Mapping the Net State:
Towards a Framework for Cyber Statecraft

Honours thesis submitted in partial fulfilment
of the requirements for the award of the degree
BACHELOR OF COMMUNICATION AND MEDIA (HONOURS)
from
UNIVERSITY OF WOLLONGONG

CALLUM JAMES HARVEY

2021
“It is not the case that we have failed to care for Creation, but that we have failed to care for our technological creations. We confuse the monster for its creator and blame our sins against Nature upon our creations. But our sin is not that we created technologies but that we failed to love and care for them.”

- Bruno Latour (2012)

“International politics proceeds essentially on nothing more substantial than a set of expectations: expectations as to where power will prove to be and how it will be used.”

- Coral Bell (1981, p. 151)

“Senator, we run ads.”

- Mark Zuckerberg, to United States Senator Orrin Hatch of Utah (NBC News 2018)
Abstract

This thesis seeks to develop the concept of the net state as a newly identified type of state-like cyber actor. States have been increasingly challenged by actors emerging from cyberspace to disrupt established norms and rules of political life. Non-state actors such as social media corporations and online networked insurgencies are regularly compared to states as a way to illustrate size and magnitude. However, the nature of these actors has not been fully analysed. This thesis remedies this gap by providing a clear framework by which state-like cyber actors can be identified. The thesis deploys an analytical framework combining international relations theory, cybercultural theory, and actor-network theory to expand upon Alexis Wichowski’s (2017; 2020) definition of the net state. This framework is then applied to three case studies to demonstrate variation across the range of state-like cyber actors. These case studies propose three variants: the corporate net state, the non-corporate net state, and the client net state. These proposed variants are addressed at increasing the utility of the net state concept in policymaking and applying the net state concept to actors other than Silicon Valley technology companies. Ultimately this thesis demonstrates that net states are distinct state-like cyber actors, and it provides a framework for analysing and engaging with them in terms of the realities of cyberspace and how these actors engage with states and other actors in their network.
**Declaration**

I certify that this thesis is entirely my own work except where I have given full documented references to the work of others, and that the material contained in this thesis has not been submitted for formal assessment in any formal course and the word length is 18,981.

Callum James Harvey 12 May 2021
Table of Contents

Abstract ................................................................................................................................. 3
Declaration ............................................................................................................................. 4
Table of Contents ............................................................................................................... 5
List of Figures ...................................................................................................................... 7
Acronyms and Abbreviations ............................................................................................ 8
Acknowledgements .......................................................................................................... 9

Chapter 1: Introduction .................................................................................................... 10
1.1 Introduction ................................................................................................................... 10
1.2 Methodology ................................................................................................................ 13

Chapter 2: Literature Review ........................................................................................... 17
2.1 Introduction ................................................................................................................... 17
2.2 States and non-states ................................................................................................. 17
2.3 The net state ............................................................................................................... 20
2.4 Cyberspace and materiality ....................................................................................... 21
2.5 The international userbase ....................................................................................... 24
2.5.1 Digital denizens ..................................................................................................... 27
2.6 Priesthoods, belief, and agendas .............................................................................. 28
2.7 Conclusion .................................................................................................................. 31

Chapter 3: The Corporate Net State ................................................................................ 32
3.1 Introduction to Case Studies ..................................................................................... 32
3.2 Beyond Big Tech ......................................................................................................... 32
3.3 Dramatis Personae ...................................................................................................... 34
3.3.1 Problematisation ................................................................................................... 34
3.4 Reassembling the techno-social ............................................................................... 36
3.4.1 Interessement ....................................................................................................... 38
3.4.2 Enrolment ............................................................................................................ 39
List of Figures

Figure 1: Comparison of various layered models of the internet ........................................... 23
Figure 2: A diagram of the Facebook actor-network ............................................................... 37
Figure 3: A diagram of the 4chan actor-network ................................................................. 45
Figure 4: A diagram of the WeChat actor-network ............................................................. 55
Figure 5: Screenshot of WeChat keyword censorship notification ....................................... 59
Figure 6: The Facebook actor-network as deployed in Australia ....................................... 63
<table>
<thead>
<tr>
<th>Acronyms</th>
<th>Abbreviations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANT</td>
<td>Actor-network theory</td>
</tr>
<tr>
<td>CCP</td>
<td>Chinese Communist Party</td>
</tr>
<tr>
<td>CEO</td>
<td>Chief Executive Officer</td>
</tr>
<tr>
<td>ICANN</td>
<td>Internet Corporation for Assigned Names and Numbers</td>
</tr>
<tr>
<td>IGO</td>
<td>Intergovernmental organisation</td>
</tr>
<tr>
<td>IR</td>
<td>International Relations</td>
</tr>
<tr>
<td>MNC</td>
<td>Multinational corporation</td>
</tr>
<tr>
<td>NGO</td>
<td>Non-governmental organisation</td>
</tr>
<tr>
<td>NSFW</td>
<td>Not safe for work</td>
</tr>
<tr>
<td>OODA</td>
<td>Observe, orient, decide, act (feedback loop)</td>
</tr>
<tr>
<td>OPP</td>
<td>Obligatory passage point</td>
</tr>
<tr>
<td>PRC</td>
<td>People’s Republic of China</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>UNGGE</td>
<td>UN Group of Governmental Experts on Information Security</td>
</tr>
<tr>
<td>US, USA</td>
<td>United States of America</td>
</tr>
<tr>
<td>WSB</td>
<td>WallStreetBets</td>
</tr>
</tbody>
</table>
Acknowledgements

To put it mildly, this thesis was completed under difficult global circumstances. As such, I must thank above all my supervisor Dr Christopher Moore. Thank you for guiding and supporting me through the process of research during a global pandemic, and for pushing and challenging me to improve throughout the whole year. I must also thank Chris for reinvigorating my passion for miniature wargaming and modelling, which has kept me sane throughout the entire Honours process. I look forward to collaborating with you in the future, whatever form that may take.

Special thanks must also be given to Dr Ted Mitew, who in 2017 delivered a lecture on memetic warfare that inspired me to delve further into the study of cyberspace. For leading an unsure politics student down the rabbit-hole of digital media, I am extraordinarily grateful to Chris, Ted, and the entire Communication and Media academic staff at UOW for their support and interest in me over the years as an undergraduate.

For the encouragement, memes, and regular feedback, thanks to friends old and new from the UOW Digital Media Society and the Australian Crisis Simulation Summit. You know who you are.

Thank you to my parents, for pushing me to go to university in the first place and for their endless support once I was there. Thanks also to my sister Leah, for providing conversation and a dose of sanity while we were both studying under lockdown.

Thanks and love to my partner Erin, for your support, feedback, patience and encouragement throughout the writing process. I could not have done this without you.

Finally, given the circumstances it seems apt that my final thanks be to the net states and non-human actants that made writing this thesis during a global pandemic possible at all. Thank you to Google Docs and Discord for enabling research and feedback during the pandemic, and to the creators, platforms and memes along the way for providing healthy distractions in an unprecedented time.
Chapter 1: Introduction

1.1 Introduction

In February 2021, Facebook followed through on a prior threat to unilaterally restrict news media content from being shared by users in Australia. The restrictions were instituted as a response to the Australian government’s News Media and Digital Platforms Bargaining Code, and affected news media as well as health agencies, charities and Australia’s Bureau of Meteorology. Facebook’s actions were characterised by members of Parliament as “an assault on a sovereign nation” (Australia, House of Representatives 2021, p. 50), and by news media as Facebook declaring “war” on Australia (Cellan-Jones 2021; NT News 2021).

Events like this are becoming regular features of political life. States are with increasing frequency outfoxed, outwitted and outgunned by cyberspace and the actors emerging from it. While the internet has transformed global political life, answering the challenges of cyberspace, defined as an experiential techno-social space enabled by the internet (Lessig 2006, p. 9), has proven difficult for state actors.¹ States may only assert their authority in material terms of “flesh and steel” (Barlow 1996), not cyberspace and computation.

Previous analysis of the politics of cyberspace makes reference to an ill-defined type of non-state actor intruding upon the relationship between state and citizen (Schmitt 2020; Zuboff 2019). Challenges emerging from cyberspace are often reduced to the term ‘cyber’, a buzzword emptied of cyberspace’s history, culture and theoretical background that functions as a placeholder for implied complexity (Futter 2018). While the comparison of stakeholders in cyberspace to states is often made, it is generally directed at Western technology companies and used to illustrate size, rarely departing from metaphor (Fairbank 2019; Farrell, Levi & O’Reilly 2018; Hoskin & Mostrous 2020; Schaake 2021). However, metaphor has history in the digital age as a way to shape policy and governance structures (Heemsbergen & Molnar 2020). If they are perceived as similar to states, what might we call these cybernetic actors?

¹ See section 2.4 for a more in-depth discussion of cyberspace.
First identified in 2017, net states are a diverse group of internet-enabled, state-like actors which exist primarily online with international userbases and possess the capacity to advance their own agendas independently of state authorities (Wichowski 2017). They possess an agency over cyberspace far outstripping that of states, incorporating both its material and social dimensions. This model encapsulates most of cyberspace’s stakeholders yet provides a framework to distinguish them from multinational corporations (MNCs) or web pages. Importantly, it recognises that cyberspace is inherently social, and at the social level the sensate ecology of the net state differs little from that of the state. Linking emerging techno-social actors to existing objects with rules (Heemsbergen & Molnar 2020) such as states can assist in solving new challenges.

The advent of cyberspace has transformed the international from a chessboard of competition to a web of networks (Barrinha & Renard 2020). Cyberspace is not only post-liberal (Barrinha & Renard 2020), but post-national (Habermas 2001). This reflects a wider problem. Although cyberspace is in theory governed by a multistakeholder model, state strategies such as Australia’s International Cyber Engagement Strategy (Spry 2019, p. 61) are missed opportunities for engaging with actors emerging from cyberspace. Although Wichowski’s (2017; 2020) definition of the net state accounts for this, it lacks the ability to engage with the reality of state-like cyber actors that we see emerging in the everyday. The approach in this thesis is to expand international relations (IR) theory through the lens of cybercultural theory, with the underlying framework of actor-network theory, to close this gap.

While net states are manifestly challenges of cyberspace, states do not engage with them as such. Given that cyberspace is “very much at the core of the politics, society and economics” of this century (Barrinha & Renard 2020, p 752), a failure to grasp the nature and strategies of the actors who control it will accelerate the concentration of relational authority in net states. The problem is that states have privileged themselves when answering questions of who controls, and who ought to control, cyberspace. Cyber statecraft, defined as the “use of technology to achieve strategic ends” (Atlantic Council, n.d.), operates at the confluence of technology and geopolitics and is demonstrably practiced by states and net states.
Responses to net states vary. Regulating digital technologies through the lens of so-called ‘Big Tech’ decreases in effectiveness beyond Silicon Valley (Zuboff 2019). 4chan and its ilk are treated as counter-terrorism challenges (Evans 2019). Finally, state-owned social media are treated as channels to engage diaspora, not as digital extensions of a state’s borders (Ryan, Fritz & Impiombato 2020). Dividing net states this way prevents engagement with their shared nature as techno-social monsters crossing epistemology, social science, and the study of communication (Latour 1993, p. 5). Abandoning this divide is an essential first step.

The net state is not solely technological - it is comprised of human and non-human actants in a flat, interoperable assemblage. While non-human actants such as algorithms, applications and servers are important, the users that interact with them and the individuals that direct them are equally so. Zuboff (2019) describes the latter as a ‘priesthood’\(^2\) that directs and governs the net state, which might equally include executives of a social media company, important end users or content creators, or a site’s administrators.

This thesis seeks to expand upon the net state concept, and by extension the notion of the priesthood, by combining rigid international relations theory and the field of cybernetics, specifically cybercultural theory - a theoretical trajectory that emerged in the 1990s as a means of grappling with the social consequences of cyberspace and digital technologies. Though often overlooked, cybercultural theory provides key clues to the symbolic, material and techno-social possibilities and limitations of both states and net states in the networked era. A case study methodology driven by actor-network theory will be deployed in support of this. I seek to expand the conceptual toolkit for states to respond to net states and cyberspace, which is defined as a social space facilitated by a material base including servers, smartphones, apps and undersea cables (Blount 2019, p. 19). This research also critiques the manner in which states have responded to cyberspace, as their engagement with the material at the expense of the techno-social and symbolic dimensions of cyberspace is a major factor.

\(^2\) Digital priesthoods are a recurring feature of dystopian and science fiction. See Asimov’s *Foundation* (1960), Pelevin’s *Babylon* (2000), and the Adeptus Mechanicus of *Warhammer 40,000* (Games Workshop 2017).
in the emergence of net states as a challenge to the Westphalian international. This research thus provides an interdisciplinary solution to an interdisciplinary problem.

The challenge to the Westphalian state-centric international outlined by Owen (2016) shall be addressed by developing the net state for use in future policymaking. I shall examine how net states assert themselves as distinct state-like stakeholders in cyberspace, and how they might be classified to reflect their diversity. I shall propose three types of net states to expand upon Wichowski’s (2017) definition, although I do not believe these are the only types of net states in existence. A review of related literature conducted in Chapter Two will assist in refining the net state definition based on a triangulated lens of cybercultural, IR and actor-network theory to locate net states, discuss the nature of their inhabitants, and establish their governing logics. Chapters Three, Four and Five will then elaborate upon the proposed definition by identifying three variations (corporate, non-corporate, and client net states) and providing a case study of each to support the proposed definition. Chapter Six will then discuss common trends emerging from the case studies.

It is important to note that this research does not make the claim that net states are simply states transposed into cyberspace. No online forum or social media company could presume to gain total control of all functions of a state. Rather, net states are major cyber stakeholders that possess their own populations, governments, and capacity to build and codify relations across a polity equivalent to that of states in cyberspace, and thus serve as bodies politic in their own right.

1.2 Methodology
This research will deploy an interdisciplinary case study methodology drawing on elements of cybercultural theory, actor-network theory (ANT), and international relations (IR) to answer the following two research questions:

**RQ1:** How do net states assert themselves as distinct, state-like stakeholders in cyberspace?

**RQ2:** How might net states be better classified?
A literature review will critically analyse the definition of the net state, the global cyberspace net states operate within, and how this space is treated by state actors. When analysing complex assemblages of users, processes, algorithms, and cyber-spaces, “unusual juxtapositions” of research methods layered together become extremely useful (Levenberg 2018, p. 15). The “methodological commons” between the humanities and computation proposed by McCarty (in Neilson, Levenberg & Rheams 2018, p. 3) can help us answer new questions posed by computation. This commons will assist in unifying the study of cyberspace and IR, remedying the latter’s struggle to engage with the former.

Three case studies will then be deployed to propose three types of net state and further develop the definition. These case studies are informed by the anti-positivist extended case methodology, a means of structuring case studies drawn from IR (Lai & Roccu 2019). Case studies, while useful in avoiding large-N data research, often tend towards positivism. The extended case methodology prioritises the construction, rather than selection, of a case by involving theory directly in the research process, utilising cases to break apart and reconfigure theory. Instead of attempting to fit a general concept to a specific case, the specific informs the general, creating robust yet flexible theory that connects present and past in anticipation of the future (Burawoy 1998).

Each of the following case studies expands upon Wichowski’s (2017; 2020) definition of the net state and attempts to rationalise inherent tension between its symbolic, material, techno-social and regulatory dimensions. The cases are structured according to Callon’s sociology of translation (1986) - a four-step process of problematisation, interessement, enrolment and mobilisation of an actor-network. Just as the internet includes discrete layers of machines, processes, and social spaces, the study of cyberspace allows for multiple levels of abstraction within a larger interdisciplinary whole (Levenberg 2018, pp. 17-18). As such, my application of the extended case methodology adopts Levenberg’s (2018) ‘layering’ model through a process of historical and political examination of the state, concentrating on structure and context; collection of text corpora; construction of actor-networks between key actants in each case; and abstraction to reconstruct theory as per these interactions.
Social and political theory have provided ample models for describing power relations between individuals and bodies politic. However, examining a heterogenous space comprising humans and technologies operating together such as cyberspace requires an investigative framework that can account for the free association of human and non-human actants (Latour 1991). Indeed, dividing the material and the social has hitherto prevented states from adequately engaging with cyberspace (Latour 1991, p. 129; Nye 2016).

The methodology deployed here is thus built around actor-network theory (ANT), an investigative toolset perceiving associations between human and non-human actants as operating within a flat ontological plane (Law 1992) - just as they do in cyberspace. ANT is not without its critics - its methodological breadth makes it opaque to some, and it has been criticised for “transforming scientists into washing machine salesmen” obsessed with posturing and rhetoric (Latour 1991, p. 115). Yet by abandoning the unnecessary division of the material and the social, and the human and non-human, ANT allows us to map the relations within a communication system as a robust, durable assemblage (Latour 1991, p. 129). In a context of dynamic innovation with ambiguous boundaries between groups, traditional social models struggle to trace associations between actors (Latour 2005 p. 11) - ANT remedies this.

The ANT model deployed in each case study reflects Callon’s (1986, p. 196) four-stage sociology of translation. This process commences with the problematisation - where one actor presents itself as indispensable to surrounding actants in solving a problem. This is followed by the interessement - a series of processes designed to bind actors to the problematisation. Accompanying this is the enrolment, a series of stratagems and tricks designed to formalise the roles of other actants. Finally, the focal actant must coordinate, and speak on behalf of, the other actors - the mobilisation of the actor-network. Each case study is organised around this process, allowing for an effective description of both the net states in question, and how those net states assert their authority against others within the actor-network to become a necessary partner or obligatory passage point (OPP). This process produces a state-like codification of relations across a social body, which shall be explored in the next chapter.
For the sake of clarity, the concerned actants will not be deconstructed into their constituent assemblages. Facebook, for example, is composed of humans (users and shareholders), advertising, algorithms, apps and technical infrastructures. Deploying this model in concert with the extended case methodology (Lai & Roccu 2019) will both provide an opportunity to develop the net state further, while also demonstrating the existence of corporate, non-corporate and client net states as agents working to reshape cyberspace and its governance.
Chapter 2: Literature Review

2.1 Introduction
To understand the implications of the emergence of net states, this chapter will provide an overview of key themes in the literature relating to the net state in terms of its definition. These are the nature of states and non-state actors; net states and the role of networks; the nature and location of cyberspace; the nature of end users; and the governing logics and agendas of net states. While the net state was identified through an IR lens, elements of the definition require reconfiguration to address contemporary developments. This chapter will thus serve to develop the net state by synthesizing IR and cybercultural theory to expand upon Wichowski’s (2017; 2020) definition, which will be applied to variants built in the case studies.

2.2 States and non-states
Since the Peace of Westphalia in 1648, the state has been considered the dominant actor in international relations and is expected in IR to remain so into the foreseeable future (Lake 2008, p. 41; Osiander 2001, p. 251). However, there is no universally accepted definition of what a state is. The most widely used is that articulated by the sociologist Max Weber (2019). Weber identifies seven key characteristics for statehood, foremost among which is a claim to a monopoly on the legitimate use of physical force within a given territory (Weber 2019, pp. 137-138). Weber’s state is not applicable across all of human history, as it would be unfair to compare the ancient Greek polis with a twenty-first century post-industrial democracy. Dusza (1989, pp. 77-78) notes that Weber’s theory of state is bound by its specific context, having only emerged in the 19th century. Weber’s state, like all political organisations, is also subject to constant revision (Dusza 1989, p. 71; Habermas 2001, p. 60). States being challenged by networked political actors is a continuation of a long-running process of revision exercised upon a historical anomaly. That IR focuses predominantly on an actor with such conditions attached is problematic, thereby leading to a failure to address emerging actors other than states (Strange 1991, p. 245).

International relations tends towards positivism in studying power, which it views as an expendable commodity residing in states (Strange 1991, pp. 245-246). By contrast,

3 Henceforth referred to as the Westphalian international.
ANT understands power as a network of relations between actors that must be performed into existence (Latour 1991, p. 18). Callon (1986) maps this process of ‘translation’ through a case study of scientists positioning themselves as indispensable to the sea scallop farming industry in Brittany to speak for fishermen, scientific colleagues, and the scallops themselves. Passoth & Rowland (2010) apply ANT to the state itself, framing it as the result of an ongoing web of social relations. State theories such as Weber’s are thus viewed as “blueprints for actual political practices” (p. 820), and ‘stateness’ thus the exercise of leveraging a network to build a socio-political community (p. 823). Foucault (2009) and Deleuze (1988) frame the state as a codification of relations across a social body. Dusza (1989) thus argues that the Weberian state is just one of many historical actors that would have exhibited ‘stateness’.

This thesis tends towards a post-international model that departs from IR’s traditional state-centric positivism (Ferguson & Mansbach 2007, p. 531) rather than subsuming non-state networked actors into an ontological hierarchy that privileges the state. Treating non-state actors as equivalent to states is the premise of the “postnational constellation” paradigm proposed by Habermas (2001, p. xiv), which recognises that the political sphere includes issues, such as the internet, that are beyond the control of the state (Baur & Arenas 2014, p. 160). Blount (2019, p. 55) agrees, arguing that cyberspace governance is an assemblage of which the state is but one component.

Eggenschwiler & Kulesza (2020, pp. 245-246) note that the term “non-state actor” deployed in IR literature is a misnomer, grouping actors as diverse as multinational corporations and terrorist groups together by virtue of not being states. For example, IR has struggled to acknowledge MNCs as central actors, insisting that corporations and all other non-state actors are ultimately subservient to state power (Babic, Fichtner & Heemskerk 2017, pp. 20-21; Strange, 1991, pp. 245-246). Corporations have been indicated in IR literature as an alternative source of authority to states, as they are juxtaposed against state authority and function as active participants in the post-national constellation (Babic, Fichtner & Heemskerk 2017; Habermas 2001; Strange 1991). Spry (2019, p. 70) argues that engagement with social media MNCs may be desirable and productive for states in the context of human rights. Some MNCs are larger than states - smartphone manufacturer Samsung possessed greater yearly
revenues in 2017 than the gross domestic product (GDP) of Saudi Arabia, the world’s second-largest producer of crude oil (Babic, Fichtner & Heemskerk 2017, p. 27).

Despite this, MNC influence is characterised by IR scholars as being a problem for a possible dystopian future over the horizon,\(^4\) rather than an extant reality (Terzi & Marcuzzi 2019). The latter already exists in the US state of Nevada, which in 2021 announced a plan to allow technology companies to form their own municipal governments (Associated Press 2021). Wolf (2005, p. 5) argues that collaboration with non-state actors would provide an opportunity for states to reassert authority over the international. Drawing on non-positivist elements as well as IR provides an opportunity to engage more constructively with non-state actors and cyberspace.

The role of non-state actors such as technology MNCs is most pertinent when considering their role in developing norms for responsible behaviour in cyberspace. Norms are a set of intersubjective, unwritten rules apparent to all actors in an assemblage that guide the behaviours of and interactions between those actors (Broeders & van den Berg 2020, p. 5; Fairbank 2019, p. 382). While there is an absence of formal treaties governing cyberspace, cyber norms are far from settled and are often treated as optional extras (Adamson 2020, p. 19; Fairbank 2019 p. 382). As the online world is man-made, actors such as technology MNCs and volunteers are essential stakeholders in establishing norms for the domain (Benkler 2006, p. 23).

Software manufacturer Microsoft has been identified as one such norms entrepreneur in its efforts to establish a Digital Geneva Convention (Hurel & Lobato 2018, p. 61). Fairbank (2019) commences her analysis by questioning whether Microsoft operates as a state. By contrast, Adamson (2020 pp. 31-33) presents states as exclusive arbiters of cyber norms, while characterising the norms produced through state-centric mechanisms such as the United Nations Group of Governmental Experts (UNGGE) examining cyber governance as being easily ignored. Excluding non-state cyber stakeholders invariably results in states being challenged by the networks they attempt to govern.

\(^4\) Cyberpunk fiction regularly features governments ceding functions to private corporations. See Stephenson’s *Snow Crash* (1992).
2.3 The net state

According to Wichowski (2017) all net states share three characteristics: they primarily exist online, possess international userbases, and are capable of advancing belief-driven agendas independently of state authority. Through a nomos of speed, cyberspace and the private stakeholders that underpin it such as technology MNCs and online forums have accelerated the pace of change and spread of information globally. Virilio’s (2006) conception of dromology (speed as power) as a driver of progress and power throughout human history seems well-suited here. That the internet is dromological is unsurprising - echoing former Intel chief executive officer Andy Grove, Google’s Eric Schmidt argues against government regulation of the internet on the grounds of not wanting to slow down:

High tech runs three-times faster than normal businesses. And the government runs three-times slower than normal businesses. So we have a nine-times gap...you want to make sure that the government does not get in the way and slow things down (Schmidt, quoted in Zuboff, 2019, p. 104).

The online world, and thus net states, draw authority from being faster than states in adapting to the new digital age – that is, dromocratic. The lawlessness of cyberspace has always been a critical factor for its success. Technological stakeholders rely on this lawless void to innovate without government regulation catching up (Zuboff 2019, p. 104).

Control over cyberspace has shifted away from states, crystallising in net states as actors capable of altering social realities online (Barrinha & Renard 2020, pp. 751-753). Owen (2016, p. 302) suggests that global digital networks have shifted power away from hierarchical states and towards decentralised networks, empowering a new layer of actors that Wichowski (2017, 2020) later identifies as distinct. Blount (2019, p. 2) argues that as a physical construct the state can only assert a right to controlling the online world based on its physical realities, echoing Virilio’s (2006, p.97) conception of dromological actors as deterritorialized and thus out of reach of slower, contextually dependent actors such as states. As power is not a commodity but a network of relations, and society is itself networked through the internet, relational ‘power’ resides in the global networks themselves (Castells 2004, p. 224). However,
existing conceptions characterise social media platforms as little more than irresponsibly run vectors for disinformation against which control can be asserted by anti-monopoly legislation (Zuboff 2019, p. 14) or by hauling executives into inconsequential government hearings (Kreps 2020, pp. 69-70). In short:

States...are no longer isolated actors with enormous power. Their power is challenged and influenced by the different powerful nodes, sub-networks, and alternative networks...in a network society, power... does not reside in institutions, states or corporations - rather, it is located in the network itself (Owen 2016, p. 303).

Net states thus codify relations across a network, fitting with the vision outlined in John Perry Barlow's Declaration of the Independence of Cyberspace (1996) by challenging states, “weary giants of flesh and steel”. While Barlow frames cyberspace in Romantic terms, the Declaration established the basic frame subsequent cyber stakeholders and net states have exploited. IR must understand this logic in order to contend with cyberspace.

2.4 Cyberspace and materiality
If the contemporary state is bound by its context, then the net state is bound by global digital networks - that is, cyberspace. Examining where, and what, cyberspace might be is essential in identifying the net state and determining where it can be found. William Gibson, in his cyberpunk novel Neuromancer, defines cyberspace as “a consensual hallucination experienced by billions of legitimate operators”, a graphical representation of a global technological network (Gibson 1984, p. 51).

Luke (1999, pp. 30-31) argues that all spaces are produced by human and non-human actors, cyberspace included. The level of interoperability between the two online thus frames cyberspace as a flat ontological plane allowing free association between humans and technologies (Latour 1991, p. 103). This consensual hallucination possesses a “unique combination of physical and virtual properties” (Nye 2016, p. 6). Turner (2010) suggests that this hallucination is demotic, not democratic. The

---

5 When asked by Senator Orrin Hatch how Facebook sustains its free service during a 2018 hearing before two United States Senate committees, Facebook CEO Mark Zuckerberg responded, “Senator, we run ads” (NBC News 2018).
interessement device of a Terms of Service on Facebook, for example, culminates in a single button for accepting the site’s terms and conditions. As for the hallucination, cyberspace is an imaginary product of relations between people and things. Much like the state, cyberspace is by definition an actor-network (Passoth & Rowland 2010). The Romantic elements of Gibson and other cyberpunks often obscures the rigorous intellectual contribution the literary movement has made to cybercultural theory.

The ubiquity of cyberspace makes it both polysemic and popular, contested both in meaning and within the space itself (Strate 1999, p. 383). In IR and related disciplines, cyberspace is used interchangeably with the internet, the Web (Nye 2016) or with “technology” in general (Fukuyama, Richman & Goel 2021). This is problematic when we consider that these disciplines are concerned with emergent threats to their authority. Thus, governing this new space is conflated with governing a technical architecture, perhaps emblematic of some anxiety regarding the collapse of material and social online. Such confusion is not recent - Strate (1999, pp. 382-383) details that cyberspace’s protean nature has extended from the space itself to its definition since Gibson coined the term.

Cyberspace is powered by digital networks, primarily the internet. Collins (2009, pp. 60-61) describes the internet as an edifice including technical architectures, physical infrastructure, users, applications and content in a series of interdependent layered regimes. However, Collins’ discussion focuses exclusively on the technical strata, not the network of socio-political associations spawned from it. In a 2016 Chatham House report, Nye (2016, p. 6) and DeNardis (2016, p. 2) both deploy “cyber governance” and “internet governance” interchangeably as bywords for managing technical rather than social strata. Both authors frame this practice as a multi-stakeholder affair between states, NGOs, IGOs and businesses, notably excluding users.

State reliance on NGOs such as the Internet Corporation for Assigned Names and Numbers (ICANN) to govern technical strata stems from a general neglect of the online domain, leaving states under-equipped to deal with actors emerging from that space (Collins 2009, p. 52). Moreover, the label of ‘internet governance’ is itself problematic. Van Eeten & Mueller (2012) detail that the term is applied to a handful of formal, centralised organisations such as ICANN, but not to the techno-social enabled by the
internet or the actors that coordinate to operate it such as Microsoft or Facebook. Equipping states with new tools to accurately engage with cyberspace will allow them to rise to the challenge of the net state - a familiar, yet disturbing Other.

Here a distinction must be made between the internet and cyberspace. The former is a communications technology, while the latter combines an immense technological edifice with a social layer as a single geography (Blount 2019, p. 19; Lessig 2006, p. 83). The immense material size of the internet attaches to it myriad questions of ownership and governance (Luke 1999, p. 31), but it forms only part of cyberspace. The internet is a material assemblage acting upon cyberspace - a techno-social space. Virilio (2006, p. 114) would classify the internet as a prosthesis for survival, much like the automobile needed to traverse urban sprawl. Figure 1 compares various layered models of the internet.

![Layered models of the internet](chart.png)

*Figure 1: Layered models of the internet. The social layer that distinguishes the internet from cyberspace occurs underneath each model. Note that cyberspace is not confined to the social layer but is the product of all layers working in concert to produce a sensate, lived space for its inhabitants.*

---

6 Diagram adapted from Blount (2019, p. 20) and Collins (2009, p. 62)
7 Post, Kulesza, Werbach, and Solum & Chung quoted in Blount (2019, p. 20)
A common feature of all the above models is their focus on physical hardware and/or internet protocol systems as the *prima facie* concern for internet governance. While often framed as a liquefaction of the physical (Zuboff 2019 p. 219), Figure 1 illustrates that the material and social interact with each other within a single assemblage. Cyberpunk fiction illustrates that ignoring the material in favour of the social leads to the decay of the former and collapse of the latter (Stephenson 1992).

The conflation of the internet and cyberspace presents serious issues for Wichowski’s net state definition. While net states have been established as existing “online” (Wichowski 2017), a lack of clarity as to what “online” means or where it might be in turn leads to confusion as to what might be considered a net state. This is clear in Wichowski’s case study of electric vehicle and battery storage manufacturer Tesla challenging the United States government in developing electricity infrastructure in Puerto Rico (Wichowski 2020, pp. 49-51). Tesla chief executive officer Elon Musk has significant memetic heft on social media, with his Twitter account being the focus of securities fraud proceedings against Tesla in the United States (US Securities and Exchange Commission 2018). However, Tesla is not solely defined by the tweets of its CEO. Labelling it as a net state is thus an ill-fitting example considering that the company manufactures cars and batteries linked to the Internet as physical products. Addressing the material in relation to cyberspace is essential.

As indicated by Nye (2016, pp. 8-9), the currently multi-stakeholder regime complex that manages cyberspace devolves the control of many of these layers to ICANN and other NGOs, as well as private internet service providers. However, this complex ignores the content and application layers, and does not consider the social. While net states are mainly the product of the social layer, they shall be identified here as part of a wider assemblage including both social and material elements.

2.5 The international userbase

While net states are nestled within cyberspace, exactly where this space is located in relation to states remains unclear. Wichowski (2017) labels net states as having “international” reach in her second criterion. Conceptions of online territory for IR place cyberspace within state boundaries, as the servers and devices that drive cyberspace are notionally subject to state authority. In practice this is often not the case. Blount
(2019, p. 2) details that UK and US authorities were unable to stop journalists from destroying devices containing leaked data from Edward Snowden with an angle grinder in the basement of The Guardian’s London offices in 2013. Similarly, Californian authorities failed to stop the operators of 8chan (then based in California) from loading its servers into a truck and absconding to restart the site following the Christchurch and El Paso shootings in 2019 (Evans 2019).

Irrespective of materiality, cyberspace is somewhat deterritorialized. Blount (2019, p. 17) details cyberspace as being both everywhere and nowhere all at once - a location that can only be described, not defined. Roguski (2020, p. 65) argues that the aterritoriality of cyberspace has led to a misconception by political theorists that the online world was contiguous with the international, and therefore subject to international law. However, Roguski admits that sovereignty (that is, a state’s ability to control its own affairs without outside influence) must evolve to account for transnational technologies and online spaces.

Weber’s (2019) model of state is built on the control of physical territory. Holding that territory is a critical link between jurisdiction and governance (Blount 2019, p. 42). States are built as ‘national’ spaces, which are the constituent elements of the international, and unlike the technical layers of the internet are not materially interoperable. An individual crossing the southern border of the United States has by default entered Mexico. While one cannot live in two states at once, states can, and do, mix at the social level.

Users may deploy a virtual private network (VPN) to ‘tunnel’ out of a certain state’s segment of cyberspace (Symanovich 2020). Heemsbergen & Molnar (2020) describe VPNs as boundary objects of the internet with both symbolic and technical value. By providing a metaphoric frame for use such as Blount’s (2019) virtual borders, VPNs establish experiential and functional rules about the digital terrain they assist users in navigating externally from the authority of a state (Heemsbergen & Molnar 2020). State authorities are relegated to playing catch-up (Schneider 2016, p. 2678).

—

8 See Nye (2016).
The material can interrupt the social in other ways. China’s control over Chinese-language platforms such as WeChat disrupts the lives of pro-democracy activists living overseas by programmatically removing avenues for dissent (Ryan, Fritz & Impiombato 2020). By exclusively focusing on the material, only half the problem can be solved. Geography is argued both to play “no meaningful role in the functioning of the Internet” even if its material base is territorial (Creemers 2020 p. 116), and to have “strong connections with geography” (Medcalf 2020, p. 182). Though the material is spatially organised, the social is not, and is both everywhere and nowhere.

Any geographical heuristic in relation to cyberspace is more political and legal than physical (Blount 2019, p. 4). In the case of Facebook, its “borders” might include both the facebook.com domain and the social platform based within, as well as other techno-socials such as Instagram and WhatsApp, and cookies to extract data from end users when they visit other websites (Nieborg & Helmond 2019, pp. 197-199; Facebook, n.d.). Cyberspace would thus appear to be both external to national space and the international, while simultaneously being marked by places where national spaces jut into it.⁹

If states wish to exert control over cyberspace, they must position themselves as indispensable to, and build alliances with, net states. Eric Schmidt & Jared Cohen (2013, p. 111) propose the creation of online spheres of influence by major technology supplying states such as the United States. Schmidt & Cohen, both Google executives with a background in IR, theorise that such spheres of influence would be built on state-specific technologies to form the spine of digital “client states” - not client net states.

The existence of client net states is most pertinent when considering the role of networked technologies in the People’s Republic of China. As the world’s largest digital economy, the PRC has utilised cyberspace to develop a “digital civilisation” by harnessing data outputs of over a billion people to improve services and control information flows by combining nationalism, content creation, and an acceptance of

---

⁹ There are no zones of exclusive state control in cyberspace, a key difference between cyber governance and the Law of the Sea established by the United Nations (Geoscience Australia, n.d.).
government surveillance (Keane & Su 2019, p. 4). Rather than accept Western multi-stakeholder models of internet governance, Keane & Su (2019, p. 9) suggest that the PRC’s tightly controlled domestic cyberspace is an extension of its centralised, undemocratic government. Creemers (2020) agrees, detailing that the PRC’s consolidation of control over its inhabitants in cyberspace is critical to ensuring its stability, supported by a vague “cyber sovereignty” doctrine designed to bar foreign-owned media from the PRC. The PRC tightly controls its citizenry’s behaviour through the Social Credit System (SCS), which Wichowski (2020, p. 135) notes is designed to ensure state control over in-person and online behaviours.

While China’s segment of cyberspace maintains some interoperability with global cyberspace (Creemers 2020, p. 118), Yu & Sun (2019, pp. 18-19) argue that WeChat, a PRC-affiliated net state, is essential for connecting the global Chinese diaspora with the “homeland”. WeChat, even internationally, is subject to censorship from the PRC government. Ryan, Fritz and Impiombato (2020, p. 25) detail that, while Chinese citizens are theoretically the only users to be censored by WeChat, in practice both domestic and international users are subject to the same controls, regardless of whether the user is a PRC citizen. The SCS and the means to effect it knit the state together with the cybercultural experience of living within that state - one can be physically beyond the Great Firewall, but socially stuck behind it.

2.5.1 Digital denizens
As a space distinct from the international, cyberspace and net states must have inhabitants. The synthesis of cybercultural and IR theory here can assist in defining who or what these inhabitants are. Schmidt & Cohen (2013, p. 32) describe cyberspace’s inhabitants as a “virtual population” of hyper-pluralistic dual citizens of both the material and online, comprising multiple online representations of an individual across various interlocuting online spaces. Loader & Mercea (2011) label these inhabitants “citizen-users” - direct participants in driving democratic innovation online through sharing content. However, a decade of algorithmic instrumentation by net states has shown that the ‘citizen-user’ is no longer fit for purpose. Cyberspace is not a democratic place (Barlow 1996), and its inhabitants can be seen as having experienced what Turner (2010, p. 2) labels a “demotic turn” focusing on participation rather than democracy.
Wichowski’s (2020) adoption of the citizen-user concept thus overstates their influence within net states. For example, WeChat users lack any democratic rights to free expression (Ryan, Fritz & Impiombato 2020), and Google’s corporate structure prevents it from implementing internal democracy through a tiered shareholding structure (Zuboff 2019, p. 101). Moreover, the citizen-user assumes a 1:1 relationship between power and influence, a logic at odds with modern machine learning and behavioural data capture systems driven by ingesting data from constant use. A system mediated by concentrated algorithmic data capture is not easily overthrown or changed by a “declaration of citizen-user rights” (Wichowski 2020, p. 208).

What, then, are users? The concept of citizenship is grounded in the state, as an endowment of all members of a political community with civil, social and political rights (Mossberger, Tolbert & McNeal 2008, p. 1; Shearing & Wood 2003, p. 400). Digital citizenship, however, is defined as the ability to participate in online society (Mossberger, Tolbert & McNeal 2008, pp. 1-2). Most net states impose changes to their social contracts (that is, their Terms of Service or End User License Agreements) unilaterally, at short or no notice, and without user consent - hardly an endowment of inalienable rights other than the right to use. As such, we cannot graft the ideal of citizenship to a world of multiple intersecting memberships of non-democratic entities. Users being afforded the right to inhabit, but not to control the future of net states would thus characterise them as denizens (Shearing & Wood 2003, p. 407). The inhabitants of net states are thus not citizen-users, but denizen-users. This presents another question - who is in charge, if not a democratic base of users?

2.6 Priesthoods, belief, and agendas
Having established that denizen-users are enrolled in a demotic relationship with the net states they inhabit, we must investigate the parties dictating that relationship and the relationships of net states with states and other actors. While the third of Wichowski’s (2020, p. 244) net state criteria invokes a “belief-driven agenda” as a vector for challenging states, exactly whose belief serves to solidify relationships between actors remains unclear. Belief, myth and symbolism are all critical in understanding cyberspace. Barlow’s independent cyberspace (1996) and Schmidt & Cohen’s “new digital age” (2013) are mutually constituted with a political economic dimension, even as they offer an entrance to a different reality (Mosco 2004, p. 7). Yet
in Wichowski’s definition, belief of the end user is never addressed, instead being a byword for the profit imperative of social media corporations (Wichowski 2020).

Many net states are underpinned by for-profit MNCs. This requires an examination of surveillance capitalism, an economic ideology that “unilaterally claims human experience as free raw material” for ingestion into computational algorithms to optimise online services (Zuboff 2019, p. 8). Developed by Google and perfected by Facebook, surveillance capitalism remains entrenched through a system of instrumentarian power, an inversion of totalitarianism that favours the automation of denizen-users over coercion to induce dependence. While totalitarianism is a fundamentally violent power structure deployed to great effect by fascist and communist dictatorships in the twentieth century, instrumentarianism modifies behaviour by relying on humans bound like puppets to sensate computation (Zuboff 2019, p. 354-358). Such a system reflects the marketised societies of control detailed by Deleuze (1992, pp. 6-7) in their debasing of social life. As demonstrated by cybernetic investment collective WallStreetBets during the 2021 GameStop short squeeze, denizen-users can impact the material and social independently of a single platform (Rajjaque 2021). Graham (2018) details that these platforms function as engines that configure users and govern the act of choosing.

Understanding the nature of who controls a net state depends on the net state in question. Zuboff (2019) argues that instrumentarian systems are not governed but planned by a godlike priesthood ‘tuning’ the network at the expense of denizen-user agency (pp. 431-442). This replaces a constitution with an imposed Terms of Service that can change at any time, ensuring control over the production of raw material, be it data or memes. For corporate net states such as Facebook, the imposition of hierarchical control structures creates a ruling class that speaks for the whole platform. In the case of the aforementioned “client” net states such as WeChat, the priesthood would not be shareholders, but government officials such as the Cyberspace Administration of China (Ryan, et al, 2020, p. 27). Priesthoods are oriented to human experience so as to extract data for behaviour modification, prediction and monetization (Zuboff 2019, p. 352). As priesthoods are responsible for directing net state assemblages, we must consider their role.
As myth is critical to understanding cyberspace (Mosco 2004), it is unsurprising that digital priesthoods are reflected in cyberpunk and dystopian fiction. Zuboff draws her metaphor from Skinner’s *Walden Two* (1948), and analogues are visible in Gibson’s *Neuromancer* (1984) and in the World Controllers of Huxley’s *Brave New World* (1932). The priesthood’s role in shaping consensual hallucinations is explored in the final chapters of Pelevin’s *Bablyon* (2000), wherein the protagonist is transformed from a copywriter to the husband of the Babylonian goddess Ishtar and a regular yet unremarkable feature of television commercials.

Surveillance capitalism and instrumentarianism are not without problems. Zuboff (2019) characterises the two as inextricable from each other and does not consider that one could exist without the other, ignoring net states that lack a profit imperative. For example, the net state 4chan has no profit imperative and is thus not surveillance capitalist but does operate on an instrumentarian model. Denizen-users are automated to function as a swarm or hive mind in pursuit of strategic narrative goals through a politics of transgression (Nagle 2017, pp. 33-34; Mitew & Wall 2017, pp. 3-4). 4chan’s priesthood would thus be contiguous with its entire population, not unlike pre-corporate online forums of the 1990s (Kleiner 2010, p. 14). This leaderless, counter-revolutionary techno-social prioritises anonymity and ironic humour above all else (Nagle 2017; 4chan n.d.), adhering to a distributed network topology (Baran 1962) rather than the economically concentrated, user-distributed model of a social media corporation.

Mitew & Wall (2017, pp. 7-10) characterise 4chan as a hive mind in its development of the #DraftOurDaughters memetic warfare campaign during the 2016 US Presidential Election, which distributed narrative control across a scalable swarm of users. #DraftOurDaughters demonstrated that 4chan shares with corporate social media a focus on performance mechanics in online spaces, with memetic recapitulation as the governing logic instead of data capture. However, its distributed, scaleable and antifragile nature is reflective of Robb’s (2005) open-source insurgency.

While it lacks clarity, the ‘belief-driven agenda’ criterion will be left open-ended here. As net states are diverse, the nature of the agenda and priesthood can wildly differ.
This criterion shall thus be framed as a broad programme of negotiations (Callon 1986, p. 212) that guides net states in building relationships with other actors.

2.7 Conclusion
Synthesizing cybercultural and IR theory into a single theoretical framework is critical to understanding the wider implications of the net state. This chapter has built upon the concept by drawing on the strengths of each discipline to compensate for theoretical weaknesses in the other. By critically examining literature from both disciplines to detail how the net state criteria might be further developed, I have asserted that IR theory must broaden its perspective on cyberspace in order to understand how it functions as both a technical and social space. Incorporating cybercultural theory and the material-social ontology of ANT serves as a means to achieve this.

As such, the three constituent elements of Wichowski’s net state (2017) have been reconfigured as follows to benchmark the extended case methodological process in the next three chapters (Lai & Roccu 2019). Net states exist in a techno-social and global cyberspace, possess a demotic character expressed through their global denizen-user populations, and are driven by agendas dictated by a priesthood which differs based on the type of net state. Three variants of the net state shall now be explored.
Chapter 3: The Corporate Net State

3.1 Introduction to Case Studies

The following chapters identify three contextual variations of the net state. These case studies are informed by the extended case study methodology (Lai & Roccu 2019, which prioritises the construction of a case to break apart and rebuild theory. The net state variants proposed here - the corporate, non-corporate, and client net state - each possess contextual quirks but are still definitively net states. A secondary aim here is to decouple the net state from ‘Big Tech’, an exonym usually applied to American technology MNCs, and from the highly variable concept of the ‘platform’ (DeNardis & Hackl 2015; Van Dijck 2012). Both terms are often deployed to justify actors with agency as vectors for business as usual. While important, these have left other essential areas, such as non-market and state-owned net states, under-examined. Nevertheless, it is with Big Tech where the net state originates, and thus where our analysis shall begin.

3.2 Beyond Big Tech

The first type of net state I propose is also that which has received the most analysis in existing literature. Corporate net states exhibit all the characteristics of net states but are underpinned and driven by a corporate entity with a dominant economic imperative used to impose and stabilise relationships with other actors. This type of net state closely resembles that initially articulated by Wichowski (2020) and occupies a similar semiotic space to the aforementioned Big Tech label. This case study will examine Facebook, an archetypal corporate net state.

A corporation is defined as a legal entity distinct from its owners, who are protected from its collapse through limited liability (Kenton 2020). The term comes from the Latin corpus (“body of people”). Corporations are classified as ‘legal persons’ in that they can borrow money, hire staff, and pay tax. In the United States, corporations are granted more legal rights only afforded to natural persons, including the right to free speech (NPR 2011). This was affirmed by the US Supreme Court in Citizens United v. Federal Election Commission 2010, which established that corporations may donate without restriction to political campaigns (Lau 2019).
Increasing economic growth after the Second World War allowed corporations to become transnational actors. As a result, taxation, regulation, and enforcement of labour standards have become difficult (Babic, Fichtner & Heemskerk 2017, p. 21). The size of corporate actors, often expressed through exonyms such as Big Tech or Big Pharma, indicates some anxiety regarding the shifting of relational power away from states and towards corporations.

How is the corporate net state distinct from the MNC? Though the comparison of businesses to states has historically proven useful to illustrate scale, we are looking for a specific capability to negotiate and structure relations. Size, like power, is merely the outcome of a network of relations (Passoth & Rowland 2010, p. 829). Thus, it is useful to examine Foucault’s (2009) conception of the state. The ‘stateness’ of a given actor is defined by Foucault as a practice that codifies relationships across a given social - the state being but one product of said practice (Deleuze 1988, p. 75; Foucault 2009; Passoth & Rowland 2010, p. 823). The state is not powerful because it is large, but because it serves as OPP for relations between other actors. Deleuze notes that “[t]here is no State, only state control” and the relations that keep the social organised (1988, pp. 75-76). Thus, the size of the corporate net state, though useful to us, is not a variable that needs accounting for. Rather, its stateness builds on existing anxieties regarding corporations and their ability to evade states in regulatory terms, but reframes them based on how they build alternative political communities. As noted previously, MNCs are challenging for IR theory. Reframing MNCs through the lens of the net state can provide it with renewed vigour to engage with other state-like actors beyond a fear of big things.

Corporate net states are understood by Zuboff (2019, p. 9) to be driven by the economic ideology of surveillance capitalism, and the control imperative of instrumentarianism. Denizen-users are induced to rely upon a techno-social which extracts data about their social experience online for sale (Zuboff 2019, p. 352). Unlike Zuboff, I do not take the term “surveillance” as pejorative. Rather, it refers to a process that structures a system to respond to feedback. As they are predicated on feedback collected by sensors, all systems - cybernetic or otherwise - require surveillance to function.
For example, successive welfare regimes in Australia have relied on surveillance, including the former limited obligations system and the more punitive system operating today. Both require welfare recipients to report worked hours and job applications to Centrelink, yet the current system continually demands more data from recipients through a range of channels including a smartphone app and cashless welfare card (Dee 2013, pp. 272-274). Although surveillance practices implemented through material assemblages are often used negatively, labelling the process as the problem is incorrect and deterministic. Centrelink’s smartphone app is driven by an underlying neoliberal logic within elements of government to punish welfare recipients for being unemployed (Dee 2013). Indeed, there is no automatic disciplinary effect of surveillance (Elmer 2003, p. 232), nor is there an automatic net gain - effect is contingent on underlying logics.10

3.3 Dramatis Personae
The previous chapter mentions that borders in cyberspace cannot be defined, only described. Facebook’s borders shall thus be described to include the Facebook social network as well as Facebook Messenger, Instagram, WhatsApp, Oculus VR and Workplace, as well as the Facebook Inc. MNC itself (Facebook, n.d.). This ecosystem is populated by 2.70 billion monthly active users worldwide (Facebook 2020), almost double the population of the People’s Republic of China (World Bank 2019). With projected revenues of between US$52-55 billion in 2020 (Facebook 2020), this net state possesses greater income than the gross domestic product of Serbia (International Monetary Fund 2020). Yet size is not wholly proscriptive. Corporate net states assert themselves within a regulatory vacuum to crystalize a relationship with states as an obligatory passage point (OPP) for political activity.

3.3.1 Problematisation
To start the process of actor-network stabilisation, Facebook presents itself as indispensable to socialising, and a logical endpoint for human communities in the digital age. This is the first of Callon’s (1986) four stage model for actor-networks - the problematisation. Facebook is no techno-social panopticon in the Foucauldian sense.

---

10 Between 2016 and 2020, Centrelink’s ‘Robodebt’ automation system for correcting overpayments issued thousands of incorrect welfare debt notices. A subsequent class action resulted in a $1.2 billion settlement paid by the Commonwealth to victims in 2020 (Braithwaite 2020; Gordon Legal 2020).
(Logan 2017). Instead, Facebook aims through surveillance to control denizen-users at a distance, producing a mediated techno-social that permits freedom within specific parameters similar to Deleuze’s (1992) society of control (Elmer 2003, pp. 240-241).

The Facebook net state is thus an oligopticon - a myopic surveillance apparatus that offers a bright, incomplete view of reality (Latour 2005, p. 181). Facebook has worked to acquire a more complete picture through growth and stabilisation of relations with denizen-users, hence its acquisition of platforms as additional sources of behavioural surplus. The critical juncture of the corporate net state is that the material MNC and the techno-social are collapsed into a single actant, guided by Facebook’s executives serving as a priesthood that instruments its inhabitants (Zuboff 2019, p. 434). This priesthood dictates the engagement of Facebook with all other actors in its orbit, including 2.70 billion denizen-users who operate both as a component of the Facebook assemblage and an external actor. 11 Whether or not a Facebook account represents a real person is irrelevant, as a human exercises a degree of agency over that account subject to parameters afforded through interessement devices such as a Terms of Service.

States are a critical actor in this assemblage, as they are the main actor diametrically opposed to Facebook as it instruments inhabitants of state actors. Ironically, Facebook is indispensable for states for outreach and public diplomacy. Spry (2018, p. 67) notes that Facebook is the “most commonly used” vector for communication and diplomatic purposes. To construe itself as an OPP for regulatory purposes, Facebook undermines the relationship between state and individual, serving to provide an alternative social where end users are free to congregate. As such, the “agenda” Facebook advances is not one of belief, but one of behavioural surplus extraction fuelling a political structure - that is, surveillance capitalism to further an instrumentarian system (Wichowski, 2020, p. 244; Zuboff 2019, p. 409). As a result, the denizen-user is subjected to confluent action - they are free to participate within strict parameters while surrendering to a vast apparatus of control (Deleuze 1992)

11 Denizen-users are one interlocuting facet of a human residing in a physical location (Schmidt & Cohen 2013).
While the demotic (Turner 2010, p. 2) nature of the net state attracts denizen-users, it does not offer a means to stabilise the relationship between the two. Corporate net states formalise this relationship between the priesthood and denizen-user through their structure as a legal entity, which in Facebook’s case takes the form of a tiered shareholding structure. This is where the aforementioned collapse of MNC and platform into one actant is critical. Class A shares in Facebook Inc., available to the general public, are worth a single vote per share, whereas Class B shares are worth 10 votes each. CEO Mark Zuckerberg owns 89.1% of all Class B shares, and the wider priesthood controls 57.9% of voting power in the corporate structure as a result. No other significant shareholder controls more than 6.8% of total Class B shares (US Securities and Exchange Commission 2020). As a result, the pursuit of significant reform to the Facebook net state by its denizen-users is impossible.

3.4 Reassembling the techno-social
Once problematised, Facebook’s relationship with both states and denizen-users must be performed into existence. This formalises the roles of other actors to bind them to the problematisation - what Callon (1986) refers to as interessement. This is accompanied by the enrolment, where Facebook negotiates, tricks, and proclaims its way into a dominant position as OPP. The resulting actor-network is depicted in Figure 2 below.
Socialising online is an inescapable part of contemporary life - as such, Facebook’s role as a distinct political actor was assured long before the 2016 US elections. Its role as OPP for engagement with cyberspace by states and denizen-users was apparent in the previous US Presidential Election in 2012, with a virtual “I voted” button deployed on Facebook for its US users leading to observable growth in voter turnout (Bond et al. 2012, pp. 297-298). Facebook subsequently worked to build further agency prior to 2016 by encouraging advertising spends by both the Trump and Clinton campaigns in support of similar voter mobilisation initiatives (Kreiss & McGregor 2018, pp. 157-158). Even before allegations of Facebook being unwilling to intervene in disinformation came to light, the relationship between state and net state was firmly established.

As for the relationship with its users, the functionality of Facebook places users in a disadvantaged position, allowing their data to be extracted while “[giving] people a voice” (Zuckerberg 2018). Predetermined sets of categories create an illusion of choice for denizen-users, allowing them to pick what they like within a techno-social of control designed and modified at will by its priesthood. If human sociality turns out to be different from the machine-inscribed sociality, users may adapt their technical
environment to support the social (van Dijck 2012, p. 146). This is the ‘surveillance’ in surveillance capitalism and explains how Facebook makes itself indispensable to users. In imposing a particular mode of social relations upon its inhabitants, Facebook is not simply a vector for socialising as usual but is transformed into an object of agency (Zuboff 2019, p. 81). However, much literature focuses on end users acting upon the net state, not the net state itself possessing agency. This is an odd distinction to make and is often followed by defining Facebook as all-powerful and capable of swinging election results (Madrigal 2017; Zittrain 2014). How can Facebook be all-powerful if it is defined by the actions of users operating in a demotic space that grants them unfree freedom? The answer is through declarations.

3.4.1 Interessement

Declarations are essential for net states at a representational level and are a core element of cyberspace’s self-image (Barlow 1996). They serve as means to establish facts out of thin air, invading an existing real to impose facts upon all others in an assemblage (Zuboff 2019, p. 176) - a theoretical map obscuring the very territory it claims to portray (Baudrillard 1994, p. 1). Facebook’s manifestos do exactly this - they performatively insert the net state as an essential political partner in the regulation and governance of cyberspace. Mark Zuckerberg’s 2017 manifesto *Building Global Community*, for example, lays direct claim to the private information of users and the right to disclose this - a right normally concentrated in the state (Zuckerberg 2017; Rider & Wood 2019). These declarations carefully utilise language to formalise the roles of actors in Facebook’s orbit. This serves to hide its posturing - indeed, language is as critical in masking true intentions as effective policy or the claiming of new digital territory (Zuboff 2019, p. 90). In particular, they reduce the authority of Facebook to one word - ‘platform’.

Political communication literature frames platforms as digital vectors for an objective reality (Kreiss & McGregor 2018, p. 157). Facebook deploys the term regularly to position itself as a neutral facilitator without agency (Plantin et al. 2018, p. 297). Yet the term has been labelled “capacious and mercurial” (DeNardis & Hackl 2015, p. 762), defined variously as a pipeline for user-generated content, a dialogic online space, or the hardware enabling the online world to proceed (Van Dijck 2012, p. 144). In the United States, regulatory policy under Section 230 of the *Communications*
Decency Act 1996 offers no assessment of neutrality or legal significance for the term, thereby assisting Facebook’s use of the term as a framing device (Greene 2020). In actuality, platforms serve as active mediators between users, technologies, and content (van Dijck 2012, p. 142). While they may be materially neutral, net states like Facebook reflect political power structures (DeNardis & Hackl 2015, p. 762).

Facebook’s use of the term, and the accompanying assumption of neutrality, relies on the positivistic perception of states being the dominant actor in IR referenced earlier to obfuscate agency (Ferguson & Mansbach 2007). Indeed, reducing dialogue on the regulation of disinformation to questions of foreign interference (Kollars 2020) serves to assist this fiction of Facebook as an actor without agency. Finally, Facebook (the corporation) has purchased additional platforms such as Instagram and WhatsApp which are interoperable with Facebook (the platform) (Facebook 2020). The net state is thus comprised of at least one platform, collapsing the MNC and platforms into a single assemblage.

### 3.4.2 Enrolment

A critical element of this obfuscation is Facebook’s use of declarations to claim that it welcomes state regulation, while acting to oppose it. Facebook thus performs itself into power by portraying state authorities as not understanding the technologies they wish to regulate. This performance activity forms the enrolment (Callon 1986) and requires Facebook to engage with the material beyond its vast server banks and offices in Silicon Valley, challenging the state on its own terms.

Since 2018, enrolment has been enacted through the acquiescence of Mark Zuckerberg and other members of the priesthood to appear before government hearings in the United States Congress, and their refusal to appear at hearings elsewhere. Zuckerberg’s attendance at hearings in 2018 were designed to frame the members of the US government as knowing nothing about Facebook. When asked how Facebook sustains a free service by Senator Orrin Hatch of Utah, Zuckerberg responded by explaining that the platform runs ads - a basic tenet of surveillance capitalism, yet one which the senator responsible for investigating Facebook was unaware of (Stewart 2018). While the 44 Senators conducting the 2018 inquiry, along with other Senators and members of Congress that have interrogated Zuckerberg
since, agree that Facebook needed to be regulated, a lack of technical understanding of the platform prevents them from doing so (Stewart 2018). This is further demonstrated by their preoccupation with regulating or ‘breaking up’ Facebook. Zuboff (2019) notes that surveillance capitalism’s unprecedented nature makes it impossible to regulate through existing corporate regulation mechanisms.

Facebook also obstructs state investigations by selectively attending government hearings. In 2018, Zuckerberg refused to appear before a joint UK-Canada hearing in the British House of Commons, which focused on Facebook enabling disinformation rather than its broader role in mediating social experience (Vincent 2018). When a report by the Committee was finally handed down in 2019, it recommended statutory regulation based on competition law and an end to self-regulation - a process that would, presumably, require Facebook to hand power over to governments who have demonstrated publicly that they do not understand the platform (Pegg 2019). Facebook admits this – the 2020 white paper Charting a Way Forward details that, while Facebook is willing to be a partner with governments in regulation, it is itself external to democracy:

People may expect similar due process channels to those that they enjoy elsewhere in modern society. For example, people in liberal democracies may expect platforms to draft content standards with user and civil society input in mind, as well as the ability to seek redress if they feel a decision was made in error (Bickert 2020, pp. 3-4).

In summary, Facebook reaffirms relationships with states by refusing to engage with those that seek to regulate it, demonstrated again during Facebook’s restrictions on news media in Australia in early 2021. The one state it does regularly engage with, the US, is publicly humiliated by Facebook’s executives for not knowing enough about the net state it seeks to regulate, while Facebook proclaims to welcome regulation - if only states were able to understand it.

3.5 Mobilisation
The trajectory of this actor-network presents the final of Callon’s (1986) four stages of actor-network assembly - mobilisation, where Facebook reinforces its control of both social and material dimensions of the actor-network. Facebook succeeds in silencing
states, either through refusing to attend government hearings or by demonstrating the failure of senators to comprehend changing technologies in those hearings. This process is enacted to ensure Facebook’s continued dominance and freedom to extract data - not to support democracy.

The individuals that live within these states, existing as interlocuting denizen-users within the Facebook net state, are treated as the source of commodified data and are secured in place through a shareholding structure that prevents the overthrow of that system. Rather than showing off individual users at its meetings, Facebook has become a unit of force that transforms users into data, and data into imperatives for growth of market capitalisation. As for its instrumentarian structure, Facebook’s modelling along the lines of a society of control may have contributed to decreasing trust in states, substituting privately governed techno-societies for a social within the state and providing a sense of certainty in an uncertain time (Zuboff 2019, p. 384).

3.6 Summary
This chapter has established the existence of the corporate net state through a case study of Facebook. Through examination of how Facebook is able to assert its own interests against those of states, I have demonstrated how Facebook cursorily fits with our revised core definition of the net state, with an additional corporate caveat: it exists primarily in cyberspace, possesses a global population of denizen-users cemented in place by a restrictive shareholding structure, and imposes its twin imperatives of surveillance capitalism and instrumentarian power upon the rest of the world, assisted by a corporate structure that prevents the overthrow of its ruling priesthood.
Chapter 4: The Non-Corporate Net State

4.1 The Non-Corporate Net State

The second type of net state to be proposed here, the non-corporate net state, differs from its corporate sibling through its lack of a dominant economic imperative. While Wichowski (2017) argues for the existence of such a net state, subsequent analysis omits the concept altogether (Wichowski 2020). Through a case study of the internet imageboard 4chan, this chapter shall serve to demonstrate the existence of non-corporate net states. I will aim to distance the net state from the concept of Big Tech and anxieties surrounding large MNCs challenging states to frame the net state as a primarily techno-social phenomenon. A combination of lacklustre regulation and dromology are demonstrated here to be as critical to the success of the net state as surveillance capitalism.

The case study here builds on a question left unanswered by Zuboff (2019) - that is, whether instrumentarian systems can exist without surveillance capitalism. Thus, while non-corporate net states exist primarily in cyberspace and advance their own agendas, the denizen-users residing within are induced to participate in a hive mind, achieving goals without ingesting human existing into algorithms designed for profit extraction. Relationships are thus formed without relying on a corporate entity - data is not sold, platforms are not purchased, and shareholders do not form a priesthood. Although non-corporate net states possess priesthoods, these are ephemeral in nature, and do not reflect the control afforded to major shareholders in a company.

4.2 The leaderless counter-revolution

4chan was founded in 2003 by Christopher Poole (aka 'moot') and was designed as an unlicensed English-language version of Japanese imageboards such as Futaba Channel (commonly known as 2chan) (Hine et al. 2017, p. 92). Imageboards continue to be popular in Japan for sharing memes and discussing anime and video games. Poole served as site administrator until 2015, when the site was acquired by Hiroyuki Nishimura (Poole 2015).

4chan’s location and borders within cyberspace are thus described (Blount 2019) as being within the twin domains of 4chan.org and 4channel.org, with material anchors in
the form of servers located in California (Poole 2012). This territory is inhabited by a memetic, transgressive discourse coagulating around more than 60 ‘boards’ discussing specific topics including anime (/a/), fitness (/fit/) and pornography. The boards available to a user depends on the domain used. For example, the ‘traditional games’ board (/tg/) containing discussion of board games, wargaming, and roleplaying games is accessible from both 4chan.org and 4channel.org. However, ‘not safe for work’ (NSFW) boards are only accessible via 4chan.org. In a 2018 Q&A thread, Nishimura indicated that the creation of a safe-for-work version of the site was due to advertisers refusing to buy ad space adjacent to NSFW content (4chan 2018).

Economic imperatives are important, but here they are not the sole driving force. Content moderation, ostensibly conducted by site administrators and volunteers, is light or non-existent irrespective of domain (Hine et al. 2017, p. 93).

If code is law (Lessig 2006), the protocols of 4chan prioritise anonymity and ephemerality, creating a dynamic environment for its approximate 27 million monthly active denizen-users (Signal 2020). This population is stripped of all identity markers - this includes bio-social identifiers such as name and age, and techno-social signifiers such as usernames. However, IP addresses are collected. Unlike the corporate net state, such data is not collected for specific economic benefits, but allows for the net state to pursue instrumentation of end users (Zuboff 2019) more efficiently. Denizen-users are instead labelled with an anonymising string of numbers as a de facto username - depending on the board, this may be generated per post, or remain stable throughout a thread (Ludemann 2018, p. 93). Despite this, 4chan does collect detailed demographics which state that its population is predominantly based in Anglophone countries, including 47% from the United States, and is 70% male (4chan n.d.).

The site possesses no long-term content archive - threads are removed or ‘bumped’ from the site after a short period of time as new content is posted, with the least recent thread on a board being purged altogether. The size of the short-term archive varies between boards (Hine et al. 2017, p. 93).

---

12 This information should be treated with some scepticism - 4chan allows for VPN usage to mask geographic location with the purchase of a 4chan Pass (4chan n.d.).
As a subject of academic enquiry, 4chan “remains largely unstudied” despite its influence upon political discourse and internet culture (Hine et al. 2017, p. 92). Where it is, examination of the net state itself is often conflated with a personal attack on the politics of the reader. Following the publication of *Kill All Normies* (2017), author Angela Nagle was subjected to a torrent of online criticism for drawing parallels between the memetic structures of 4chan and Tumblr-brand identity politics of the mid-2010s (Libcom 2018), her work labelled an “anti-Left polemic” (Cummings 2017).

Existing analysis of 4chan tends to skew towards /b/, one of the site’s first two boards and a major driver of 4chan’s role in generating internet culture (Ludemann 2017; Tuters & Hagen 2020). As net states draw their ability to influence other actors from being non-monolithic (as opposed to states) and dialogic (as opposed to legacy media), characterising one board as representative of all 4chan is inaccurate. So too are proclamations in academic and popular literature that 4chan is wholly populated by fringe political movements such as the alt-right. While 4chan did serve as a staging ground for that movement, it did the same for Anonymous, and later QAnon - both distributed movements occupying vastly different memetic spaces (Hine et al. 2017; Martineau 2017). More recently, the role of /pol/ (the “Politically Incorrect” board) has been examined due to its role in influencing wider far-right discourse (Ludemann 2018; Sparby 2017). Yet this, too, generally conflates 4chan as a single polity with one of its prefectures.

### 4.3 Dramatis Personae

Since its establishment in 2003 the 4chan net state has served as an influential generator for internet culture - the first, and most well-known ‘meme factory’ (Poole 2010; Sparby 2017, p. 87). Upon accessing the site, 4chan’s denizen-users join a collective swarm or hive mind with a stable, shared collective built on established norms and behaviours (Mitew & Wall 2017; Sparby 2017, p. 87). This explains why specific segments of 4chan are conflated with the site as a distinct actor - an action undertaken by a single user or board can be equated with the site itself (Sparby 2017, p. 87). Given a lack of bio-social and techno-social signifiers aside from numerical labels, an individual denizen-user only sees a monolithic 4chan as a prosthesis for memetic survival rather than the users on the other side of the screen (Virilio 2006, p.
114). Through participation, other denizen-users simultaneously serve as general population and OPP, fulfilling the roles of both priest and parishioner.

Unlike Facebook, 4chan’s site administrator and moderators do not guide the net state’s agenda. Instead, the direction of the net state and its interaction with other actors is determined entirely by the population, extending the demotic aspect of the site (Turner 2010, p. 2) to its belief-driven agenda and allowing it to function as a unitary hive mind. Thus, 4chan’s entire population serves as its priesthood. This assemblage is illustrated in Figure 3 below.

**Figure 3:** An illustration of the 4chan actor-network, based on a similar diagram from Callon (1986 p. 207). Note the presence of memes as distinct actants.

### 4.3.1 Problematisation

Much like Facebook, 4chan presents itself to other actors as indispensable to socialising in the age of cyberspace - in this case, a community free of the bounds of political correctness and identity. Participation in 4chan discourse, irrespective of the topic, is highly memetic. So too is its problematisation (Callon 1986). Indeed, the reason why individual segments of 4chan are conflated with the entire net state is their
capacity to weld together adjacent actors into a unified assemblage despite exhibiting the characteristics of a distributed network. Key actors and their relationship to 4chan as OPP are illustrated in Figure 3. 4chan must assert itself against state actors, its denizen-users as simultaneous internal and external actants, and memes as identity markers for denizen-users.

To stabilise the parish, internet memes provide a substitute form of identity marker, allowing for the creation of membership-based distinctions (Nissenbaum & Shifman 2017). Coined by Dawkins (2006), memes are defined as the smallest possible unit of culture, which replicates in the mind of other individuals similar to how genes replicate to create life (p. 192). By this definition, all forms of human expression are communicated via, and comprised of, memes. The derivative internet meme is a digital object such as an image macro, video, or soundbite, which replicates in cyberspace through the efforts of denizen-users remixing and sharing them (Nissenbaum & Shifman 2017, p. 484).

In the absence of other identity markers, denizen-users develop a collective identity built on memes as the prime vector, assisted by anonymity and minimal moderation ascribed by 4chan’s protocols (Sparby 2017, p. 88). User behaviour is shaped as a “memetic recapitulation” of the behaviour of others (Sparby 2017, p. 86) within a thread or board to impress other inhabitants with their understanding of the site’s culture and etiquette. In short, “each participant posting a meme on 4chan simultaneously co-constructs himself or herself and the collective community in which she or he operates” (Nissenbaum & Shifman 2017, p. 488). Memes are thus drawn to 4chan as their OPP, as they cannot replicate in the absence of users (as demonstrated in Figure 3). Denizen-users unfamiliar with memetic norms are labelled as newfags, a derogatory term attacking outsiders using the exact transgressive memes the targets do not understand (Nissenbaum & Shifman 2017, pp. 489-490).

As a non-corporate net state, 4chan is not a practitioner of surveillance capitalism. However, the above process of memetic recapitulation is a form of instrumentarianism - a structural mode that is both an opposite and twin of totalitarianism, albeit one that Zuboff (2019) slaves to surveillance capitalism without consideration of non-marketised actors. This participatory, collegial instrumentarianism reflects the concept
of the ‘hive mind’ applied to 4chan by Mitew & Wall (2017), with the net state serving as a distributed network (Baran 1962, pp. 3-4). Each node is induced to behave as part of a swarm, with a centralised strategy, decentralised tactics and distributed formations (Mitew & Wall 2017), without needing to export this social experience for profit. Thus, 4chan is governed by an OODA loop - a “feedback decision cycle of observing, orienting, deciding and acting” developed by Boyd (1986; Mitew & Wall 2017), undertaken autonomously by each denizen-user in their own memetic recapitulations while contributing to a wider entity. As the non-corporate net state possesses such an innate capacity to effect rapid change and exchange of information, it can be considered dromocratic, more so than the corporate net state (Virilio 2006). Whether or not this is a net positive is irrelevant.

4.4 Reassembling the counter-revolution
Having problematised its relationship with other key actors, 4chan’s interessement and enrolment are similarly memetic. It is these stages where the significance of 4chan for states in terms of national security policy is visible, as it directly intersects with state interests through proclamations and tricks. As efforts by the state to control net states recognise only physical realities (Blount 2019, p. 2; Evans 2019), 4chan’s technosocial serves to challenge states by extending its politics of transgression into the physical.

4.4.1 Intersettement
The transgressive brand of discourse that 4chan is known for is argued by Nagle (2017, p. 28) to at once reject leftist ideas and assume the aesthetics of counterculture. A rejection of authority is built into the culture of cyberspace - 4chan’s aesthetic choices are thus in keeping with Barlow’s (1996) championing of collective action and framing of states as aliens to cyberspace, with ironic humour and memes used as interessement devices to shut out states. Both interpretation and judgement are “evaded through tricks and layers of metatextual self-awareness and irony” (Nagle 2017, p. 31). Any denizen-user of 4chan can justify homophobia, racism, fringe political views, or advocation for terrorism on the grounds that doing so is an irony-laden rejection of imposed morality that still recognises such behaviour as horrible. This includes enacting said behaviours through what Her (2019, p. 404) refers to as detournement, that is, to detour or hijack the internet culture of ‘normies’. In this
process, there is no ownership of a meme, only its annihilation through emulation and obfuscation through transgression. The distributed nature of 4chan allow it to manifest its politics of transgression anywhere in the form of scaleable memetic offensives across the entire periphery of the distributed network, from direct force engagements or attacks on critical infrastructure, to individuals performing terrorist acts in Western cities, as well as attacks across media under the same open source dynamics (Mitew & Wall 2017).

Such actions demonstrate an open-source insurgency that, while reflective of the actions of a monolithic corporate net state, are not planned or consistently effective and are instead conducted and directed from the bottom up (Robb 2017). As such, rather than proclaiming a set of facts via manifesto, 4chan is able to simultaneously proclaim and act out its own reality, leading to a rapid reaffirmation of its relations with other actors. It does so through “raids”, defined by Hine et al. (2017, p. 98) as offensives that disrupt actor(s) through content, rather than network infrastructure.

4.4.2 Enrolment

While 4chan raids are typically executed by /pol/ or /b/, previous research limits the impact of these raids to other net states and assumes that both the perpetrator and target net states are wholly implicated. Nagle (2017, pp. 46-47) notes that attacks made by the alt-right against Tumblr deliberately targeted a certain brand of identity politics made popular on that site, yet the whole site was not affected.¹³

Raids demonstrate the scaleable nature of the swarm and are a key means to enact enrolment. 4chan activity tends to increase during and after raids, including those that explicitly undermine the state’s monopoly over the use of physical violence within its territory (Weber 2019, p. 137). Immediately after mass shootings perpetrated by 4chan denizen-users in Christchurch, New Zealand and El Paso, Texas in 2019, activity on 4chan drastically increased (Malevich & Robertson 2020; Zelenkauskaite et al., 2020). Raids on other net states and segments of their populations nevertheless do serve to affirm the relationship between state and net state - while 4chan could send a member of its priesthood to government hearings, it would betray its encoded anonymity in

¹³ Until the site was purchased by Yahoo in 2017 and much of this content was purged (Nguyen 2021).
doing so. Instead, it relies upon the nature of cyberspace’s inhabitants as hyper-
pluralistic, comprising multiple representations of a given individual (Schmidt & Cohen
2013, p. 32). As denizen-users are in some way inhabitants of a state, raids on the
physical will impact the state. Moreover, state moves to counter net states can only
occur through those physical avenues - either by addressing the user or cyberspace’s
underlying technical infrastructure. Thus, 4chan must perform itself in material terms.

The 2016 #DraftOurDaughters distributed memetic warfare campaign provides a
prime example. Engineered by 4chan denizen-users during the 2016 United States
presidential elections, primarily on /pol/, the campaign was designed to hijack concern
over Democratic candidate Hillary Clinton’s complex relationship with the Russian
Federation by sharing memes suggesting that Clinton would amend conscription
policy to include women in a potential war with Russia (Mitew & Wall 2017). The
campaign was developed though this hive mind dynamic. Users ‘swarmed’ to develop,
prototype and deploy media objects in public with increasing intensity as more users
joined the hive. Deploying Clinton campaign assets including official logos and
typefaces extracted from its official website, the style of deployed memetic objects
became increasingly consistent. Objects were then shared on other platforms, filtering
first into Reddit followed by Twitter and Facebook. This served to contribute to a wider
open-source insurrection that resulted in the election of Donald Trump as President -
however, the enshrinement of anonymity in 4chan’s code makes attribution
impossible. Indeed, the Trump campaign or foreign intelligence operatives (Kollars
2020) could have easily as participated as you or I.

4.5 Mobilisation
Similar to Callon’s (1986, p. 215) assessment of the mobilisation of an actor-network
involving scallop farms in France, certain actors in the assemblage are incapable of
expressing dissent independently. In each dialogic interaction, an individual denizen-
user is drawn into a wider hive mind consisting of every other denizen-user rendered
down to anonymised interactions, who in a specific interaction can speak only for
themselves rather than the wider population. Denizen-users additionally serve as a
priesthood for 4chan through memetic recapitulation, as they simultaneously establish
the belief-driven agenda and are subject to it. 4chan, its denizen-users, and state
representatives (both the state in general and citizens affected by raids in particular)
are capable of speaking for themselves. However, memes - reliant upon 4chan and denizen-users to speak - remain silent. Instead, they vote and grant support (or dissent) via replication. Future analysis might inspect the meme as a dissenting actant. Other actors in the assemblage perceive 4chan as a monolithic entity through its ability to reinforce a shared identity within its population - in actuality, it is highly decentralised.

4.6 Summary
This chapter has examined the non-corporate net state by expanding its remit to include networked actors other than multinational corporations. This incorporates the modified definition proposed in the literature review and has also served to decouple instrumentarianism from surveillance capitalism where the net state is concerned. As a net state, 4chan exists primarily in cyberspace within two domain enclosures, possesses a global population of denizen-users serving as priesthood and parish, and works to impose a collaborative, memetic agenda upon its own population and other actors in its orbit.
Chapter 5: The Client Net State

5.1 The Client Net State

The third type of net state to be identified here is also the most difficult to conceptualise, as it debases fundamental tenets of cyberspace. Client net states can be thought of as the digital equivalent of a client state - a net state dependent upon a state actor. While they exist in cyberspace with a global population of denizen-users and pursue their own agendas (Wichowski 2020), client net states are wholly dependent upon a state. This chapter will first examine client actors in international relations and cybercultural theory, before proceeding to a case study of Chinese-language social media service WeChat - a client net state of the People’s Republic of China. This chapter will distinguish the client net state from the previous two variants and illustrate how they may be leveraged to extend control beyond the physical borders of a state.

5.2 Instruments of Servitude

Net states and states are both products of codified programmes of relations across a social body (Foucault 2009; Passoth & Rowland 2010). A client state, however, is a state “economically, politically, and/or militarily dependent” upon another within a relationship affording benefits to both parties (Graham Fry, Goldstein & Langhorne 2002, p. 10). The concept has a precedent in antiquity. The Roman Empire utilised client kingdoms to control parts of its frontier, such as the Bosporan Kingdom in modern Crimea (Haensch 2009 p. 211; Schneid 2008 p. 572). The Roman historian Tacitus thus labelled client states as “instruments of servitude” (Tacitus 2013). Later examples, such as Napoleonic France’s client Confederation of the Rhine, were created from previous polities defeated in war and demonstrate the value of empire-building by “fostering satellites” (Schneid 2008, pp. 571-572). In each case, the client state existed at the pleasure of a sovereign Emperor indispensable to others in the assemblage.

In cybercultural terms, clients are subject to a similar programmatic regime. Client-server relationships are a critical component of internet functionality. Hypertext Transfer Protocol (HTTP), the main protocol allowing web browsing, is built on such a relationship - content is hosted on a ‘server’, which a ‘client’ must request data from.
via a HTTP request, enabling web pages and documents to be accessed by an end user (Bell et al. 2004, p. 89). Other web applications are built on similar relationships. Music streaming service Spotify and Valve Corporation’s Steam game distribution service both run on closed-source client systems, which cannot be used without users being forcibly prompted to install updates by the server (Kreitz & Niemela 2010; Werning 2019).

Though less common now due to privatisation, state-controlled telecommunications enterprises were prominent features of the early digital age. Telstra, formerly Telecom, was owned wholly by the Commonwealth of Australia before being privatised over 14 years from 1997 to 2011 (Castelnovo, Del Bo & Florio 2011, p. 106). Client net states may also be controlled through non-financial mechanisms. The Russian Federation has moved to prevent anti-state speech on Russian social media service Vkontakte by leveraging the close association between Russian President Vladimir Putin and Alisher Usmanov, the co-owner of Vkontakte’s parent company Mail.ru Group (Myles-Primakoff & Sherman 2020; Vasilyeva 2014).

Client net states have subsequently been suggested as solutions to an independent net state possessing unchecked authority. This is not limited to illiberal states and empires - though Vkontakte is one example, liberal democracies have also proposed this. A government-owned social networking site was proposed by the Australia Institute in 2020 to lessen the potential impact of corporate net states ceasing operations in Australia in response to the News Media and Digital Platforms Mandatory Bargaining Code (Guiao 2020 p. 27). The idea gained traction following Facebook’s ban of Australian news media on its platform in February 2021.

Wichowski (2020) implicitly refers to client net states through analysis of the Social Credit System (SCS) in the People’s Republic of China – a state-wide interressement device that co-opts WeChat and other digital services into an immense surveillance apparatus. However, her analysis lacks reference to specific net states and focuses on the state as material rather than social, characterising the SCS as a single control vector rather than a patchwork regime of oligoptica (Latour 2005, p. 181). While the following case study focuses on China, it is also a cautionary tale not of an Othered cyberspace beyond the Great Firewall, but of internet regulation’s current trajectory.
Indeed, should client net states become the norm for state control of cyberspace, it would spell the end of cyberspace as a free, consensual hallucination.

5.3 Dramatis Personae
Problematising WeChat as a client net state requires an examination of China’s rise in cyberspace as part of a broader state-driven strategy to propel economic growth under the aegis of the CCP (Bozhkov 2020). The PRC has supported the development of digital ecosystems under its aegis since the Twelfth Five-Year Plan of 2011-2015 (Hong 2011). China is also a source of significant anxiety regarding cyberattacks for Western countries but is not mentioned by name in terms of foreign interference in Australian cyber strategies (Spry 2019, p. 63).

WeChat, launched by technology conglomerate Tencent in 2011 under the name Weixin, is commonly referred to as an ‘everything app’, both “massively popular and increasingly integrated into civic life in today’s China” (Wu & Wall 2019 p. 1715). As of 2020, WeChat possesses a global population of approximately 1.206 billion denizen-users (Tencent 2020). This population is estimated to spend a third of their mobile time on WeChat, returning to the application at least ten times a day (Ryan, Fritz & Impiombato 2016, p. 6). WeChat functionalities include instant messaging, video conferencing, gaming, a public account system similar to Twitter, and WeChat Pay, a digital wallet service provided to all users (Knockel et al. 2020).

Registering for WeChat must be completed using a phone number. All users with Chinese phone numbers are granted digital denizenship on Weixin, whereas all international numbers use WeChat (Ryan, Fritz & Impiombato 2020, p. 25). Additional functionality and heavier content controls are available to those users on Weixin, and a denizen-user remains attached to Weixin even if they switch to an international phone number or travel outside of China. WeChat and Tencent thus function as a single regime, with the latter serving as the priesthood of the former (OPP - β in Figure 4) similar to Facebook Inc. and the platforms it controls.

---

14 Weixin was rebranded as WeChat for international audiences in 2012. The Weixin name is retained within China, and Tencent treats the two as the same platform in its reports (Tencent 2020).
5.3.1 Problematisation

WeChat is owned and operated by Tencent, a major Shanghai-based MNC with interests in video games, social media, and other internet-related products (Tencent 2020). Here, the priesthood (Zuboff 2019, p. 466) is led by Ma Huateng, Tencent’s co-founder, CEO, and China’s richest man. Like all Chinese MNCs, Tencent is subject to strict security and counter-espionage laws, chiefly among which is a requirement in the PRC constitution for any enterprise with three or more CCP members to host internal party committees (Cave et al. 2019). Tencent’s board of directors alone has enough Party members to fulfil these requirements (Tencent 2020). Ma is one of these, serving as a delegate to the rubber-stamp National People’s Congress (Tabeta 2018).

By 2013, Tencent was one of the only Chinese technology forms to have publicly disclosed in English its internal Party structure, which in 2017 comprises 3,386 CCP members across 9 general branches and 8 party branches, along with a party propaganda magazine and an automated human resources system to identify CCP members in its employ (Australian Strategic Policy Institute 2019). Having party membership is essential to succeed in business within the PRC as it creates career opportunities (Straits Times 2017). Dissenting businesspeople are forcibly disappeared, as Alibaba group CEO Jack Ma was in 2021 (Majeed 2021). Thus, the CCP can be considered the true priesthood and OPP here, illustrated as OPP - $\alpha$ in Figure 4 below.
Figure 4: Key actors in the WeChat-PRC assemblage. Note the presence of two OPPs around which relationships are concentrated. OPP - α is dominant, forcing actors passing through OPP - β to also pass through it. The presence of one OPP does not preclude the existence of others within an assemblage. Based on diagram from Callon (1986, p. 207).

The integration of WeChat (and Tencent) with the PRC is critical in examining the position of denizen-users in this assemblage. Though the term ‘citizen-users’ could be deployed in reference to WeChat’s role within the PRC, I shall retain the denizen-user term here for two reasons. Firstly, WeChat users have no say in WeChat’s governance, and secondly, WeChat’s deployment as an interessement vector outside the PRC involves users who are not PRC citizens. While Chinese media serves an essential role in stabilising a sense of identity in Chinese communities outside the PRC, social interaction is no longer dependent on simultaneous physical co-presence - instead, mediated techno-socials serve as cultural brokers (Zhang & Wang 2019, pp. 54-57). Diaspora, defined as a “spatial concept” that overlays experience, location, movement and economic activity within an interrelated set of places (Zhang & Wang 2019, p. 54) is critical to understanding WeChat’s success outside of China. A long-term examination of PRC migrants by Gao (2006) found that Chinese diaspora communities oscillate between a sense of belonging within new home countries and a
sense of loyalty to China, shifting between the two to prevent marginalisation and adapt to hardship and racism.

Where PRC client net states intervene to great effect with the diaspora is in manipulating the reputational identity concept of *guanxi*. *Guanxi* is never shaped in isolation, instead building one’s social capital through trustworthiness, reciprocating favours, obligations and social skills (Wu & Wall 2019, p. 1719). Controlling the techno-social used to contact family ‘back home’ allows the PRC to harness *guanxi* to prevent contentious political thought. Exhibiting anti-Party sentiment through private chat or public broadcast is prevented through algorithms and *guanxi* penalties (Wu & Wall 2019, p. 1719). That WeChat is essential for diaspora communities has the added effect of politicians in democracies with sizeable Chinese communities such as Australia having to use the app to communicate with voters in those communities (Ryan, Fritz & Impiombato 2020, p. 29). While providing a means to achieve a stable long-term identity, using *guanxi* to instrument denizen-users outside the PRC demonstrates how client net states are leveraged to effectively extend national borders into cyberspace.15

5.4 One App, One System

While the relationship between the PRC and its inhabitants is primarily physical, that between its client net states in cyberspace has yet to be formalised. WeChat must now be bound to the problematisation through interessement (Callon 1986), and the relationship must be performed into existence - the enrolment (Callon 1986). Sear, Jensen and Chen (2018) note that controls over online expression are present within the PRC, but it is “unclear” whether those same controls are present outside it. As the term ‘platform’ obscures the agency of a techno-social mediating user experiences (van Dijck 2012), it follows that WeChat’s mediation of experience obscures its subjugation by a higher power. Cave et al. (2020) and Ruan et al. (2016) both note that WeChat, while notionally being governed by a so-called “One App, Two Systems” policy16 is instead managed as a single ecosystem with two different veneers. Under

---

15 The 2020 Hong Kong national security law and the 2021 China Coast Guard law also include provisions for the PRC to enforce domestic laws outside its geographic territory (Martinson 2021, Tsoi & Wai 2020).

16 This is not the policy’s formal name, but a label derived from the ‘One Country, Two Systems’ governance model in place until 2020 in Hong Kong and Macau.
this system, in theory only Chinese users initially registered with a Chinese phone number (and thus inhabiting Weixin) are subject to censorship. Less restrictive rules apply to those outside China registered with a foreign number despite residing in the same ecosystem (Ryan, Fritz & Impiombato 2020, p. 25). In practice, this is not the case.

5.4.1 Interessement

China’s client net states are kept in place through a doctrine of ‘cyber sovereignty’, which argues that the PRC is the critical OPP for the experience of cyberspace in China (Xi 2015). The CCP has feared “ideological subversion” and challenges to its narrative from cyberspace since its inception (Creemers 2020, p. 107). Cyber sovereignty prevents this and ensures control, promoting a strategy of non-interference that

Respect[s] the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies...No country should pursue cyber hegemony, interfere in other countries' internal affairs or engage in, connive at or support cyber activities that undermine other countries’ national security. (Xi 2015)

Cyber sovereignty is thus a techno-social doctrine essential for the PRC to maintain its core values, allowing states to prevent their citizens from being exposed to ideas harmful to the regime (Schia & Gjesvik 2017). As such, networked actors engaging in political discourse in China’s cyberspace remain subject to a system of regulation combining hard and soft controls (Schneider 2016, pp. 2664-2665).

This system was not imposed upon existing infrastructure, instead arising with the nascent digital sector in China. Cyber sovereignty is a rejection of an earlier version of cyberspace that fundamentally disagrees with the core values of the CCP (Barlow 1996). China’s status as a latecomer to cyberspace prevented it from influencing cyberspace as it emerged - instead, technologies were “marshalled” as part of a broader Party project to combine economic development with strict political control rather than the Romantic, utopian space envisaged by Barlow (1996; Creemers 2020, p. 113). Thus, any economic imperative is superseded by a political one, preventing
WeChat – or the PRC - from being labelled as surveillance capitalist (Bozhkov 2020, pp. 1-2; Zuboff 2019). ¹⁷

The client net state thus serves as one moulding enclosure within a wider society of control - an inescapable techno-social extension of the Party-state (Deleuze 1992, p. 4), and one that has controlled a dromocratic vector for its own ends by creating and manipulating digital infrastructures (Virilio 2006, p. 85). While Medcalf (2020) refers to this as a new kind of “networked totalitarianism” incorporating a vast apparatus of surveillance and coercion (p. 246), the indispensability of WeChat to daily life in the PRC and Chinese-language communities makes it far more instrumentarian than totalitarian (Zuboff 2019 p. 385). As such, the client net state can be considered as both dromocratic and instrumentarian, although both modes are subject to the wider goals of a state actor. This inverts Schmidt & Cohen’s (2013) assertion of high tech being faster than the state.

5.4.2 Enrolment

As previously established, declarations are essential for net states as vectors to establish facts out of thin air (Zuboff 2019, p. 176) and enrol actors into an assemblage (Callon 1986). Two types of declarations imposed on WeChat’s denizen-users are examined here. The first, government declarations, serve to establish the PRC’s cyber sovereignty doctrine which argues that states should not interfere with other states in cyberspace, and that states are entitled to control non-state actors (Creemers 2020, pp. 114-115). This rejects existing multistakeholder norms of cyberspace governance and the aterritorial nature of cyberspace (Roguski 2020, p. 65). Adhering to this doctrine ironically allows the PRC to interfere in the jurisdiction of other states and net states.

The second declaration type is that programmed into WeChat to censor discussion. Ruan et al. (2016, pp. 10-12) note that server-level keyword censorship is implemented by Tencent to censor anti-CCP speech and pro-democracy mottos. Tests run in 2013 caused an alert to be displayed to the sender, but not the receiver (Figure 5). Offending URLs and links are also censored, with sharing functionality

¹⁷ This label fails to describe the PRC in cyberspace - surveillance is a natural part of state functionality, and the PRC is notionally a communist state.
disabled or viewable only in English (Ryan, Fritz & Impiombato 2020, pp. 30-31). Subsequent analysis in 2020 found that these censorship measures were implemented for all WeChat users irrespective of their geographic location or status as a Chinese or internationally registered account (Knockel et al. 2020).

![Image](image.png)

**Figure 5:** Alert displayed to WeChat users on a Chinese network (left) and a Canadian network (right) when attempting to use censored keywords in 2013 (Ruan et al. 2016).

Keyword censorship forms part of a “programme of negotiations” designed to assert PRC authority (Callon 1986 p. 212). Denizen-users who the PRC determines require special attention due to aberrant behaviour on WeChat are pressured to cease this behaviour via guanxi or other vectors. Former Tiananmen Square student leader Zhou Fengsuo, now based in the United States, indicated that his WeChat account had been repeatedly suspended over a seven-year period (Ryan, Fritz & Impiombato 2020, p. 25). Uyghur activists living overseas have also recorded threats from PRC security forces who have obtained data from WeChat to harass family members living in the PRC. The diaspora is conscious of being monitored at all times - evidence of a surveillance regime wherein behavioural surplus is ingested not for sale, but for the structuring of a durable, instrumentarian assemblage (Ryan, Fritz & Impiombato 2020, pp. 25-27). The algorithms detecting banned keywords, images and references serve as an interessement device. This also results in foreign politicians being subject to
PRC authority. In response to foreign ministry spokesman Zhao Lijian’s posting of a meme critical of Australia’s response to a war crimes investigation, Prime Minister Scott Morrison issued a statement via WeChat criticising the image and praising Chinese-Australians (Harvey 2020). This statement was blocked by WeChat within 24 hours, on the grounds that it violated regulations by distorting historical events and confusing the public (Needham 2020). In short, WeChat is utilised to silence critics and assert PRC dominance far outside its borders in direct contravention of its own cyber sovereignty doctrine.

5.5 Mobilisation
Across the entire assemblage, the OPP for all other actors is the PRC. By concentrating all relations within itself, the PRC “has conflated its own regime survival with infringement” on the security of other states through positioning its client net states as vectors for instrumentation of the Chinese diaspora (Medcalf 2020, p. 246). WeChat denizen-users, irrespective of geographic location or registration method, have been caught in an extension of China’s Great Firewall, subjecting them to surveillance within a techno-social used as an essential vector for daily life (Ryan, Fritz & Impiombato 2020, p. 2). A monopoly over the means to pursue guanxi keeps denizen-users in line as a form of instrumentarianism, with behavioural surplus used to fuel the system. The actors that should serve as the priesthood, Tencent’s executives, are also co-opted into the system as middlemen whose authority comes from maintaining relationships with higher beings (Virilio 2006, p. 112). The locus of this assemblage remains the PRC - all other actors must pass through it to retain their position.

5.6 Summary
In this chapter, I have demonstrated the existence of client net states, detailing them as actors existing primarily in cyberspace with global denizen-user populations but subject to the belief-driven agenda of a state actor. While WeChat (and Tencent) should function as corporate net states, structuring their relations with other actors according to a profit imperative, the role of the PRC in its success removes any pretence of independence it may otherwise have. Client net states present the most effective method thus far in melding cyberspace into the apparatus of state, codifying relations within a single body rather than competing material and techno-social actors.
Chapter 6: Discussion

This research was designed to identify the ways net states assert themselves as significant stakeholders in cyberspace, and to propose some net state variants. This chapter discusses the major findings in relation to the literature outlined in Chapter 2 regarding the nature of net states, the role of states online, cyberspace, and denizen-users. Suggestions for future research and the limitations of the proposed revisions to the definition will also be discussed. Finally, a short examination of the implications of the net state for policymaking will be examined in relation to Facebook’s unilateral restriction of news media content in Australia in February 2021, which presents the most recent instance to test the actor-network model described here. This discussion will be considered in relation to the research questions:

RQ1: How do net states assert themselves as distinct, state-like stakeholders in cyberspace?
RQ2: How might net states be better classified?

The literature review established that the current definition of the net state requires expansion in terms of cybercultural theory to increase its utility. An expanded definition was proposed based on the following criteria: primarily existing in cyberspace; possessing a global population of denizen-users, and; being capable of advancing a belief-driven agenda independently of states. Three case studies were then deployed to test this revised definition in order to answer the first research question, and demonstrate variations of net states in order to answer the second.

Regarding the first research question, the case studies indicate that although the net state is primarily a creature of cyberspace, its establishment of positions of influence takes place through a process of translation incorporating both material and social objects - that is, a variety of human and non-human actants. This covers a greater range of activities than the original, positivist definition (Wichowski 2020). A great deal of work is involved for a net state to build and maintain its position as OPP. Like states, net states codify relations across a wider social body, thereby exhibiting stateness (Passoth & Rowland 2010). Thus, net states must be examined and considered as
distinct practitioners of stateness. Failing to engage with net states is done at the peril of the state, and the Westphalian international.

Engaging with the second research question required the grouping of net states into three categories based on how they build and codify these relationships. I proposed the corporate net state, with an underpinning MNC and dominant economic imperative; the non-corporate net state, which does not possess a dominant economic imperative or corporate structure; and the client net state, which has wholly ceded agency to a state actor. These categories are not exclusive - more net states may be identified in future, including both new variants and those emerging from combinations of existing ones. The proposed categories accommodate a broad range of means by which net states build relations. Combining IR theory, cybercultural theory and ANT has proven useful in this regard. This interdisciplinary lens is not limited to examining actors driven by economic imperatives alone, although such imperatives are essential to understanding corporate net states and the intermediary OPP of a corporation in the case of a client net state.

This necessitates a re-evaluation of the importance of surveillance capitalism when examining net states. Zuboff (2019) describes the phenomenon as universally applicable to online actors, yet in practice the relationship was only visible in the corporate case. However, instrumentarianism was visible in all three case studies irrespective of economic imperatives, as net states marshall their denizen-users into position. Non-corporate net states do the same with memes, and the client net state is itself marshalled into position by a state actor. Despite Zuboff's (2019) characterisation of the two as inextricable from each other, instrumentarianism is more valuable a framework in comprehending net states than surveillance capitalism. Future research could work to decouple the two, as well as assess the role of platform ecologies and spatiality as forms of online territory.

We might test our expanded definition, and the corporate net state variation, through Facebook’s restriction of legacy media content for Australian denizen-users - a key moment for demonstrating effective cyber statecraft. While social media is a survival prosthesis (Virilio 2006, p. 114) for legacy media, the Australian government’s News Media and Digital Platforms Mandatory Bargaining Code forces Facebook to pay
legacy media for hosting content. As this would obstruct its surveillance capitalist logic, on 18 February Facebook pre-empted the Code and unilaterally imposed restrictions upon its Australian denizen-users preventing the sharing or viewing of news content (Easton 2021), as well as content from charities and some government agencies prior to the Code’s implementation (Reuters 2021a). Figure 6 details this assemblage, which adds legacy media to the assemblage described in Figure 2.

Figure 6: Facebook’s interactions with its Australian actor-network in response to the News Media and Digital Platforms Mandatory Bargaining Code, implemented in February 2021. Based on Callon (1986, p. 207).

Approximately 68% of Australians use the Facebook net state’s platforms for news (Newman et al. 2020, p. 96), forming a problematisation (Callon 1986). Legacy media, though reliant on Facebook and other digital platforms, felt they were not receiving the financial benefits and wished to be paid for their content. When restrictions were enacted by Facebook, the Code - the device meant to establish the government as OPP - had yet to be enacted. A dromocratic programme of relations was thus established, supported by a declaration from Facebook’s chief Australian priest, William Easton (2021) leaving the government scrambling to react.

---

18 The Code was to be enacted on 25 February 2021.
While the restrictions were an effective interressement device, their removal on 23 February (Hitch 2021) is more so. Direct negotiations led to Facebook agreeing to pay major legacy media outlets on a by-case basis. As a corporate net state, Facebook used cash as an interressement device, with the accompanying agreements functioning as enrolment mechanisms (Callon 1986; Neuman 2021). While the Code was established as a means to, among other things, support journalism in regional areas and small media outlets (Frydenberg 2021), in practice the monies paid were not conditional on any investment in said areas.

News media, academics and politicians within and outside Australia characterised the event as a ‘war’ between Facebook and a sovereign country (Reuters 2021b). The United States of America, where Facebook is headquartered, considers the issue external to its relationship with Australia (Reuters 2021b). This effectively grants Facebook license to act out what it already possesses - an independent foreign policy. This constitutes the mobilisation (Callon 1986). Not only has Facebook remained OPP without being forced to reform, but legacy media are now even more dependent on it in both in terms of audience reach and revenue. Denizen-users are restored access to content, having acknowledged that Facebook possesses a monopoly over the means of media within its online borders. Australia has failed to address the underlying techno-social problems of cyberspace intersecting with its physical territory. Facebook’s ‘unfriending’ of Australia thus demonstrates the value of the net state concept, and the extent to which Facebook’s cyber statecraft has succeeded.
Chapter 7: Conclusion

Net states are crucial stakeholders in cyberspace - and states ignore them at their peril. Inhabited by global populations of denizen-users and driven by an immense technological base, net states are assemblages of human and non-human actants capable of challenging states in both material and social terms. Like states, net states codify relations across a social, and should be considered distinct practitioners of stateness and political actors on par with states. What is significant about net states is the pattern they represent. Once only challenged by other states, then by terrorist groups and MNCs, states are now confronted by alternative state-like actors emerging from cyberspace.

A crucial aspect of the net state’s character is its ability to impose and stabilise relations with adjacent actors. How it does this varies considerably between net states, although common trends have revealed at least three types of net state. While some may be as large as states, their size is an outcome of a high-velocity programme of relations. Actor-network theory reveals that this programme occurs on a single plane combining the material and social (Latour 1992), while states may only respond in the realm of the material (Blount 2019, p. 2). While code is law and thus social (Lessig 2006), the enactment of law is distinctly material. This allowed me to answer the first research question: how do net states assert themselves as distinct, state-like stakeholders in cyberspace?

Intense variation in structure and the means by which net states structure relations with other actors allowed me to answer the second research question: how might net states be better classified? The original definition does not address this, only stating that net states exist (Wichowski 2017; 2020). I proposed three variants - the corporate, non-corporate and client net state. While practices of surveillance capitalism have been observed in Silicon Valley’s social media titans (Zuboff 2019), the original net state definition does little to accommodate actors from anywhere else, or actors that are not multinational corporations. These did, however, all share instrumentarian logics, inducing their denizen-users to wholly depend on them for social life online.
The practical value of the net state, and the revised definition and variants described here was again demonstrated, twice, during the final months of writing this work. In addition to Facebook’s ‘unfriending’ of Australia described in the previous chapter, the actions of investment swarm WallStreetBets (WSB) are worth examining. Driven by memetic share trading strategies, WSB began purchasing GameStop shares in early 2021. This increased the value of those shares while inflicting significant losses on hedge funds betting against them, bankrupting at least one fund (Yeung 2021). When pressed on the matter by the US Congress, WallStreetBets member Keith Gill justified his investment strategy by stating he simply liked the stock (CNET 2021), and that WallStreetBets functioned as a swarm network (Mitew & Wall 2017). Deploying the reconceptualised net state definition developed in this thesis to WSB would assist in answering whether it is a net state, as well as the net state’s temporal and dromocratic dimensions in relation to states (Virilio 2006).

In both cases, state authorities demonstrated a failure to understand cyberspace in material, symbolic and techno-social terms. Dissent to the order based on material realities - hitherto the main way for states to control cyberspace - is becoming increasingly difficult. Had Facebook and WSB been treated as net states, rather than companies or online forums, the results may have been different.

Net states open a raft of new avenues for interrogating who or what controls cyberspace. Future research should acknowledge that net states codify relations across a social body, just as states do, and could examine net states which continue to exist online but encroach upon physical geographies such as Amazon. The role of Elon Musk in relation to net state materiality should also be explored - while this is mentioned in Chapter 2, it should be examined more closely following Musk’s announcement of a potential SpaceX city to be built in Texas in 2021 (Roulette 2021).

Metaphor has already proven valuable in explaining the relational authority of net states. Concepts of digital territory would also be a valuable starting point. While the physical infrastructure underpinning a net state may be based in a state, the controlling priesthood acts in a manner befitting a foreign agent. Future research might examine Facebook’s physical offices as extraterritorial net state embassies, or Amazon Web Services’ servers as freeports. Future analysis, particularly that combining IR and
cybercultural theory as done here, can offer increased value to policymakers by moving from metaphor to praxis.

The mercurial nature of the term ‘platform’ (DeNardis & Hackl 2015) could also be reframed in relation to net states. WallStreetBets, for example, is based on Reddit, but operates across a variety of share trading applications and services. Facebook is one net state, consisting of several platforms (Facebook 2020). Denizen-users, outlined here as demotic subjects of a net state, flit between platforms. How might we conduct a more accurate digital census, or a declaration of denizen-user rights - if any?

In this thesis I have responded to the evolving needs of cyber policy and socio-cultural understandings of cyberspace by expanding what is more mundanely referred to as social media into a separate practitioner of cyber statecraft. The implications of this research are far broader - indeed, they form the core of a new digital international involving states, net states and denizen-users freely associating with one another. New sites and modes of conflict are only now beginning to be understood (Easton 2021). Both the net state and the denizen-user expand the theoretical base of cyber statecraft beyond capitalist frameworks, providing policymakers with a greater ability to comprehend, describe and analyse the structuring principles of cyberspace. This reframing of the techno-social dimension of cyberspace would provide ample fodder for interdisciplinary higher degree research.

States must take the lead and work proactively to reframe relationships with net states, perhaps through a Concert of Cyberspace bringing states and net states together. Hostile net states might be countered through similar measures taken against hostile states, as opposed to reactionary measures such as site and content blocking that address material realities rather than social ones. All these questions and more are interdisciplinary in nature and could be explored in further research.

That the net state exists at all is evidence of a failure on the part of states. It is not that we have sinned by creating technology - it is that states have failed to love and care for cyberspace (Latour 2012). Doing so has permitted the rise of a priesthood which has perfected cyber statecraft, building assemblages which can memetically outfox a
state, cause chaos in its financial markets, strangle its news media, and beat down the doors of its Capitol.

Net states possess direct implications for the future of cyberspace - and indeed, all of us as its inhabitants. Net states are diverse, accessible, increasingly default modes for social life, and overturn every expectation of what power is and where it is concentrated in a world markedly transformed by cyberspace. Meeting the actors that inhabit and control this space as equal authorities, not subjects, is a fundamental challenge to states and the international system they inhabit.
References


Asimov, I 1960, Foundation, Grafton, London

Associated Press 2021, ‘Nevada bill would allow tech companies to create governments’, Associated Press, 4 February, viewed 20 February 2021, <https://apnews.com/article/legislature-legislation-local-governments-nevada-economy-2fa79128a7bf41073c1e9102e8a0e5f0>


Braithwaite, V 2020, ‘Beyond the bubble that is Robodebt: How governments that lose integrity threaten democracy’, *Australian Journal of Social Issues*, vol. 55, no. 3, pp. 242-259


CNET 2021, ‘WallStreetBets goes to Washington: GameStop investor testifies!’, YouTube, viewed 21 February 2021, <https://www.youtube.com/watch?v=F3NUNoZPvk>


Collins, R 2009, *Three Myths of Internet Governance*, Intellect, Bristol


Deleuze, G 1992, ‘Postscript on the Societies of Control’, *October*, vol. 59, pp. 3-7


Futter, A 2018, ‘Cyber’ semantics: why we should retire the latest buzzword in security studies’, *Journal of Cyber Policy*, vol. 3, no. 2, pp. 201-216

Fukuyama, F, Richman, B & Goel, A 2021, ‘How to Save Democracy from Technology: Ending Big Tech’s Information Monopoly’, *Foreign Affairs*, vol. 100, no. 1, pp. 98-110


Games Workshop 2017, *Warhammer 40,000 - Codex: Adeptus Mechanicus*, Games Workshop, Lenton, Nottingham


Haensch, R 2009, ‘Not official, but permanent: Roman presence in allied states - The examples of Chersonesus Taurica, the Bosporan Kingdom and Sumatar Harabesi’, in C Eilers (ed.), *Diplomats and diplomacy in the Roman world*, Brill, Boston, pp. 209-225


Medcalf, R 2020, *Contest for the Indo-Pacific: Why China won’t map the future*, La Trobe University Press, Carlton


Nagle, A 2017, Kill All Normies: Online Culture Wars from 4chan and Tumblr to Trump and the Alt-Right, Zero Books, Winchester


Ryan, F, Fritz, F & Impiombato, D 2020, TikTok and WeChat: Curating and controlling global information flows, Australian Strategic Policy Institute International Cyber Policy Centre, Canberra, viewed 19 October 2020, <https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-09/TikTok%20and%20WeChat.pdf?7BNJWaoH1mPVE_6KKcBP1JRD5fRnAVTZ>=

Schaake, M 2021, ‘Big Tech is trying to take government’s policy role’, Financial Times, viewed 29 January 2021, <https://www.ft.com/content/7f85a5ff-326f-490c-9873-013527c19b8f>

Schia, N N & Gjesvik, L 2017, China’s cyber sovereignty, Norwegian Institute of International Affairs, Policy Brief 2/2017


Schneider, F 2016, ‘China’s ‘info-web’: How Beijing governs online political communication about Japan’, New Media & Society, vol. 18, no. 11, pp. 2664-2684


Skinner, B F 1948, Walden Two, Hackett, Indianapolis


Tuters, M & Hagen, S 2020, ‘(((They))) rule: Memetic antagonism and nebulous othering on 4chan’, *New Media & Society*, vol. 22, no. 12, pp. 2218-2237


van Eeten, M JG & Mueller, M 2012, ‘Where is the governance in Internet governance?’, *New Media & Society*, vol. 15, no. 5, pp. 720-736


Wu, Y & Wall, M 2019, ‘The ties that bind: How the dominance of WeChat combines with *guanxi* to inhibit and constrain China’s contentious politics’, *New Media & Society*, vol. 21, no. 8, pp. 1714-1733

Xi, J 2015, *Remarks by H.E. Xi Jinping President of the People’s Republic of China at the Opening Ceremony of the Second World Internet Conference*, Ministry of


Zhang, G & Wang, W Y 2019, “Property talk” among Chinese Australians: WeChat and the production of diasporic space’, Media International Australia, vol. 173, no. 1, pp. 53-65


