deployed standards alternative to TCP/IP nor has it adopted a separate DNS (Arsène 2018). On the contrary, Chinese stakeholders' growing presence and acceptance of multistakeholderism proxies an increased interest in shaping the existing universal Internet standards. This holds true for the Internet's critical resources: although the first decade of the twenty-first century saw the arrival of concerning news as China anticipated ICANN in deploying IDNs in parallel with the ICANN-supervised DNS, currently the former are fully part of the latter. Clearly, suspicions around China's attitude towards the existing Internet architecture are longstanding and persisting, as exemplified in Chapter 4 by the debate around the launch of the New IP proposal at the ITU in 2019. However, the likelihood of such technical proposal yielding technical fragmentation was questioned by most interview participants.

In conclusion, China adopts the same numerical identifiers and transport

protocols used globally as well as the same DNS. Furthermore, Chinese stakeholders have increased their participation and interest in carrying influence within global multistakeholder Internet governance fora.

Nonetheless, this contrasts with China's domestic regulatory and technical tools of online control, which Mueller (2017) dubs 'alignment' of the Internet to domestic regulation. While a deep dive into, and interpretation of, the history of Chinese media is outside the scope of this thesis, it is necessary to look at China's domestic dynamics for a full interpretation of Chinese stakeholders' stance within and towards multistakeholder Internet governance. As illustrated in Chapters 3 through 5, the Chinese government played a major role – both in terms of economic incentives and forms of control – in establishing telecommunication architecture and services within the country. Since China established its first permanent connection to the Internet in 1994, state doctrine mandated that China harness the economic advantage of cyberspace while maintaining control on online social phenomena (Brady 2017).

It would be simplistic to maintain that the Chinese government has full control on the activities individuals conduct online. On the contrary, online citizenry in China expresses a whole variety of opinions and views, although this is constrained within the boundaries of what the state allows (M. Jiang 2010), which have become stricter under Xi Jinping's presidency (Brady 2017). To different extents, the integration of China in the global cyberspace has always been balanced domestically by tools of social control. In 1998, the Golden Shield Project (also dubbed 'the Great Firewall of China' in the West) was launched. While the most salient immediate need for the government was to contrast the spread of Falun Gong, this system of regulation and technical tools for censorship was strengthened and brought fully in place in 2008 (Negro 2017). Following this, China shut down Facebook within its territory in 2009 following social and political turmoil in the Xinjiang city of Urumqi and closed Google's browser in 2010, with the company redirecting its server to Hong Kong and maintaining only few offices and minor services within China's mainland (Negro 2017).

Cyberspace control in China does not only affect content and services availability, but also the way in which such contents and services are enjoyed and/or provided. In 2017, the 'Cybersecurity Law' (网络安全法, wangluo anquan fa) established provisions for data localisation, that is, the legal requirement to store sensitive data collected in China on servers and data centres based within the Chinese territory (Liu 2020). At the time of writing, a broader data protection framework is being established, mandating different forms of data localisation based on different types of data (Nanni 2022). 2017 was also the year when the Internet Domain Name Management Rules (互联网域名管理办法, hulianwang yuming guanli banfa) were introduced. A first key element of this law is contained in article 9:

> *For the domestic establishment of a domain name root server or domain name root server-running body, a domain name registration management body or a domain name registration service body, permission from the Ministry of Industry and Information Technology or provincial, autonomous region or municipal telecommunications management departments (hereafter jointly named telecommunications management bodies) shall be obtained* (MIIT 2017)[1].

A second key point is found in the following article, first comma, where conditions for domain name registrants are set:

> *Those applying to establish a domain name root server or domain name root server-running body, shall meet the following conditions: (1) the domain name root server is to be set up within the borders, and shall conform to corresponding Internet development plans and the requirements of the safe and stable operation of the domain name*

[1] English translation retrieved from (edited by Rogier Creemers): https://chinacopyrightandmedia.wordpress.com/2016/03/25/internet-domain-name-management-rules-opinion-seeking-revision-draft/ (September 17, 2021).
Full final text of the law (original language) retrieved from: https://tinyurl.com/49bwc6fw (September 17, 2021).

system […] (MIIT 2017).

These rules have been established along with the aforementioned Cybersecurity Law. Furthermore, they can be read in the same context as the 2010 White Paper on the (state of the) Internet in China (The State Council Information Office of the PRC 2010, hereafter SCIO) and the International Strategy of Cooperation on Cyberspace (ISCC, 网络空间国际合作战略, wangluokongjian guoji hezuo zhanglüe) of 2017 (Xinhua 2017). The former document is recognised as having introduced the concept of 'cyber sovereignty' in China's official governmental discourse for the first time (Creemers 2020b).

The timing of such domestic developments is telling when read in conjunction to changes in China's stance in global Internet governance. Elaborating from Chapter 4, the Golden Shield Project was completed in 2008, though constantly enhanced, right by the beginning of the deployment of 3G in China – that is, when access to the Internet among the population started spreading much further: in 2008, Chinese Internet usership reached 298 million, surpassing the US's (Flor Cruz, Seu 2014). The concept of 'cyber sovereignty' was introduced in the same years when crackdowns on Facebook and Google began (2009/2010), accompanied by the launch of home-grown Chinese applications such as WeChat (微信, weixin) in 2011 (The Economist 2016). These were also the years (2008-2012) when development of 4G at 3GPP was conducted and Chinese companies participated in them. Furthermore, after 2007 Huawei's participation in the IETF increased steeply (Arkko 2021). Following the 2013 PRISM scandal, China pushed for ICANN reform internationally, but maintained its participation in it as per Chapter 3 and the newly-established Xi Jinping presidency (2012/2013) maintained continuity with its predecessors in the management of the online activities. It was enhanced with a few major measures: the 2017 closure of WhatsApp in China (B. Haas 2017), the aforementioned DNS rules, and the crackdown on domestic *big techs* that began in late 2020 with antitrust measures against Alibaba and is ongoing at the time of writing (Nanni 2022).

Considering this development, the growing dependence of China's major international companies (such as Huawei (Brown 2021)) on domestic market revenues can reinforce state control on Chinese private actors. This can impact multistakeholderism as formally private actors would de facto be tools for governmental influence in the governance mechanism. However, this cannot be established at the current stage. Instead, one can first draw conclusions in historical hindsight on the role of Chinese stakeholders in Internet fragmentation. Before concluding, this can then be connected to their role in ICANN-centred multistakeholder Internet governance as illustrated above and in Chapter 4.

First of all, it can be safely affirmed that the Chinese government has always sought to exercise strict control on the Internet and on online activities. In addition to the aforementioned examples, a 2019 report by the technology company Oracle stressed that China's way to connect to the global Internet is peculiar (Allen 2019): only domestic companies interconnect in China at Internet exchange points (IXPs) and when data is transferred within the country, it is routed exclusively within China, whereas in most other countries data travels from senders to recipients through links based in other countries. Conversely, almost no other country relies on China for domestic traffic according to Oracle. At the same time, this report finds that when Chinese users connect to the global Internet, traffic mostly goes through the US (Allen 2019). The report concludes that

> *China could effectively withdraw from the global public internet and maintain domestic connectivity (essentially having an intranet). This means the rest of the world could be restricted from connecting into China, and vice versa for external connections for Chinese businesses/users.*
>
> *Conversely, China is uniquely dependent upon the West. [Circa] 63% our measurements into China are coming through the United States. If that connectivity were impacted by a global event, we would expect users in China could feel a significant impact* (Allen 2019).

In other words, China's increased control on the Internet limits content and

services, with both a political and economically protectionist goal (Shen 2021) and enhances the capacity of the Chinese government of potentially preventing users and content providers within China to connect to users and content providers outside China and vice-versa. Paradoxically, this creates a form of independence but also of vulnerability, as illustrated by Allen (2019). This also purports China's unwillingness to detach from the global Internet. While China constantly seeks to enhance its regulatory and technical control over what goes on in cyberspace, aligning it to domestic regulation (Mueller 2017), it maintains connectivity to the global Internet and adopts the same transport and identification protocols as the rest of the world (Arsène 2018; Mueller 2017).

Furthermore, China never established a truly separate DNS. When one was developed, Chinese authorities ensured it would be interoperable with the ICANN-supervised DNS and such unconventional split only lasted until ICANN accepted to recognise Chinese actors' requests on Chinese-characters IDNs (Arsène 2015), as illustrated in Chapter 3. Simply put, China could possess the tools and capacity to create a separate DNS root and establish standards alternative to TCP/IP for device identification and data transfer, thus establish a technically incompatible *splinternet*. However, this would be costly in terms of development and establishment (Mueller 2017; 2020b) and would hamper scale economies. As a large group of interview participants familiar with IETF work maintained, companies like Huawei see no advantage in having to produce technically different devices for different markets. On the contrary, potential for technical Internet fragmentation is most likely to come from a political push rather than economic interest. However, this is currently not on Chinese elite's radar: first, a country's capacity to influence decision-making is strongly tied to its domestic companies' capacity to influence standard-making in such venues as the IETF. Second, the latter capacity is strongly tied to a company's economic weight, which in the global digital market depends on the global reach of its production.

To go back to the second working statement on critical Internet resources governance, it is safe to say that the increased participation and influence of Chinese stakeholders in the IETF has not enhanced the likelihood of new

incompatible Internet standards being established. The need for scalability in Internet-connected technologies, along with the normative path dependence generated by the need for consensus in IETF decision-making process, create an incentive mechanism for Chinese stakeholders to adapt to and adopt existing norms (including technical protocols) on the Internet and its governance. To foster domestic control on information fluxes on the Internet, China resorted to regulatory alignment instead of technical fragmentation to avoid losing network benefits, as theorised by Mueller (2017).

The statements on multistakeholderism and Internet fragmentation illustrated in this section must be qualified by explicating a number of unknowns. To start with, the emerging restrictions on big techs in China, connected to Huawei's growing dependence on its domestic market, can foster governmental control on private stakeholders. This could enhance state power in private-based governance. After all, a number of research participants have shown scepticism on China's likelihood to acknowledge ICANN and accept existing architectural designs in the long run. Such interpretations stem variably from the unknowns around such technologies as the New IP/FVCN, China's dominance in multilateral fora such as the ITU, the strong control on content and data fluxes exercised by the government, and the characteristics of the architecture illustrated above. Furthermore, literature voicing this scepticism has emerged, also hinting at the possibility that Chinese government-driven technological development may bring forms of technical fragmentation. For example, Hoffmann, Lazanski and Taylor (2020) maintain that the Chinese government-driven technological development is in fact enhancing state influence in Internet governance and could result in a technical split in the worst-case scenario where such solutions were not to integrate with those promoted by other global actors. After all, the techno-nationalist lens has often been adopted in the study of Chinese technological development (Kim, Lee, Kwak 2020; Plantin, De Seta 2019).

Nonetheless, convergence in standards, the unwillingness of Chinese stakeholders to establish a separate DNS root, and their increased participation and influence in such fora as ICANN, IETF, and 3GPP all paint a picture of

increased integration of Chinese stakeholders in the existing governance mechanisms and acceptance of existing Internet standards. This holds despite the persistence of ambiguities in public-private relations and positioning towards multilateral fora on China's part, along with the question of alignment of the Internet to national regulation that does not encompass China alone.

6.4 *Drawing conclusions*

This thesis has cast new light on the interaction between Chinese public and private actors, on the one hand, and Internet governance, on the other. It adds to theoretical and empirical innovation to IR-informed literature on Internet governance with new empirical nuances and a mixed methodological approach. Furthermore, it contributes to bridging gaps among IR Theory, STS, and China Studies. However, a number of research paths remain open. This conclusive section addresses these aspects.

6.4.1 *Empirical findings and their academic and policy relevance*

Chinese stakeholders have adapted to multistakeholderism and refrained from establishing a *splinternet*. This entails acceptance of private-based governance at ICANN, IETF and 3GPP, as well as no fragmentation at the technical level, whereby China adopts TCP/IP and the IANA-endorsed DNS in its domestic infrastructure. Furthermore, in the standardisation process of 5G, Chinese stakeholders sought to lead the making of a universally compatible standard at 3GPP instead of promoting a separate domestically implemented one as they did with 3G. To foster societal control, China resorted to alignment of the Internet to national regulation (Mueller 2017), rather than establishing a separate network.

This counters the narrative spread in part of the media, policy, and scholarly communities of China as a monolithic national actor that is re-writing

the Internet's rules, its standards, and pushing for the creation of a separate *splinternet*. On the contrary, what emerges here is a portrait of Chinese stakeholders as norm entrepreneurs that push forward measures of contestation through such practices as forum-shopping (Leal-Arcas, Morelli 2018), and that adapt to the existing normative settings when that allows them to influence decision-making. In this context, Chinese stakeholders prefer technical interoperability over a split network to retain scale economies (Mueller 2017).

To be sure, underlying changes and tensions exist in the development of the Internet infrastructure and Internet-enabled technologies. While mobile connectivity is dependent on TCP/IP, it is in turn putting strain on the latter's functioning as anticipated in the introductory chapters. Furthermore, the growing reliance on 5G infrastructure for Internet-based connectivity is creating new forms of overlap and interdependence between Internet and mobile telephony infrastructure. For example, sectors of the literature observe that IOT development is bringing myriads of Internet-connected devices based on the 5G infrastructure for Internet connectivity onto the market and among the usership. As 5G is a telephony infrastructure, its network is centralised and fully determined as opposed to the Internet's traditional building-blocs architecture where intelligence is at the periphery (devices) as previously described in this thesis. This development therefore entails reliance on a more centralised infrastructure for a growing number of Internet connections, with potential implications for the future models of development of the Internet infrastructure itself (Ten Oever 2020). Multistakeholder, private-based Internet governance remains a site of contestation and China (along with other state actors) is seeking to reassert authority on the Internet architecture (Haggart, Scholte, Tusikov 2021).

The extent to which this will trigger the emergence of new actors and power dynamics within the existing governance settings and fora is unknown, as well as the potential changes in governmental influence through market actors in the near future. In the case of China, such influence could be enhanced through its ongoing antitrust crackdown on domestic *big techs* and the latter's growing dependence on China's domestic market amid the US-

China technological and commercial competition. Furthermore, a trend towards centralised infrastructure could yield change in these dynamics (Allen 2019; Douzet 2021).

These aspects are open for further research in the forthcoming years. However, at this stage, the existing multistakeholder, private-based Internet governance regime complex centred on ICANN shows resilience and such powerful actors as China and its domestic stakeholders show interest in and gain advantage from participating in it. As norm entrepreneurs, Chinese stakeholders have adapted to and adopted the existing normative ecosystem to a large extent, while keeping venues for contestation open (Negro 2020).

6.4.2 *Theoretical implications and their relevance*

In theoretical terms, these findings show that the regime complex for Internet governance is characterised by such resilience as to incentivise emerging powers to adapt to and integrate in, rather than contest, the existing normative order (Leal-Arcas, Morelli 2018). All in all, the concept of regime complexity proves useful in conceptualising Internet governance and in identifying the venues of influence in decision-making and how they intersect. This helped in making sense of normative rigidity and why norm entrepreneurs may choose adaptation over contestation. However, it must be acknowledged that such normative rigidity does not stem only from regime complexity in and of itself, but also from the specific characteristics of the regime complex in question. As illustrated, Internet standards and standards for Internet-based technologies need scalability to be economically viable. Thus, an extent of coordination on standards is better than no coordination at all for most actors. This creates an incentive for actors to integrate in existing standard-making processes when drifting or reforming them is not feasible.

Such findings carry implications for theorisation on the Liberal International Order at large as illustrated in the previous section. In this view, this thesis contributes to the literature addressing normative contestation within the order itself, rather than the existential challenges à la Mearsheimer (2019).

In doing so, this work added a methodological and conceptual contribution. By systematically including technologists' views (through interviews) and behaviour (through network analysis) in this study, this thesis contributed to filling a gap in IR Theory, namely the tendency to overlook technologists' contribution to technology-related politics and its making (Tanczer, Brass, Carr 2018). As a matter of fact, a tendency to treat technical aspects as separate from politics is very much present in society at large, with decades of technical as well as social literature addressing the non-neutrality of technology (Polgar 2010; Strate 2012; Whelchel 1986). Nonetheless, the need to combine technical expertise and social-scientific approaches in studying the politics that affects the Internet infrastructure emerges powerfully also by reading the IETF's own mission statement: "The Internet isn't value-neutral, and neither is the IETF" (Alvestrand 2004).

To summarise, this thesis contributes to theorisation on the Liberal International Order amid the rise of China from a regime-theoretic perspective. It has done so by addressing critical conceptual aspects anticipated in other sectors of technology-related social-scientific literature, such as STS, but are not mainstreamed in IR Theory yet.

6.4.3 *Caveats and future venues for research*

The findings of this thesis have been qualified all throughout the process by three major caveats. First, the author is not a technologist, which made access to technical knowledge more complicated and most often filtered through the eyes of interview participants possessing technical expertise. Second, the author speaks Chinese but is not a native speaker. Linguistic barriers can be a major obstacle, especially when they involve languages with no common roots, such as Chinese on the one hand and English and Italian on the other. Third, the unknowns around public-private relations in China and the transformation in the relationship between Chinese state and big techs that is ongoing at the time of writing make some of this thesis conclusions subject to potential revision in the near future. These three caveats add to the ethical and

positionality issues addressed in Chapter 2. Furthermore, Russia's 2022 aggression to Ukraine (ongoing at the time of writing) fostered new debates on Internet fragmentation, this time without China as its main protagonist (Internet Society 2022a).

Such caveats suggest that future research would benefit from studies involving experts cutting across the areas of IR Theory, China Studies, Media Studies, and Computer Science, an interdisciplinarity issue that this thesis has sought to partially address. Furthermore, the Internet's and Internet-based technology's developments are path-dependent but fast, with fewer than ten years separating the beginning of 3G rollout in most continents and the earliest 3GPP 5G-related release. Such changes have the potential to affect future developments of the Internet infrastructure at a fundamental level, as emphasised throughout this thesis (Ten Oever 2020). The development of this latest aspects will also depend on the way in which the outcomes of the ITU's 2020 World Telecommunication Standardization Assembly (WTSA-20) – held in March 2022 owing to the Covid-19 pandemic – will concretise in standardisation terms. Held every four years, WTSA sets out the period of study for ITU-T. According to the Internet Society (2022b), the content of the Resolutions approved and modified at WTSA-20 on the non-radio aspects of telecommunications standards will affect Internet-based networking. Nonetheless, delays due to the Covid-19 pandemic delayed such standardisation activities, leaving their medium- and long-term assessment outside the scope of this thesis.

The same speed of change is visible in China's domestic environment and in the transforming relations between the state and its domestic companies, protected through the Golden Shield Project (Shen 2021) but also controlled and cracked down upon through antitrust measures and new data protection mechanisms (Creemers 2021; Zhong 2021). Therefore, the empirical findings of this research will possibly need to be regularly readdressed against the backdrop of emerging issues.

Nonetheless, the theoretical claims advanced in this thesis and the empirical findings illustrated are durable in their relevance albeit subject to

potential change. This is due to three main factors: first, the transferability of findings about Internet governance regime resilience illustrated in the empirical chapters. Second, the long historical perspective taken by this thesis in exploring Chinese stakeholders' stances in their mutability make findings relevant in interpreting their current policy positions. Third, building on the previous one, findings on Chinese stakeholders' adaptation to and contestation of multistakeholderism and the technical foundation of the Internet feed directly into the emerging debate on digital sovereignty and the return of state in Internet governance.

6.4.4 *Concluding remarks*

In conclusion, this thesis contributed to knowledge on Chinese stakeholders in Internet governance generating new data through both emerging and traditional methods. It has cast new light on the behaviour of such actors and their influence on norms in Internet governance. Furthermore, it contributes to regime theory and addresses conceptual and methodological loopholes pre-existent in the literature.

While several research venues remain open and unanswered questions are many, this thesis has brought its own contribution to debates on China's rise and the future of the Liberal International Order, the future of multistakeholderism in Internet governance, and the question of Internet fragmentation. This thesis' contribution on state authority on the Internet infrastructure constitutes ground for future research on such emerging debates as the rise of digital sovereignty.

References

3rd Generation Partnership Project 2009. “Release 8.” https://www.3gpp.org/specifications/releases/72-release-8 (August 27, 2021).

3rd Generation Partnership Project 2020. “3GPP. A Global Initiative.” https://www.3gpp.org/ (October 15, 2020).

3rd Generation Partnership Project 2021a. “LTE.” https://www.3gpp.org/technologies/keywords-acronyms/98-lte (January 15, 2021).

3rd Generation Partnership Project 2021b. “SA3-Security.” https://www.3gpp.org/specifications-groups/sa-plenary/sa3-security (July 6, 2021).

3rd Generation Partnership Project 2021c. “3GPP TR 21.900 V17.1.0 (2021-06).” https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=555 (November 10, 2021).

Abbott, K. W. and Faude, B. 2022. “Hybrid institutional complexes in global governance”, *The Review of International Organizations*. 17: 263-291.

Abramowitz, M. and Bosworth, S. 2006. “America Confronts the Asian Century”, *Current History.* 105 (690): 147-152.

Acharya, A. 2018. *The End of American World Order*. 2nd ed. Cambridge: Polity Press.

African Network Information Centre 2020. “Autonomous System Number (ASN) from AFRINIC.” https://afrinic.net/asn (October 19, 2020)

Allen, D. 2019. “Analysis by Oracle Internet Intelligence Highlights China’s Unique Approach to Connecting to the Global Internet” *Oracle Cloud Infrastructure Internet Intelligence*. July 19. https://blogs.oracle.com/internetintelligence/analysis-by-oracle-internet-intelligence-highlights-china%e2%80%99s-unique-approach-to-connecting-to-the-global-internet (December 18, 2019).

Alter, K. J. and Raustiala, K. 2018. “The Rise of International Regime Complexity”, *Annual Review of Law and Social Science*. 14 (1): 329-349.

Alvestrand, H. 2004. “RFC 3935. A Mission Statement for the IETF”, *IETF Datatracker*. https://datatracker.ietf.org/doc/rfc3935/ (January 10, 2022).

Arkko, J. 2021. “Distribution of Authors per Companies”, *IETF Statistics*. https://www.arkko.com/tools/allstats/companydistr.html (July 21, 2021).

Arsène, S. 2015. “Internet Domain Names in China. Articulating Local Control with Global Connectivity”. *China Perspectives*, (4): 25-34.

Arsène, S. 2018. “China, Internet Governance and the Global Public Interest”. In: Sieckmann, S. and Triebel, O. (eds.) *A New Responsible Power China?*. Online book: HAL Open Science.

Axelrod, R. 1980. “More Effective Choice in the Prisoner's Dilemma”, *Journal of Conflict Resolution*. 24 (3): 379-403.

Belli, L. 2015. “A Heterostakeholder Cooperation for Sustainable Internet Policymaking”, *Internet Policy Review*. 4 (2): 1-21.

Benthall, S. 2021. “Towards a Data Science of Institutional Power: Progress with BigBang”, *IETF Human Rights Protocol Consideration Working Group*. https://datatracker.ietf.org/meeting/110/materials/slides-110-hrpc-towards-a-data-science-of-institutional-power-progress-with-bigbang-00 (October 27, 2021).

Benthall, S., Ten Oever, N., Doty, N., and Becker, C. 2021. “Bigbang”, *Github.com*. August 24. https://github.com/datactive/bigbang (October 27, 2021).

Blanco, B., Fajardo, J. O., Giannoulakis, I., Kafetzakis, E., Peng, S., Pérez-Romero, J., Trajkovska, I., Khodashenas, P. S., Goratti, L., Paolino, M., Sfakianakis, E., Liberal, F. and Xilouris, G. 2017. “Technology Pillars in the Architecture of Future 5G Mobile Networks: NFV, MEC and SDN”, *Computer Standards and Interfaces*. 54 (4): 216-228.

Blondel, V. D., Guillaume, J., Lambiotte, R. and Lefebvre, E., 2008. “Fast Unfolding of Communities in Large Networks”, *Journal of Statistical Mechanics: Theory and Experiment*. 10: 1-12.

Bo, P. 2018. “China, Global Governance, and Hegemony: Neo-Gramscian Perspective in the World Order”, *Journal of China and International Relations.* 6(1): 48-72.

Bradner, S. 1996. “RFC 2026: The Internet Standards Process - Revision 3”, *IETF Datatracker*. https://datatracker.ietf.org/doc/html/rfc2026 (May 28, 2021).

Brady, A. 2017. “Plus ça change?: Media Control Under Xi Jinping”, *Problems of Post-Communism*. 64 (3): 128-140.

Brown, A. 2021. “Huawei's Global Troubles Spur Beijing’s Push for Self-reliance”, *Mercator Institute for China Studies*. June 1. https://merics.org/en/short-analysis/huaweis-global-troubles-spur-beijings-push-self-reliance (June 18, 2021).

Buckley, C. and Bradsher, K. 2020. “The Chinese communist party pledged to uphold private companies but stressed that the party ‘leads everything’”, *New York Times Chinese Online Edition*. September 18. https://cn.nytimes.com/asia-pacific/20200918/china-communist-private-business/?utm_source=newslist&utm_medium=email&utm_campaign=new

sletter. (December 21, 2020). [储百亮 and Bradsher, K. (2020). “中共承诺支持民营企业, 但强调党‘领导一切’”. 纽约时报中文网, 9月18号].

Bush, R., Patel, K. and Ward, D. 2019. “RFC 8654. Extended Message Support for BGP”, *Internet Engineering Task Force*.

Buzan, B. 2010. “China in International Society: Is ‘Peaceful Rise’ Possible?”, *The Chinese Journal of International Politics*. 3 (1): 5-36.

Buzan, B. 2014. *An Introduction to the English School of International Relations*. Cambridge: Polity Press.

Cai, C. 2018a. “Global Cyber Governance. China’s Contribution and Approach”, *China Quarterly of International Strategic Studies*. 4 (1): 55–76.

Cai, C. 2018b. “China and Global Cyber Governance: Main Principles and Debates”, *Asian Perspectives*. 42 (4): 647-662.

Camarillo, G. and Livingood, J. 2020. “RFC 8712: The IETF-ISOC Relationship”, *IETF Datatracker*. https://datatracker.ietf.org/doc/html/rfc8712 (May 28, 2021).

Carr, M. 2015. “Power Plays in Global Internet Governance”, *Millennium: Journal of International Studies*. 43 (2): 640-659.

Cath, C. 2021. “The Technology We Choose to Create: Human Rights Advocacy in the Internet Engineering Task Force”, *Telecommunications Policy*. 45 (6). https://doi.org/10.1016/j.telpol.2021.102144.

Chan, G., Lee, P. K. and Chan, L. H. 2011. *China Engages Global Governance. A New World Order in the Making?*. London: Routledge.

Chan, L. H., Lee P. K. and Chan, G. 2008. “Rethinking Global Governance: A China Model in the Making?”, *Contemporary Politics*. 14 (1): 3-19.

China Communications Standards Association 2020. “CCSA Organisational Structure.”

http://www.ccsa.org.cn/orgnization?title=%E7%BB%84%E7%BB%87%E6%9E%B6%E6%9E%84 (November 11, 2020). [中国通信标准化协会2020. 中国通信标准化协会组织机构].

China Communications Standards Association 2021. “The Organization Behind 5G Global Standards.” http://www.ccsa.org.cn/dqzz?desc=2538&link=2539&list=92&title=3GPP (January 21, 2021).

Ciuriak, D. 2019. “The US-China Trade War: Technological Roots and WTO Responses”, *Global Solutions Journal*. 4: 130-135.

Clapham, A. 2022. “Non-State Actors”. In: Moeckli, D., Shah, S. and Sivakumaran, S. (eds.) *International Human Rights Law*. 3rd ed. Oxford: Oxford University Press.

Conrad, D. 2020. “Brief Overview of the Root Server System (OCTO-010)”, *ICANN Office of the Chief Technology Officer*. May 6. https://www.icann.org/en/system/files/files/octo-010-06may20-en.pdf (October 19, 2021).

Council on Foreign Relations 2017. “The Case of .Amazon and What It Means For ICANN”. October 4. https://www.cfr.org/blog/case-amazon-and-what-it-means-icann (May 27, 2021).

Creemers, R. 2020a. “China’s Conception of Cyber Sovereignty: Rhetoric and Realization”. In: Broeders, D. and Van den Berg, B. (eds.) *Governing Cyberspace. Behavior, Power, and Diplomacy*. London: Rowman and Littlefield.

Creemers, R. 2020b. *China’s Approach to Cyber Sovereignty*. Konrad Adenauer Stiftung.

Creemers, R. 2021. “China’s Emerging Data Protection Framework”, *SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3964684 (December 21, 2021).

Cross Community Working Group Accountability 2015. “Stress Tests”. *Internet Corporation for Assigned Names and Numbers*.

Dahlman, E., Parkvall, S. and Sköld, J. 2016. *4G, LTE-Advanced Pro and The Road to 5G*, 3rd ed., London: Elsevier.

Deibert, R. J. 2009. “The Geopolitics of Internet Control. Censorship, Sovereignty, and Cyberspace”. In: Chadwick, A. and Howard, P. N. (eds.) *Routledge Handbook of Internet Politics*. London and New York: Routledge

DeNardis, L. 2014. *The Global War for Internet Governance*. New Haven and London: Yale University Press.

DeNardis, L. 2016. “One Internet: an Evidentiary Basis for Policy Making on Internet Universality and Fragmentation”. In: Global Commission on Internet Governance (ed.) *A Universal Internet in a Bordered World. Research on Fragmentation, Openness and Interoperability*. Waterloo (CA) and London: CIGI and Chatham House.

DeNardis, L. and Musiani, F. 2016. “Governance by Infrastructure”. In: Musiani, F., Cogburn, D., DeNardis, L. and Levinson, N. S. (eds.) *The Turn to Infrastructure in Internet Governance*. Basingstoke: Palgrave Macmillan.

Deudney, D. and Ikenberry, G. J. 2018. “The Resilient Order”, *Foreign Affairs*. July/August. https://www.foreignaffairs.com/articles/world/2018-06-14/liberal-world (March 23, 2020).

DiploFoundation 2015. *Multistakeholderism in IGF Language*. http://www.diplomacy.edu/IGFLanguage/multistakeholderism (November 25, 2020).

Doffman, Z. 2020. “Huawei suddenly gives millions of users this surprise Google alternative”, *Forbes*. March 20. https://www.forbes.com/sites/zakdoffman/2020/05/20/huawei-surprises-

millions-of-users-with-critical-google-replacement/#5cb6d66b6caa. (December 21, 2020).

DotAsia 2019. ".Asia Top-Level-Domain Now Licensed for Sale in Chi-na". 12 February. https://www.dot.asia/asia-top-level-domain-now-licensed-for-sale-in-china/ (May 3, 2021).

DotAsia 2021. ".asia". https://www.dot.asia/ (May 3, 2021).

Douzet, F. 2021. "The Shrinking of Cyberspace: A Blind Spot of Cyber Policy". *The Hague Programme for Cyber Norms*. https://www.thehaguecybernorms.nl/conference-2021-speakers/frederick-douzet (November 17, 2021).

Drahokoupil, J., McCaleb, A., Pawlicki, P. and Szunomár, A. 2017. "Huawei in Europe: Strategic Integration of Local Capabilities in a Global Production Network". In: Drahokoupil, J. (ed.) *Chinese Investment in Europe: Corporate Strategies and Labour Relations*. Brussels: ETUI.

Drake, W. J., Cerf, V. G. and Kleinwächter, W. 2016. *Internet Fragmentation: An Overview*. Davos: World Economic Forum.

Duncombe, C. and Dunne, T. 2018. "After liberal world order", *International Affairs*. 94 (1): 25-42.

Durand, A. 2020. "New IP", *ICANN OCTO-017*. October 27. https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf (November 26, 2020).

Economist, The 2016. "WeChat's World". August 6. https://www.economist.com/business/2016/08/06/wechats-world (September 20, 2021).

Economist, The 2020. "America's war on Huawei nears its endgame". 16 July. https://www.economist.com/briefing/2020/07/16/americas-war-on-huawei-nears-its-endgame (October 30, 2020).

Ermert, M. and Hughes, C. R. 2003. " What's in a Name? China and the Domain Name System". In: Hughes, C. R. and Wacker, G. (eds.) *China and The Internet: Politics of the Digital Leap Forward*. London: Routledge, 127-138.

European Telecommunications Standards Institute 2020a. "3GPP". https://www.etsi.org/committee/1418-3gpp (November 11, 2020).

European Telecommunications Standards Institute 2020b. "Our Structure". https://www.etsi.org/about/our-structure (November 11, 2020).

Finnemore, M. and Hollis, D. B. 2016. "Constructing Norms for Global Cybersecurity", *The American Journal of International Law*. 110 (3): 425-479.

Finnemore, M. and Sikkink, K. 1998. "International Norm Dynamics and Political Change", *International Organization*. 52 (4): 887-917.

Fishman, G. 2012. “Decision-Making and Approval Procedures: Soft and Hard Decisions”, *International Telecommunication Union*. October 30-31. https://www.itu.int/en/ITU-T/tutorials/Documents/201210/Session-06-Rapporteur%20Tutorial%201208G-Decision_Making.pdf (October 22, 2020)

Flonk, D., Jachtenfuchs, M. and Obendiek, A. S. 2020. “Authority conflicts in internet governance: Liberals vs. sovereigntists?”, *Global Constitutionalism*. 9 (2): 364-386.

Flor Cruz, J. A. and Seu, L. 2014. “From Snail Mail to 4G, China Celebrates 20 Years of Internet Connectivity”, *CNN*. April 24. https://edition.cnn.com/2014/04/23/world/asia/china-internet-20th-anniversary/index.html (September 20, 2021).

Forst, R. and Günther, K. 2011. “Die Herausbildung Normativer Ordnungen. Zur Idee Eines Interdisziplinären Forschungsprogramms.” In: Forst, R. and Günther, K. (eds.) *Die Herausbildung Normativer Ordnungen. Interdisziplinäre Perspektiven*. Frankfurt: Campus.

Friedberg, A. L. 2005. “The Future of U.S.-China Relations: Is Conflict Inevitable?”, *International Security*. 30 (2): 7-45.

Fukuyama, F. 1989. “The End of History?”, *The National Interest*. 16: 3-18.

Gabusi, G. 2019. “Global Standards in the Asian Infrastructure Investment Bank: The Contribution of the European Members”, *Global Policy*. 10 (4): 631-638.

Galloway, T. 2015. *China and Technical Global Internet Governance: From Norm-Taker to Norm-Maker?*. PhD Thesis. Deakin University.

Ginsberg, L., Previdi, S., Wu, Q., Tantsura, J. and Filsfils, C. 2019. “RFC 8571. BGP - Link State (BGP-LS) Advertisement of IGP Traffic Engineering Performance Metric Extensions”, *Internet Engineering Task Force*.

Glaser, C. 2011. “Will China's Rise Lead to War? Why Realism Does Not Mean Pessimism”, *Foreign Affairs*. 90 (2): 80-91.

Glen, C. M. (2014) “Internet Governance: Territorializing Cyberspace?”, *Politics and Policy*. 42 (5): 635-657.

Gómez-Mera, L. 2016. “Regime Complexity and Global Governance: The Case of Trafficking in Persons”, *European Journal of International Relations*. 22 (3): 566-595.

Gong, Y. 2019. “Standardisation Boosts National Governance Systems and Governance Capabilities. A Basic Analysis of the Modernisation Drive”, *16th Chinese Standardisation Forum Paper Collection*. 11-249. http://www.china-cas.org/u/cms/www/201910/30142846q7r0.pdf (October 20, 2020). [龚月芳 2019. “标准化助推国家治理体系与治理能力. 现代化建设浅析”. 第16届中国标准化论坛论文集, 11-249]

Governmental Advisory Committee 2015a. “Dublin – Board and GAC Meeting”. October 21. https://meetings.icann.org/en/constituency/governmental-advisory-committee-gac?page=4 (July 6, 2021).

Governmental Advisory Committee 2015b. “Governmental Advisory Committee (GAC): Minutes of Meeting. ICANN 54 Dublin”. https://gac.icann.org/contentMigrated/icann54-dublin-meeting-minutes (May 19, 2021).

Guttman, E. 2018. “5G Standardisation in 3GPP”, *International Telecommunication Union*. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201807/Documents/3_Erik_Guttman.pdf (May 28, 2021).

Haas, B. 2017. “China Blocks WhatsApp Services as Censors Tighten Grip on Internet”, *The Guardian*. July 19. https://amp.theguardian.com/technology/2017/jul/19/china-blocks-whatsapp-services-as-censors-tighten-grip-on-internet (September 20, 2021).

Haas, P. M. 1993. “Epistemic Communities and the Dynamics of International Environmental Cooperation”. In: Rittberger, V. (ed.) *Regime Theory and International Relations*, Oxford: Oxford University Press, 168-201.

Haggart, B., Scholte, J. A. and Tusikov, N. 2021. “Introduction. Return of the State?”. In: Haggart, B., Tusikov, N. and Scholte, J. A. (eds.) *Power and Authority in Internet Governance. Return of the State?*. London: Routledge.

Haggart, B., Tusikov, N. and Scholte, J. A. (eds.) 2021. *Power and Authority in Internet Governance. Return of the State?*. London: Routledge.

Harcourt, A., Christou, G. and Simpson, S. 2020. *Global Standard Setting in Internet Governance*. Oxford: Oxford University Press.

Hoffmann, S., Lazanski, D. and Taylor, E. 2020. “Standardising the Splinternet: How China’s Technical Standards Could Fragment the Internet”, *Journal of Cyber Policy*. 5 (2): 239-264.

Hofmann, S. C. 2019. “The politics of overlapping organizations: hostagetaking, forum-shopping and brokering”, *Journal of European Public Policy*. 26 (6): 883-905.

Hofmann, J., Katzenback, C. and Gollatz, K. 2017. “Between Coordination and Regulation: Finding the Governance in Internet Governance”, *New Media and Society*. 19 (9): 1406-1423.

Hogewoning, M. 2011. “IPv4 and IPv6”, *RIPE NCC*. April 4. https://www.ripe.net/about-us/press-centre/publications/presentations/2011/ipv4-and-ipv6 (January 6, 2022).

Hogewoning, M. 2020. “Update on WTSA-20 Preparations and New IP”, *RIPE NCC*. November 10.

https://labs.ripe.net/Members/marco_hogewoning/update-on-wtsa-20-preparations-and-new-ip (November 26, 2020).

Huawei 2021. "History." https://www.huawei.eu/who-we-are/history (January 18, 2021).

Hurel, L. M. and Santoro Rocha, M. 2018. "Brazil, China and Internet Governance: Mapping Divergence and Convergence", *Journal of China and International Relations*. Special issue: 98-115.

Hurel, L. M. and Lobato, L. C. 2018. "Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs", *Journal of Cyber Policy*. 3 (1): 61-76.

Huston, G. 2022. "DNS4EU", *APNIC*. February 11. https://labs.apnic.net/?p=1582&_ga=2.267316558.1542866134.1649672277-585079642.1628671470 (April 11, 2022).

Ikenberry, G. J. 2008. "The Rise of China and the Future of the West - Can the Liberal System Survive?", *Foreign Affairs*. 87 (1): 23-37.

Ikenberry, G. J. 2011. *Liberal Leviathan: The Origins, Crisis, and Transformation of the American World Order*. Princeton: University Press.

Ikenberry, G. J. 2018. "The End of Liberal International Order?", *International Affairs*. 94 (1): 7-23.

Institute of Electrical and Electronics Engineers 2013. "Silicon and the Wide Bandgap Semiconductors, Shaping the Future Power Electronic Device Market". *IEEEXplore*. https://doi.org/10.1109/ULIS.2013.6523479 (July 15, 2021).

Institute of Electrical and Electronics Engineers 2019. "IEEE Lifts Restrictions on Editorial and Peer Review Activities". June 2. https://www.ieee.org/about/news/2019/statement-update-ieee-lifts-restrictions-on-editorial-and-peer-review-activities.html (July 8, 2021).

International Business Machines Corporation 2020. "TCP/IP Protocols". https://www.ibm.com/docs/en/aix/7.1?topic=protocol-tcpip-protocols (May 14, 2021).

International Telecommunication Union 2005. "Tunis Agenda for the Information Society." WSIS-05/TUNIS/DOC/6(Rev.1)-E. https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html (December 18, 2019).

International Telecommunication Union 2020a. "International Telecommunication Regulations." https://www.itu.int/en/wcit-12/Pages/itrs.aspx (October 20, 2020).

International Telecommunication Union 2020b. "ITU towards 'IMT for 2020 and beyond'". https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx (October 15, 2020).

International Telecommunication Union 2020c. “ITU completes evaluation for global affirmation of IMT-2020 technologies”, *Press Release*. November 26. https://www.itu.int/en/mediacentre/Pages/pr26-2020-evaluation-global-affirmation-imt-2020-5g.aspx (January 14, 2021).

International Telecommunication Union 2021. “New ITU standards optimize transport networks support for IMT-2020/5G”, *ITUNews*. March 15. https://www.itu.int/en/myitu/News/2021/03/15/12/36/New-ITU-standards-optimize-transport-networks-support-for-5G (May 28, 2021).

Internet Assigned Numbers Authority 2019. “IPv4 Recovered Address Space.” March 1. https://www.iana.org/assignments/ipv4-recovered-address-space/ipv4-recovered-address-space.xhtml (April 4, 2022).

Internet Corporation for Assigned Names and Numbers 1999. “Memorandum of Understanding between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers.” https://www.icann.org/resources/unthemed-pages/icann-mou-1998-11-25-en (July 22, 2020).

Internet Corporation for Assigned Names and Numbers 2002. *ICANN Archives*. https://archive.icann.org/en/meetings/shanghai/ (August 19, 2021).

Internet Corporation for Assigned Names and Numbers 2011. *ICANNWiki*. https://icannwiki.org/ (October 30, 2020).

Internet Corporation for Assigned Names and Numbers 2013. “Procedure to Develop and Maintain the Label Generation Rules for the Root Zone in Respect of IDNA Labels.” 20 March. https://www.icann.org/en/system/files/files/lgr-procedure-20mar13-en.pdf (May 26, 2021).

Internet Corporation for Assigned Names and Numbers 2015. “Internationalized Domain Names”. *New Generic Top-Level Domains*. https://newgtlds.icann.org/en/about/idns (May 3, 2021).

Internet Corporation for Assigned Names and Numbers 2017. “.amazon.” *ICANNWiki*. https://icannwiki.org/.amazon (January 10, 2021).

Internet Corporation for Assigned Names and Numbers 2020. “Regional Internet Registry.” *ICANNWiki*. https://icannwiki.org/Regional_Internet_Registry (December 17, 2020).

Internet Corporation for Assigned Names and Numbers 2019. “Bylaws for Internet Corporation for Assigned Names and Numbers. A California Nonprofit Public-Benefit Corporation.” November 28. https://www.icann.org/resources/pages/governance/bylaws-en (May 27, 2021).

Internet Corporation for Assigned Names and Numbers 2021. “Generation Panel.” https://www.icann.org/resources/pages/generation-panel-2015-06-21-en (May 26, 2021).

Internet Engineering Steering Group 2014. "[Ianaplan] WG Action: Formed Planning for the IANA/NTIA Transition (ianaplan)." *IETF Mail Archive*. September 8. https://mailarchive.ietf.org/arch/browse/ianaplan/?q=blanchet&so=date (April 4, 2022).

Internet Engineering Task Force 2020. "Internet Standards." https://ietf.org/standards/ (February 5, 2020).

Internet Engineering Task Force 2021a. "Note Well". https://www.ietf.org/about/note-well/ (May 28, 2021).

Internet Engineering Task Force 2021b. "Draft/RFC Statistics." https://datatracker.ietf.org/stats/document/author/documents/ (July 21, 2020).

Internet Engineering Task Force 2021c. "Datatracker." https://datatracker.ietf.org/ (January 6, 2022).

Internet Society 2017. "State of IPv6 Deployment 2017". May 25. https://www.internetsociety.org/resources/doc/2017/state-of-ipv6-deployment-2017/ (July 19, 2021).

Internet Society 2022a. "Defend the Internet, Stop the Splinternet". April 7. https://www.internetsociety.org/news/statements/2022/defend-the-internet-stop-the-splinternet/ (April 12, 2022).

Internet Society 2022b. "ITU World Telecommunication Standardization Assembly 2020 (WTSA-20) – Summary Issues Matrix". April 5.

IPLytics 2020. "Connectivity and 5G. The Next Technology Revolution and Standard Essential Patents", *Virtual Boardroom Series Report*. https://www.iplytics.com/report/virtual-boardroom-report-connectivity-5g/ (October 30, 2020).

ITU Development Sector 2021. "Mobile Communications", *International Telecommunication Union*. https://www.itu.int/ITU-D/tech/MobileCommunications/IMT_INTRODUCING/IMT_2G3G4G.html (May 28, 2021).

Jia, L. and Winseck, D. 2018. "The Political Economy of Chinese Internet Companies: Financialization, Concentration, and Capitalization", *International Communication Gazette*. 80 (1): 30-59.

Jiang, M. 2010. "Authoritarian Deliberation on Chinese Internet", *The Electronic Journal of Communication*. 20 (3): 1-22.

Jiang, M. 2012. "Internet Companies in China. Dancing between the Party Line and the Bottom Line", *AsieVision*. 47.

Jongen, H. and Scholte, J. A. 2021. "Legitimacy in Multistakeholder Global Governance at ICANN", *Global Governance*. 27 (2): 298-324.

Kania, E. B., Costello, J. K. 2018. *Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership*. Centre for a New American Security.

Kawabata, T. 2020. "Private Governance Schemes for Green Bond Standard: Influence on Public Authorities' Policy Making", *Green Finance*. 2 (1): 35-54.

Keohane, R. O. and Martin, L. L. 1995. "The Promise of Institutionalist Theory", *International Security*. 20 (1): 39-51.

Keohane, R. O. and Victor, D. G. 2011. "The Regime Complex for Climate Change", *Perspectives on Politics*. 9 (1): 7-23.

Kettemann, M. C. 2020. *The Normative Order of the Internet*. Oxford: Oxford University Press.

Kim, M., Lee, H. and Kwak, J. 2020. "The Changing Patterns of China's International Standardization in ICT under Techno-nationalism: A Reflection through 5G Standardization", *International Journal of Information Management*. 54: 1-8.

King, N., Horrocks, C. and Brooks, J. 2019. *Interviews in Qualitative Research*. 2nd ed. London: Sage.

Kissinger, H. 2011. *On China*. New York: Penguin Books.

Klimburg, A. 2013. "The Internet Yalta", *Center for a New American Security*.

Kourandi, F., Krämer, J. and Valletti, T. 2015. "Net Neutrality, Exclusivity Contracts, and Internet Fragmentation", *Information Systems Research*. 26 (2): 320-338.

Krasner, S. D. 1982. "Structural Causes and Regime Consequences: Regimes as Intervening Variables", *International Organization*. 36 (2): 185-205.

Leaffer, M. 1998. "Domain Names, Globalization, and Internet Governance", *Indiana Journal of Global Legal Studies*. 6 (1): 139-165.

Leal-Arcas, R. and Morelli, A. 2018. "The Resilience of the Paris Agreement: Negotiating and Implementing the Climate Regime", *Georgetown Environmental Law Review*. 31 (1): 1-64.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G. and Wolff, S. 1997. "Brief History of the Internet", *Internet Society*. https://www.internetsociety.org/internet/history-internet/brief-history-internet/ (May 20, 2021).

Levinson, N. S. and Cogburn, D. L. 2016. "The Next 'Turn' in Internet Infrastructure Governance". In: Musiani, F., Cogburn, D. L., DeNardis, L., Levinson, N. S. (eds.) *The Turn to Infrastructure in Internet Governance*. Basingstoke: Palgrave Macmillan.

Li, R. 2020. “Some Notes on ‘An Analysis of the “New IP” Proposal to the ITU-T’”, *Internet4Future*. June 02. https://internet4future.wordpress.com/2020/06/02/some-notes-on-an-analysis-of-the-new-ip-proposal-to-the-itu-t/ (October 22, 2020).

Lipton, J. D. 2016. “Looking Back on the First Round of New gTLD Ap-plications: Implications for the Future of Domain Name Regulation”. In: Global Commission on Internet Governance (ed.) *Mapping the Digital Frontiers of Trade and Intellectual Property*. London: Royal Institute for International Affairs.

Liu, J. 2020. “China’s Data Localization”, *Chinese Journal of Communication*. 13 (1): 84-103.

Ma, S. (2020). “Political Risk Analysis of Huawei’s International Expansion in the Context of US-China Competition”, *Journal of Contemporary Asia-Pacific Studies*. 13 (1): 4-29. [马骊2020. “中美竞争背景下华为 5G 国际拓展的政治风险分析”. 当代亚太, 13年第1 期: 第 4-29 页]

Mahon, S. 2017. “The 5G Effect on RF Filter Technologies”. *IEEE Transactions on Semiconductor Manufacturing*, 30 (4): 394-399.

Maxigas and Ten Oever, N. 2021. *The People’s 5G Laboratory: Critical Perspectives on Media Technologies*. Amsterdam: The People’s 5G Laboratory.

Mayer, M. 2020. “China’s Authoritarian Internet and Digital Orientalism”. In: Feldner, D. (ed.) *Redesigning Organizations. Concepts for the Connected Society*. Luzern: Springer.

Mearsheimer, J. J. 2001. *The Tragedy of Great Power Politics*. New York: W. W. Norton and Company.

Mearsheimer, J. J. 2006. “China‘s Unpeaceful Rise”, *Current History*. 105 (690): 160-162.

Mearsheimer, J. J. 2019. “Bound to Fail: The Rise and Fall of the Liberal International Order”, *International Security*. 43 (4): 7-50.

Ming, S., and Ouyang, C. 2008. “Beyond 3G”, *Finance Magazine*. 4.

Ministry of Foreign Affairs of the People’s Republic of China 2017. “International Strategy of Cooperation in Cyberspace”. http://www.xinhuanet.com//english/china/2017-03/01/c_136094371_5.htm (July 14, 2021).

Ministry of Industry and Information Technology of the People’s Republic of China 2017. “Internet Domain Name Management Rules”. https://tinyurl.com/49bwc6fw (September 17, 2021). [中华人民共和国工业和信息化部 2017. 互联网域名管理办法]

Morozov, E. 2011. *The Net Delusion: How not to Liberate the World*.

New York: Penguin.

Mueller, M. L. 2010. *Networks and States: The Global Politics of Internet Governance*. Cambridge, US: MIT Press.

Mueller, M. L. 2013. "Are We in a Digital Cold War?", *GigaNet: The Global Governance of the Internet: Intergovernmentalism, Multistakeholderism and Networks*. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.363.2569&rep=rep1&type=pdf (July 18, 2019).

Mueller, M. L. 2017. *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace*. Cambridge: Polity Press.

Mueller, M. L. 2020a. "The Knake-Mueller Wager: Will China Form an Alternate DNS Root?", *Internet Governance Project*. February 26. https://www.internetgovernance.org/2020/02/26/the-knake-mueller-wager-will-china-form-an-alternate-dns-root/ (October 10, 2021).

Mueller, M. L. 2020b. "About that Chinese 'reinvention' of the Internet…", *Internet Governance Project*. March 30. https://www.internetgovernance.org/2020/03/30/about-that-chinese-reinvention-of-the-internet/ (October 22, 2020).

Mueller, M. L. and Badiei, F. 2020. "Inventing Internet Governance: The Historical Trajectory of the Phenomenon and the Field". In: DeNardis, L., Cogburn, D., Levinson, N. and Musiani, F. (eds.) *Researching Internet Governance: Methods, Frameworks, Futures*. Cambridge, US: MIT Press.

Murgia, M. and Gross, A. 2020. "Inside China's Controversial Mission to Reinvent the Internet", *Financial Times*. March 27. https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f (October 22, 2020).

Musiani, F. 2013. "Network Architecture as Internet Governance", *Internet Policy Review*. 2 (4): 1-9.

Musiani, F. 2020. "Science and Technology Studies Approaches to Internet Governance: Controversies and Infrastructures as Internet Politics". In: DeNardis, L., Cogburn, D., Levinson, N. and Musiani, F. (eds.) *Researching Internet Governance: Methods, Frameworks, Futures*. Cambridge, US: MIT Press.

Nanni, R. 2022. "La nascente normativa cinese sulla protezione dei dati personali alla luce dei rapporti tra stato e attori privati", *Comunicazionepuntodoc*. Special issue "Lower the Top".

Negro, G. 2017. *The Internet in China: From Infrastructure to a Nascent Civil Society*. Basingstoke: Palgrave Macmillan.

Negro, G. 2020. "A History of Chinese Global Internet Governance and its Relations with ITU and ICANN", *Chinese Journal of Communication*. 13 (1): 104-121.

NetMundial 2014. “Multistakeholder Statement.” https://www.cgi.br/media/docs/publicacoes/1/16570020190607-CadernosCGIbr_DeclaracaoNETmundial.pdf (October 16, 2020).

Nye, J. S. 2014. “The Regime Complex for Managing Global Cyber Activities”, *Global Commission on Internet Governance Paper Series*, 1. http://www.cigionline.org/publications/regime-complex-managingglobal-cyber-activities (July 25, 2019).

Palladino, N. and Santaniello, M. 2021. *Legitimacy, Power, and Inequalities in the Multistakeholder Internet Governance. Analyzing IANA Transition*. Basingstoke: Palgrave Macmillan.

Pang, Z. and Lye, L. F. 2012. “China and Global Governance”. In: Wang, G. and Zheng, Y. (eds.) *China: Development and Governance*. Singapore: World Scientific.

Parsi, V. E. 2018. *Titanic. The Shipwreck of the Liberal Order*. Bologna: Il Mulino. [Parsi, V. E. 2018. Titanic. Il Naufragio dell’Ordine Liberale. Bologna: Il Mulino].

Petrescu, A. 2021. “[6gip] IP-related New Efforts.” *IETF Mail Archive*. January 15. https://mailarchive.ietf.org/arch/browse/6gip/?gbt=1&q=IP-related%20new%20efforts (April 4, 2022).

Phillips, A. 2013. “A dangerous synergy: energy securitization, great power rivalry and strategic stability in the Asian century”, *The Pacific Review*. 26 (1): 17-38.

Plantin, J. and De Seta, G. 2019. “WeChat as Infrastructure: The Technonationalist Shaping of Chinese Digital Platforms”, *Journal of Chinese Communication*. http://eprints.lse.ac.uk/91520/1/Plantin_WeChat-as-infrastructure.pdf (November 15, 2021).

Poggetti, L. 2021. “EU-China Mappings: Interactions between the EU and China on Key Issues”, *Mercator Institute for China Studies*. 20 January. https://merics.org/de/kurzanalyse/eu-china-mappings-interactions-between-eu-and-china-key-issues (July 13, 2021).

Pohle, J. and Thiel, T. 2020. “Digital Sovereignty”, *Internet Policy Review*. 9 (4). https://doi.org/10.14763/2020.4.1532.

Pohlmann, T., Blind, K. and Hess, P. 2020. *Fact finding study on patents declared to the 5G standard*. Berlin: IPLytics and Technische Universitaet Berlin.

Polgar, J. M. 2010. “The Myth of Neutral Technology”. In: Oishi, M. M. K., Mitchell, I. M. and Van der Loos, H. F. M. (eds.) *Design and Use of Assistive Technology*. Berlin: Springer Nature.

Previdi, S., Filsfils, C., Lindem, A., Sreekantiah, A. and Gredler, H. 2019. “RFC 8669. Segment Routing Prefix Segment Identifier Extensions for BGP”, *Internet Engineering Task Force*.

Pupillo, L. 2019. “5G and National Security”, *CEPS*. 21 June. https://www.ceps.eu/5g-and-nationalsecurity/ (October 20, 2020).

Qin, Y. 2012. *A Relational Theory of World Politics*. Cambridge: Cambridge University Press.

Quinn, B. 2012. “Google Services Blocked in China”, *The Guardian*. November 9. https://www.theguardian.com/technology/2012/nov/09/google-services-blocked-china-gmail (July 6, 2021).

Radu, R. 2019. *Negotiating Internet Governance*. Oxford: Oxford University Press.

Radu, R., Kettemann, M. C., Meyer, T. and Shahin, J. 2021. “Normfare: Norm Entrepreneurship in Internet Governance”, *Telecommunications Policy*. 45 (6): 1-7.

Randriamasy, S., Yang, R. Y., Wu, Q., Deng, L. and Schwan, N. 2020. “RFC 8896. Application-Layer Traffic Optimization (ALTO) Cost Calendar.” *Internet Engineering Task Force*. https://www.ietf.org/proceedings/91/slides/slides-91-alto-3.pdf (April 4, 2022).

Raustiala, K. and Victor, D. 2004. “The Regime Complex for Plant Genetic Resources”, *International Organization*. 58 (2): 277-309.

Raymond, M. and DeNardis, L. 2015. “Multistakeholderism: Anatomy of an Inchoate Global Institution”, *International Theory*. 7 (3): 572-616.

Resnick, P. 2014. “RFC 7282. On Consensus and Humming in the IETF”, *Internet Engineering Task Force*. June. https://tools.ietf.org/html/rfc7282 (July 21, 2020).

RFC Editor 2021. “Official Internet Protocol Standards”. https://tinyurl.com/3x22kre4 (May 28, 2021).

Rosenau, J. N. 1992. “Governance, Order, and Change in World Politics”. In: Rosenau, J. N. and Czempiel, E. (eds.) *Governance without Government: Order and Change in World Politics*. Cambridge: Cambridge University Press.

Russell, A. L. 2013. “OSI: The Internet That Wasn’t”, *IEEE Spectrum*. July 30. https://spectrum.ieee.org/tech-history/cyberspace/osi-the-internet-that-wasnt (November 27, 2020).

Salmons, J. (2015). *Qualitative Online Interviews*. 2nd ed. London: Sage

Santaniello, M. 2021. “From Governance Denial to State Regulation: A Controversy-Based Typology of Internet Governance Models”. In: Haggart, B., Tusikov, N. and Scholte, J. A. (eds.) *Power and Authority in Internet Governance. Return of the State?*. London: Routledge.

Schackleford, S. and Craig, A. 2014. “Beyond the New 'Digital Divide': Analyzing the Evolving Role of National Governments in Internet

Governance and Enhancing Cybersecurity", *Stanford Journal of International Law*. 50 (119): 1-65.

Scholte, J. A. 2017. "Complex Hegemony. The IANA Transition in Global Internet Governance", *GigaNet: Global Internet Governance Academic Network, Annual Symposium 2017*.

Segal, A. 2016. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York: PublicAffairs

Segal, A. 2018. "When China Rules the Web: Technology in Service of the State", *Foreign Affairs*. September/October. https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web (November 10, 2020).

Sharp, H. and Kolkman, O. 2020. "Discussion Paper: An analysis of the 'New IP' proposal to the ITU-T", *Internet Society*. April 24. https://www.internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/#:~:text=%20Key%20Elements%20of%20the%20proposed%20%E2%80%9CNew%20IP%E2%80%9D,transport%20architectures.%20C83%20and%20its%20associated...%20More%20 (October 22, 2020).

Shen, H. 2016. "China and global internet governance: toward an alternative analytical framework", *Chinese Journal of Communication*. 9 (3): 304-324.

Shen, H. 2018. "Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative", *International Journal of Communication*. 12: 2683-2701.

Shen, H. 2021. "On How Tech Really Works behind the Great Firewall", *CIGIOnline*. July 8. https://tinyurl.com/um7dxn4w (July 8, 2021).

Shih, G. 2015. "Exclusive - Huawei CEO says Chinese cybersecurity rules could backfire", *Reuters*. April 21. https://in.news.yahoo.com/exclusive-huawei-ceo-says-chinese-cybersecurity-rules-could-133148214--finance.html (June 16, 2021).

Sin, B. 2020. "What Google ban? How to get Huawei phones working with US apps and services like Google maps and Instagram", *South China Morning Post*. April 1. https://www.scmp.com/lifestyle/gadgets/article/3077689/what-google-ban-how-get-huawei-phones-working-us-apps-and. (December 21, 2020).

Socolofsky, T. and Kale, C. 1991. "RFC 1180: A TCP/IP Tutorial". *IETF Datatracker*. https://datatracker.ietf.org/doc/html/rfc1180#page-2 (May 14, 2021).

State Council Information Office of the PRC 2010. "White Paper on the Internet in China". http://www.scio.gov.cn/zfbps/ndhf/2010/Document/662572/662572.htm

(September 17, 2021). [中华人民共和国国务院新闻办公室2010. 中国互联网状况]

Stewart, J., Shen, X., Wang, C. and Graham, I. 2011. "From 3G to 4G: Standards and the Development of Mobile Broadband in China", *Technology Analysis and Strategic Management*. 23 (7): 773-788.

Strange, S. 1982. "Cave! Hic Dragones: A Critique of Regime Analysis", *International Organization*. 36 (2): 479-496.

Strate, L. 2012. "If It's Neutral, It's Not Technology". *Educational Technology*, 52 (1): 6-9.

Swartz, N. 2006. "China Launches Chinese Language Domains". *Information Management Journal*, 40 (3): 11.

Tanczer, L. M., Brass, I. and Carr, M. 2018. "CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy", *Global Policy*. 9 (3): 60-66

Tang, M. 2020. "From 'Bringing-in' to 'Going-out': Transnationalizing China's Internet Capital Through State Policies", *Chinese Journal of Communication*. 13 (1): 27-46.

Tayal, A. 2021. "5G – Industry 4.0 and Fragmentation of the Internet", *Phronesis Partners*. https://phronesis-partners.com/insights/5g-network-slicing/ (July 22, 2021).

Ten Oever, N. 2020. "Power and Optimization in the Internet Architecture: The Programmable Infrastructure of 5G Networks", *Selected Papers of #AoIR2020: The 21st Annual Conference of the Association of Internet Researchers*.

Ten Oever, N. 2021. "5G and the Notion of Network Ideology, or: the Limitations of Sociotechnical Imaginaries", *Sixteenth Annual Giganet Symposium*.

Ten Oever, N., Milan, S. and Beraldo, D. 2020. "Studying Discourse in Internet Governance through Mailing-List Analysis". In: DeNardis, L., Cogburn, D., Levinson, N. and Musiani, F. (eds.) *Researching Internet Governance: Methods, Frameworks, Futures*. Cambridge, US: MIT Press.

Tilli, J. M. and Kantola, R. 2017. "Data Plane Protocols and Fragmentation for 5G", *IEEE Xplore*. https://doi.org/10.1109/CSCN.2017.8088623 (October 30, 2020).

Tjahja, N., Nanni, R. and Baiduk, R. 2022. "Unpacking digital sovereignty: strategic narratives from China, the European Union, and Russia", *ICA pre-conference: Platform Governance - Sovereignty and the Return of Governance for Digital Platforms*.

Vidal, I., Garcia, J., Valera, F., Soto, I. and Azcorra, A. 2007. "Integration of a QoS Aware End User Network within the TISPAN NGN

Solutions", *IEEEXplore*. https://doi.org/10.1109/ECUMN.2007.29 (August 30, 2021).

Wang, D., Chen, D., Song, B., Guizani, N., Yu, X. and Du, X. 2018. "From IoT to 5G I-IoT: The Next Generation IoT-Based Intelligent Algorithms and 5G Technologies", *IEEE Communications Magazine*. 56 (10): 114-120.

Wang, J. 2011. "China's Search for a Grand Strategy", *Foreign Affairs*. March/April. https://www.foreignaffairs.com/articles/china/2011-02-20/chinas-search-grand-strategy (April 9, 2020).

Wannstrom, J. 2013. "LTE-Advanced", *Third Generation Partnership Project*. https://www.3gpp.org/technologies/keywords-acronyms/97-lte-advanced (July 22, 2021).

Wen, Y. 2020. *The Huawei Model. The Rise of China's Technology Giant*. Champaign: University of Illinois Press.

Wendt, A. 1992. "Anarchy Is What States Make of It: The Social Construction of Power Politics", *International Organization*. 46 (2): 391-425.

Westwinter, O. 2021. "Transnational Public-private Governance Initiatives in World Politics: Introducing a New Dataset", *The Review of International Organizations*. 16 (1): 137-174.

Whelchel, R. J. 1986. "Is Technology Neutral?", *IEEE Technology and Society Magazine*. 5 (4): 3-8.

Winseck, D. 2020. "Is the International Telecommunication Union Still Relevant in 'the Internet Age?' Lessons From the 2012 World Conference on International Telecommunications (WCIT)". In: Balbi, G. and Fickers, A. (eds.) *History of the International Telecommunication Union*. Berlin: De Gruyter.

Working Group on Internet Governance 2005. *Report of the Working Group on Internet Governance*. 05.41622.

World Intellectual Property Organization 2020. "WIPO Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP)." https://www.wipo.int/amc/en/domains/guide/#:~:text=The%20Uniform%20Domain%20Name%20Dispute%20Resolution%20Policy%20%28the,adopted%20the%20UDRP%20Policy%20on%20a%20voluntary%20basis. (January 10, 2021).

Xinhua, 2017, "International Strategy of Cooperation on Cyberspace (full text)". March 1. http://www.xinhuanet.com/politics/2017-03/01/c_1120552767.htm (July 24, 2021) [新华社2017网络空间国际合作战略（全文）]

Xinhua. (2020a). "Adhere to the 'two unshakables'. Bring private enterprises around the party to better promote the healthy development of the private economy". September 17.

http://www.xinhuanet.com/mrdx/2020-09/17/c_139375287.htm. (December 21, 2020) [新华网 (2020). “坚持‘两个毫不动摇’. 把民营经济人士团结在党的周围 更好推动民营经济健康发展”. 9月17号].

Xinhua. (2020b). “Xi focus: Xi stresses promoting healthy development of private sector”. 16 September. http://www.xinhuanet.com/english/2020-09/16/c_139373545.htm. (December 21, 2020).

Yan, X. 2014. “From Keeping a Low Profile to Striving for Achievement”, *The Chinese Journal of International Politics*. 7 (2): 153-184.

Yu, J., Malerba, F., Adams, P. and Zhang, Y. 2017. “Related Yet Diverging Sectoral Systems: Telecommunications Equipment and Semiconductors in China”. *Industry and Innovation*, 24 (2): 190-212.

Yu, Jiang 2011. “From 3G to 4G: Technology Evolution and Path Dynamics in China's Mobile Telecommunication Sector”, *Technology Analysis and Strategic Management*. 23(10): 1079-1093.

Zhang, J. 2019. “Internationalized Domain Names and Universal Acceptance: Spreading the Word in China”, *Internet Corporation for Assigned Names and Numbers*. 8 January. https://www.icann.org/en/blogs/details/internationalized-domain-names-and-universal-acceptance-spreading-the-word-in-china-8-1-2019-en (May 26, 2021).

Zhang, J. and Liang, X. 2007. “3G in China: Environment and Prospect”. *IEEEXplore*. https://ieeexplore.ieee.org/abstract/document/4349642 (Accessed 27 April 2021).

Zheng, B. 2005. “China‘s ‘Peaceful Rise’ to Great- Power Status”. In: Shambaugh, D. (ed.) 2016. *The China Reader*, 6th edition, Oxford: Oxford University Press.

Zhong, R. 2019. “Who Owns Huawei? The Company Tried to Explain. It Got Complicated”, *New York Times*. 25 April. https://www.nytimes.com/2019/04/25/technology/who-owns-huawei.html (October 20, 2020).

Zhong, R. 2021. “China Orders Didi Off App Stores in an Escalating Crackdown”, *New York Times*. July 4. https://www.nytimes.com/2021/07/04/technology/china-didi-app-removed.html (July 6, 2021).

Zhou, X. 2019. “Research on CICT’s 5G Development Strategy Based on the Theory of Competitive Advantage. China National Knowledge Infrastructure.” http://cdmd.cnki.com.cn/Article/CDMD-10013-1019066684.htm (October 20, 2020). [周雪平2020. “基于竞争优势理论的中信科5G场景发展策略研究”. 知网空间]

Zürn, M. 2018. *A Theory of Global Governance. Authority, Legitimacy, and Contestation*. Oxford: Oxford University Press.

APPENDIX A

ELABORATIONS ON METHODOLOGICAL ASPECTS: SEMI-STRUCTURED EXPERT INTERVIEWS

Chapter 2 illustrates the methodological choices operated in this research. Building on it, this appendix provides further details on the interview process. While interviews are kept confidential to allow participants to freely speak their mind, this appendix unpacks the six Internet stakeholder groups illustrated in Chapter 2 (government, international organisations, tech companies, civil society, academia, and technical community) and addresses the challenges encountered in categorising participants into one stakeholder group or the other. After all, categorisations are ideal-typical and stakeholder groups are overlapping – an element that is structural to multistakeholder Internet governance (Palladino, Santaniello 2021).

The twenty-nine participants involved in interviews feature five between Chinese nationals and Chinese-born people. However, it must be stressed that non-Chinese people affiliated to Chinese corporate actors and Chinese people affiliated to Western institutions have been interviewed. In terms of stakeholder groups, the interview participants can be categorised as follows:

- Three participants are affiliated to government, both from the Western hemisphere.
- One participant is member of staff of an international organisation. They are European.
- Nine participants are affiliated to the business sector, two of whom work for Chinese network manufacturers.
- Two participants fall within the scope of civil society and both are Western.
- Seven participants are members of the technical community, affiliated to both Western and Eastern organisations.

- Seven participants are members to academic institutions, featuring both Western and Chinese people.

This taxonomy is imperfect for the reasons illustrated above. For example, the seven participants from the technical community do not encompass companies-affiliated technologists, who have been counted within the business community. Nonetheless, the knowledge and expertise they have access to, especially when their main professional role revolves around standardisation, is that of a member of the technical community.

Conversely, the seven participants classified within the technical community encompass ICANN staff members. This classification has been operated due to the role their organisation plays and its *sui generis* form that distinguishes it from public (state-based) international organisations. Nonetheless, the knowledge they possess and shared during interviews may originate from a business or civil society background rather than a technology one.

Furthermore, the only interview participant counted within the "international organisations" stakeholder group is an international organisation's staff member. Nonetheless, technologists employed by private companies participate in standardisation within such organisations as the ITU, thus adding a further layer of complexity to the classification operated. In this context, an organisation such as the EU, with both supranational and intergovernmental elements, falls in between the "government" and "international organisation" categories.

Briefly, Chinese and Western perspectives were obtained throughout the interview process from each stakeholder group, with the sole exception of government and civil society. No Chinese person affiliated – even unexclusively – to one of these two stakeholder group participated in interviews. This aspect has been addressed within Chapter 2.

APPENDIX B

A SAMPLE INTERVIEW QUESTIONNAIRE

While interviews retained a similar structure across the research process, two slightly different lists of questions have been drafted: one related to critical Internet resources and one related to the mobile connectivity realm. Questions were then adjusted to the interview participant's experience, background, and affiliation.

One element that influenced the length of the question list was the time available to the interview participant. While the general duration of an interview was one hour, the author conducted interviews as short as twenty minutes and as lengthy as three hours.

While the questionnaire contained prompts and follow-up questions, new unanticipated questions have emerged time and again throughout an interview.

The following is a sample interview list of question. Numbered questions are main questions, while questions listed through letters are prompts and follow-ups.

A sample interview questionnaire

On China's engagement in the governance of critical Internet resources:

1. Has China's participation in ICANN GAC increased since its reaccessions in 2009?
2. How does China's participation in GAC compare to Chinese stakeholders' participation in other ICANN bodies and constituencies?
3. How does Chinese participation in ICANN compare to Chinese stakeholders' participation in IETF?

4. What activities are China's government and Chinese non-state stakeholders conducting in the ITU?
5. What types of proposals are generally advanced by the Chinese government in critical Internet resources governance bodies (ICANN GAC and ITU mainly)?
6. How does it compare to the proposals advanced by Chinese non-state stakeholders in ICANN, ITU, and IETF?
7. Between 2007 and 2010 there was a steep increase in CN proposals at IETF, which later remained more or less stable at 2010 level: what is the reason of this steep increase?
8. How did China's participation change in ITU, ICANN, and IETF throughout the periods below? What is your opinion?
    a. Before and after the GAC boycott
    b. From Jiang Zemin's presidency to Hu Jintao's (2003-2013), to Xi Jinping's (2013-now)
    c. Before and after the IANA stewardship transition
9. In critical Internet resources management body:
    a. What is your view on the way in which governments react to Chinese (both government and non-state stakeholders) actions in CIRs governance bodies?
    b. What is your view on the way non-state stakeholders react to Chinese (both government and non-state stakeholders) actions in CIRs governance bodies?
    c. Can patterns of reaction be identified (e.g. along stakeholder community lines, along nationality lines, etc.)?
10. Do China's government and Chinese non-state stakeholders influence ICANN's decisions? Can you please provide an example?
11. Do Chinese stakeholders influence IETF's decisions? Can you please provide an example?
12. Have you seen changes in relations among states and stakeholder groups in critical Internet resources governance bodies (main reference:

ITU, ICANN, IETF) through the last two decades? Can you please provide an example?

13. Have critical Internet resources governance rules and norms changed throughout the last two decades? Can you please provide an example?
14. (If the answer to questions 13 and/or 14 is ‘yes’), do you think China’s non-state stakeholders and government had an influence in shaping rules and/or relations?
15. Is there any further important information that you would like to add?