Author:
Stevens, Clare L

Title:
'Bounding' US Cybersecurity

Negotiating a Symbolic and Organisational Thing of Boundaries

‘Bounding’ US Cybersecurity: Negotiating a Symbolic and Organisational Thing of Boundaries

Clare Stevens

A dissertation submitted to the University of Bristol in accordance with the requirements for award of the degree of Doctor of Philosophy in the Faculty of Social Sciences and Law. School of Sociology, Politics and International Studies and South West Doctoral Training Partnership, March 2021.

This work was supported by the Economic and Social Research Council (Grant number ES/P000630/1)

WORD COUNT: 88,501

Abstract

Despite its prominence in security discourses and policies in the United States, what counts as 'cybersecurity' and how it is to be practised by state actors is still a matter of contention. While these debates feature recurring accounts of the challenges that cybersecurity poses to longstanding conceptual and symbolic distinctions, by deploying the analytical framework of 'boundary work,' this project critically examines how boundaries are (re)constituted in US cybersecurity politics, and, conversely, the extent to which cybersecurity is shaped by historically resonant boundaries and institutionalised cultures.

The thesis argues that what cybersecurity 'is,' and how its boundaries are drawn, are not overdetermined by strategic or technological imperatives, so much as they reflect the efforts of different entities to defend and extend their own organisational and symbolic boundaries. In adopting such a position, this thesis highlights the boundary work of different actors and their attempts to 'fix' the boundaries of cybersecurity via an in-depth analysis of illustrative junctures and debates in US cybersecurity politics. This in turn opens up critical questions over the extent to which security imaginaries and conceptions of US national identity work as important codes of intelligibility in (and transformed through) cybersecurity politics over time: as the thesis seeks to demonstrate, it finds that technologies, consequential categories, institutional responsibilities, political authority, and national identity are also constituted and challenged in and through these debates.

Addressing these issues, the thesis thus seeks to develop a distinctively processual framework to help security scholars de-essentialise cybersecurity discourses, instead arguing that cybersecurity is best approached as a culturally and temporally contingent concept. Rather than a singular object then, what cybersecurity *is* emerges at the point of boundary work that emphasises different boundaries and characteristics at different times, depending upon the position of the speakers and the resources they can assemble to stabilise their claims.

Keywords: cybersecurity; boundary work; politics; imaginaries; culture; technologies

Dedication and Acknowledgements

This thesis represents not just a lot of time at a keyboard, it is also the product of a journey that has taken nearly seven years, on and off, to complete. A lot of life happened in that time, and I also owe a debt of gratitude and appreciation to a lot of people.

My thanks to the Economic and Social Research Council, and the South West Doctoral Training Partnership, for supporting me in this endeavour, and to the School of Sociology, Politics and International Studies at the University of Bristol for giving me an institutional home. To my supervisor, Dr John Downer, whose impressive attention to editorial detail drove me to finally learn to stop using hyphens and to start telling the story. My thanks too, to Prof David Galbreath. My sincere thanks go too to Dr Columba Peoples, who offered such good humoured and invaluable (but un-programmed) support, guidance and tracked changes. Thank you all so much for your patience on this long journey, and for helping me to one day become an actual grown-up scholar.

To my colleagues and comrades at 1 Priory Road, I salute you. Thanks especially to Dr Cameron Hunter for our heartening discussions over the years on technology, politics and geekery. To my critical cybersecurity compatriot Lilly Muller, thank you for all the great sounding-board talks and support over the years: here's to many more.

My partner Dai has weathered this process with me, and I can thank him for being my steadying rock throughout. Diolch, cariad bach fi. My family have been the intellectual stimulus for this whole venture, so thank you for all the proof reading and debating and encouragement even when it was seemingly impossible. My big little brother Jim especially provided the straight-talking translation service that I needed. My cat Dusty has been the expensive but vital companionable familiar throughout, sitting on the paperwork at those key moments. This thesis is dedicated to Grum (Philippa Gould): I wouldn't have been able to do this without you, and I also took a little bit longer to do it for you. But last of all, present-me is telling past-me to keep at it: it's all worth the effort, even if it feels most lovely only when it stops!

Author's Declaration

I declare that the work in this dissertation was carried out in accordance with the requirements of the University's *Regulations and Code of Practice for Research Degree Programmes* and that it has not been submitted for any other academic award. Except where indicated by specific reference in the text, the work is the candidate's own work. Work done in collaboration with, or with the assistance of, others, is indicated as such. Any views expressed in the dissertation are those of the author.

SIGNED: ...C Stevens..... DATE:....10/03/2021.....

Table of Contents

List of Figures:

List of abbreviations

APT	Advanced Persistent Threat
CDM	Continuous Diagnostics and Mitigation
CDT	Center for Democracy and Technology
CISA	Cybersecurity and Infrastructure Security Agency
CNA	computer network attack/offense
CNCI	Comprehensive National Cybersecurity Initiative
CND	computer network defence
CNE	computer network exploitation
CNI	computer network investigation
CNO	computer network operations
CRS	Congressional Research Service
CSD	Cybersecurity Directorate
CSIS	Center for Strategic and International Studies
CSS	Central Security Service
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DIRNSA	Director, NSA
DISA	Defence Information Systems Agency
DoD	Department of Defense
EFF	Electronic Frontier Foundation
FBI	Federal Bureau of Investigation
GAO	Government Accountability Office
IAD	Information Assurance Directory
IC	intelligence community
ICT	Information Communications Technologies
ISIL	Islamic State of Iraq and the Levant
ISIS	Islamic State of Iraq and al-Sham
ISPs	Internet Service Providers
JCWA	Joint Cyber Warfighting Architecture
JFCC-NW	Joint Functional Component Command-Network Warfare

NCC	National Cybersecurity Center
NCPS	National Cybersecurity Protection System
NDAA	National Defense Authorization Act
NICCS	National Initiative for Cybersecurity Careers and Studies
NPPD	National Protection and Programs Directorate
NSA	National Security Agency
OMB	Office of Management and Budget
ONCE	Office of the National Counterintelligence Executive
PATCH	Protecting our Ability To Counter Hacking (PATCH) Act
PSYOPS	Psychological Operations
SIGINT	Signals Intelligence
STRATCOM	Strategic Command
STS	Science and Technology Studies
TIC	Trusted Internet Connection
TMA	traditional military activities
TTPs	tactics, techniques and procedures
UN GGE	United Nations Group of Governmental Experts
UNGA	United Nations General Assembly
UP	Unified Platform
USCC	U.S. China Economic and Security Review Commission
US-CERT	United States Computer Emergency Readiness Team
USCYBERCOM or **CYBERCOM**	Cyber Command
VEP	Vulnerabilities Equities Process

Chapter One: Bounding Cybersecurity in the United States

1.0 Introduction

Unlike its four predecessors, the fifth iteration of the United Nations Group of Governmental Experts (UN GGE) – who had assembled in June 2017 to consider 'Developments in the Field of Information and Telecommunications in the Context of International Security' – would fail to reach a consensus on how to define and address "existing and potential threats in the sphere of information security." (UNGA, 2015b, p. 2) The self-described task of the UN GGE was to develop international norms for how states should use "information and communication technologies" (ICTs) and govern the "conduct of ICT-related activities," and to subsequently publish their findings in a consensus report (UNGA, 2013, 2015a). Citing the draft report's explicit references to the potential applicability of the law of armed conflict and principles of self-defence to the conduct of such 'ICT-related activities,' Cuba, China and Russia declined to accept the draft (Henriksen, 2019). As members of the group, they disagreed with the conclusions of others in the meetings that international law was applicable to the use and governance of ICTs. Thus, after the UN GGE collapsed, the Cuban representative stated that they were concerned by…

> …the pretension of some ... to convert cyberspace into a theater of military operations and to legitimize, in that context, unilateral punitive force actions, including the application of sanctions and even military action by States claiming to be victims of illicit uses of ICTs (Rodriguez, 2017, p. 1)

They went on to express a concern that the draft report's references to the applicability of the law of armed conflict and international humanitarian law "would legitimize a scenario of war and military actions in the context of ICT" (Rodriguez, 2017, p. 2). While the objections of representatives such as Mr Rodriguez were voiced in terms of the applicability of extant international law to this context, the earlier reports had already decided that the principles of the UN Charter applied to this matter, suggesting there were strategic reasons for their objections (Sukumar, 2017; Henriksen, 2019). These UN GGE meetings had become the foremost international forum for discussions on rules of behaviour for states in cyberspace, but here had apparently broken down on how to classify and govern those behaviours.

These differences in definitions and conceptions of security underpin entire national approaches to the threats, risks, and opportunities thought to come from networked communications and computation, with important implications for the policies and practices that emerge as a result. The earlier consensus reports in 2013 and 2015 had used the terms of 'ICT' and 'ICT-related activities' to describe the object of governance here, rather than security of and in 'cyberspace' (favoured by

the US) or 'information' security' (favoured by the Chinese and Russians for example), so as to avoid such disagreements and foster cooperation. Instead of 'cyberspace,' both China and Russia have tended to frame the issue in terms of 'information space' which for them includes the cognitive space of human information processing and communication. As a result, their concept of security and what they are securing is predicated upon fundamentally different conceptual approaches to that of the US and its allies (Thomas, 2001; Giles and Hagestad, 2013; Godwin III *et al.*, 2014). Security of 'information' is different to security of 'cyberspace' because it focuses political attention and resources on different places, people and technical matters.

Other countries have thus come up with framings of networked communication technologies and their security other than 'cyberspace' and 'cybersecurity.' Concerns like Mr Rodriguez' that the ICT environment may be conceived of and internationally formalised as a theatre of military operations in this way was a reference to the United States' declaration in 2010 that 'cyberspace' was to be conceived of as a domain of warfighting akin to land, air, sea and space (Lynn, 2010). This was followed in September of 2012 with a statement by State Department Legal Adviser Harold Koh that the US recognised that extant international law governing armed conflict and humanitarian law applied to this 'domain' (Koh, 2012). When conceived of in terms of spatial metaphors such as 'cyberspace,' and approached as a warfighting domain, 'security' here may be associated with military and strategic priorities. Meanwhile, a focus on 'information security' as exemplified by other countries implies a conception of 'security' that enrols a broader national and governmental effort of controlling citizens' access to information. As the UN GGE's consensus reports show then, 'cyberspace' is not the only way of framing the opportunities and challenges presented by the internet and globally networked computation.

What is 'cybersecurity,' then? This seems like a simple question, but in fact it has been a matter of significant national and international contention. In the United States in particular, 'cybersecurity' has become a catch-all term that draws together disparate practices and actors. It involves a varied range of political and technical practices and is a field of shared concern for many different actors, each involved in defining and responding to matters where 'computer security' is thought to intersect with US homeland or national security (Nissenbaum, 2005), particularly in policy circles. Computer security has thus become the remit not just of individual or corporate practitioners but is increasingly a shared concern for a very wide range of people, organizations and technologies. As such, computer security has been layered with meaning and complexity over time, so that what is now widely referred to as 'cybersecurity' has come to represent a varied set of concerns. As modern industrialised societies are becoming more bound to, and reliant upon, networked technologies, so the relationship between critical infrastructures and the integrity of these networks are becoming ever more closely interwoven with ideas of societal continuity or resilience. 'Cybersecurity' has thus

come to signify a complex and emergent series of interactions and processes, meaning different things to different stakeholders at different times and places depending on their focus and orientation (Shires, 2019), with the further complication that state actors are not the only entities articulating its parameters as a matter of concern.

As this chapter – and the project as a whole – will seek to argue, such definitional differences also represent the coexistence of multiple and competing understandings of security rationales for security policy. Such dynamics are evident not just between states, but also in the state-oriented discourses and practices emerging around 'cybersecurity' within the US. Here, 'cyber' has come to represent a heterogenous set of concerns predicated on security in and through 'cyberspace.' Though the term 'cyberspace' started as a concept in popular culture (Saco, 1999; Valovic, 1999; Agre, 2002), it has accrued and transformed its cultural references through the ways that state actors (and society more widely) have constituted it over the years. Ubiquitous computing and widespread interconnected communications infrastructures have therefore led governments, and as the thesis will show, multiple agencies of the US government, to grapple with the tensions between the opportunities afforded by these technologies against the challenges they pose to established jurisdictions, symbolic boundaries and institutionalised practices, in the name of 'cybersecurity.'

As a precursor to developing its arguments in further depth in the proceeding chapters, this introductory chapter will proceed as follows. First, it will outline why it is important to recognise the contextual emergence of 'cybersecurity' as a term, where a brief discussion will highlight that though it has been a conspicuous focus for security actors in the US for nearly a quarter of a century, what counts as 'cybersecurity' or how it is practised by state actors is a matter of contestation on both procedural and political grounds. For the critical purposes of this project wishing to denaturalise technologically determinist state discourses, establishing that 'cybersecurity' is a dynamic and emergent phenomenon will begin to justify why static definitions do not suit its analysis. The chapter will then outline some key academic sources from the security studies literatures and beyond to outline the scholarly work that this project is building upon, but to also outline its unique contributions. By situating itself between critical security studies and Science and Technology Studies (STS), this thesis will seek to develop a framework to help security scholars avoid essentialising 'cybersecurity' as a state security matter. Drawing on these literatures, the thesis argues, enables us to draw out how and why these contests over 'cyber' matter politically and technologically, and to recognise the ways in which technologies, consequential categories, institutional responsibilities, political authority and national identity are also constituted and challenged in and through these debates. Outlining key aspects of relevant literatures, the chapter then outlines the research question that animates the project, so as to explain the rationale for the thesis' approach.

The argument in this thesis is that 'cybersecurity' is not overdetermined by strategic or technological imperatives, by the nature or essence of things: instead, it argues that the boundaries of 'cybersecurity' reflect the efforts of different entities (not just state agencies) to defend and extend their own organisational and symbolic boundaries. To this end, its chapters will set out how 'cybersecurity' is best approached as a culturally and temporally contingent concept that is both a source for and outcome of 'boundary work.' In adopting such a position, and engaging with extant theorisation of the concept of 'boundary work' within science and technology studies (Gieryn, 1983, 1999; Langley *et al.*, 2019), the thesis will focus on the boundary work of different actors involved in articulating cybersecurity discourses and how they may stabilise those efforts in initiatives that in turn construct and promote specific 'cybersecurity' imaginaries. As we shall see however, it is not simply the boundaries of 'cybersecurity' as a practice that are being variously contested, negotiated and constituted within US 'cybersecurity politics': in some important ways, efforts to 'bound' cybersecurity are also constitutive of broader symbolic boundaries, institutionalised distinctions and security imaginaries in those contexts, worked and re-worked in a recursive and iterative manner. The chapter will conclude by drawing out a key premise in this thesis that cybersecurity is emergent, a 'thing of boundaries,' as a potentially important counter to technologically or strategically determinist explanations of the risks and benefits of globally interconnected communications technologies.

1.1 What is cybersecurity?

'Cybersecurity', as indicated in the outline of this thesis' argument above, is emergent. By this I mean that cybersecurity is not an end-state but is a performative and complex set of processes, iterating and emerging through 'boundary work' – a point I shall return to shortly. It started as a matter primarily of interest to computer scientists and technical practitioners under the labels of computer and information security, which focussed on the confidentiality, integrity and availability of data (Andress, 2014). However, as daily societal processes have become more interwoven with and reliant upon ICTs, a much broader set of security concerns have emerged (Nissenbaum, 2005; Solms and Niekerk, 2013). Concerns about the technical vulnerabilities of information-based systems have meant that computer and information security have evolved from a focus three decades ago on technical access controls, to an entire infrastructure of technologies, organisations, policies, regulations and practices focusing on the security and functioning of networked ICTs and the societal processes that rely upon them (Denning, 2003).

In contemporary US discourses 'cybersecurity' is thus concerned with the vulnerabilities to the nation that emerge from reliance upon these networked technologies. Here, the internet and networked communication and computation technologies (or in contemporary US security policy

formulations, 'cyberspace'), are repeatedly being interpreted in terms of both its systemic vulnerabilities (threats *to* cyberspace and processes that rely on it) and the threats that come *from or through* cyberspace (Deibert and Rohozinski, 2010). Tensions between cyberspace's risks and opportunities were made explicit in a speech President Obama gave in May 2009 to mark the release of a comprehensive Cyberspace Policy Review that he had ordered to be undertaken at the start of his Presidency. The speech outlined his Administration's assessment of cyberspace and their statement of intent for the subsequent years. Declaring that this was a "transformational moment" in American history, he described "the great irony of our Information Age -- the very technologies that empower us to create and to build also empower those who would disrupt and destroy." The speech envisaged an expansive range of issues to be addressed through and by cybersecurity, encompassing anything reliant upon those networking computational technologies that had "become woven into every aspect of our lives" (Obama, 2009 n.p.). This concern, 'cybersecurity,' has gradually evolved out of (and informed) those imaginaries of technological and societal vulnerabilities.

Here, cyberspace and cybersecurity are ubiquitous, both in their presence in everyday processes and in the attention that they have been granted by the debates amongst state actors and policymakers in the US. Though the term 'cybersecurity' first appeared in 1989 (Merriam-Webster, 2020; Furber, 1989 cited in Stevens 2016), as a state concern its meaning and scope has gradually emerged and iterated in the thirty years since (Dunn Cavelty, 2007; Warner, 2012; Dunn Cavelty and Wenger, 2020). Over time, the terminology and definitions have changed from a focus on critical infrastructure resiliency outlined by President Clinton's Commission on Critical Infrastructure Protection (1998) to a more expansive matter of concern, incorporating security *from* cyberspace as Obama's speech above indicated. By 2018, the Trump Administration's National Cyber Strategy similarly described cyberspace as "an integral component of all facets of American life, including our economy and defense" (White House, 2018, p. i). This document would invoke the security of the internet as concerned with more than just its cables, routers, protocols and servers but a broader concern that "a secure cyberspace […] reflects our principles, protects our security, and promotes our prosperity" (White House, 2018: 1). Over time, 'cybersecurity' has thus been layered with culturally specific meanings and significance.

This conceptualisation of the empirical complexity of cyberspace, and ideas about the nation's existential reliance upon it, has meant that securing 'cyberspace' has been articulated as a 'whole-of-government' concern. Ten years after Obama's articulation of the scope of 'cybersecurity,' it was widely viewed as an all-encompassing matter for government agencies. This was underscored by a glossary definition of the term in 2019 by a programme intended to be the premier source of government-funded cybersecurity training across the nation. The 'National Initiative for Cybersecurity Careers and Studies' (NICCS) glossary thus defined 'cybersecurity' as the...

> …[s]trategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. (NICCS, 2019 n.p.)

This definition was designed to set the terms of the debate for the next generation of cybersecurity practitioners in the United States. Nearly every branch and mission of government was captured in this definition, and activities ranged in scope from the most granular level of technical and incident response to the most far-reaching level of international engagement and military strategies. The broad range of activities, actors and referents subsumed under official discussions of 'cybersecurity' thus give an impression of the breadth and scope claimed in the security of and operations in 'cyberspace.'

As the discussion has begun to draw out, then, the factors identified so far mean that determining what counts as 'cybersecurity,' and establishing the bounds of state responsibility in this matter, have become complex and all-encompassing concerns. As a result of the breadth of the concerns about cybersecurity's scope, the Congressional Research Service (CRS), in a report written in preparation for the new administration's term in 2016, advised that as "[a] broad and arguably somewhat fuzzy concept, cybersecurity can be a useful term but tends to defy precise definition" (Fischer, 2016, p. 1). The report went on to state that "[c]ybersecurity means different things to different stakeholders, often with little common agreement on meaning, implementation, and risks." (Fischer, 2016, p. 9). Despite cybersecurity's prominence in national security discourses, a primary source for congressional policy advice was here warning policymakers how contested the concept was in US policy settings.

Indeed, in trying to capture the range of activities that relate to 'cyber,' officials often cite a lack of conceptual clarity as a recurring feature and issue. In trying to delineate exact figures and programs for the 2015 Department of Defense (DoD) budget, for example DoD Comptroller Bob Hale explained, "[w]e tried to capture it all, but I'd say there's a gray area here in what counts as cyber" (cited in Corrin, 2014). Analytically and politically, this 'gray area' extends to how to define 'cyber' activities across classified and unclassified programs and across agency jurisdictions. One academic commentator suggested the problem was more profound than the lack of common agreement cited by the CRS, writing:

> …we've been experiencing cyber creep for years, letting the term grow and extend its tentacles until it is so vast, encompasses so much, *that it is virtually meaningless and absolutely impossible to avoid*. (Wolff, 2016 n.p., emphasis added)

Seemingly in tandem with the ever-increasing ubiquity of the term, this 'cyber creep' did more than exceed the remit of any one department, agency or entity as the NICCS glossary definition offered earlier would suggest. Working out the bounds of legitimate state (security) action in cyberspace is thus complicated too in the way the terms have also "grown" in scope and become, at least in the view of some, "virtually meaningless." Retired General Michael Hayden, former director of the Central Intelligence Agency (CIA) and NSA, who in the same article had endorsed the concept of cyberspace as a military 'domain' as being an intuitive framework would go on to observe:

> …as I witness and participate in discussions about the future of things "cyber" […] rarely has something been so important and so talked about with less clarity and less apparent understanding than this phenomenon. (Hayden, 2011, p. 3)

As the later chapters will draw out in more detail, struggles over common definitions of cyberspace and cybersecurity present more than conceptual ambiguity but are evidence of the interests and power involved in articulating cybersecurity as an object.

Cybersecurity is thus a matter of complexity, both practically in policy and discourse, and methodologically as a matter of analysis. In the discourses related to matters of 'cyber,' this is exemplified in the range of metaphors and analogies variously used by policymakers, security actors and congressional witnesses to describe cybersecurity or cyber variously as: "a complex issue," "a journey… a race with no finish line" (Starkey, in US Senate, 2014a, p. 29); "sort of an evil layer cake" (Comey, in US Senate, 2013d, p. 16); and "the new frontier," "a new terrain for warfare" and "a battlefield of the future" (Panetta, 2012 n.p.). Each of these framings come from different institutional perspectives and are likely to be products of their political agendas as much as their organisational cultures. The first, congressional testimony from the chief security officer for the State of Delaware, was explaining from a technical practitioner's standpoint for the utility (but practical difficulties) of ongoing public private partnerships. The 'evil layer cake' was how Director of the Federal Bureau of Investigation (FBI) James Comey described to Congress the agency's difficulties in addressing the broad range of threats and risks in cyberspace whilst also protecting civil liberties. Secretary Panetta's remarks meanwhile were an articulation typical of the Department of Defense's conceptualisation of the operating environment to tell business leaders in New York that the military was addressing their concerns about threats to intellectual property and network security. However, each of these framings is also indicative of a more profound variation across different communities of practice about what counts as this matter of 'cybersecurity.' Here, different conceptions of the matter at hand, and what needs doing about 'it,' both coexist and compete.

Adding additional "layers" of complexity, as alluded to in some of the quotes above, is the fact that the ways that these networked communication technologies are increasingly integrated into

everyday societal processes is changing and iterating with each passing day. These networked communication technologies are made up of a vast and interconnected topology of software, hardware and protocols. When communications and networking technologies become so closely coupled and integrated with so much of a nation's daily processes, then it is inevitable that they should produce unexpected and unintended consequences (Wynne, 1988). The interactions between new software and hardware, between new installations and old legacy systems, generates unforeseen (and often unforeseeable) technical glitches, vulnerabilities and failures that arise as the result of the 'vicissitudes of execution' (Chun, 2008). However, concerned with more than just technical glitches, we have already seen in this short introductory section how cybersecurity discourses are "shot through with commercial, military and political anxieties" (Jones-Imhotep, 2017, p. 18). As the discussion so far has begun to indicate, because the tightly coupled and complex systems of networked ICTs are so far-reaching and often function in registers that are beyond human cognition, people have developed a whole series of metaphors or analogies to parse these processes, drawing on shared cultural and social resources to make sense of them.

Navigating the tensions between the threats, risks and benefits afforded by networked communications and computational technologies has created pressure for policy responses from state agencies, which has manifested in and through these cybersecurity discourses. While the term 'cybersecurity' has been a conspicuous feature of state discourses in the US for at least two decades therefore (Dunn Cavelty, 2007; Warner, 2012; Stevens, 2016), in important ways it defies neat substantive definition. This is, arguably, a symptom of the range of different actors and interests involved in negotiating their respective agendas, whilst also reflecting the evident empirical complexity of the technologies, organisations and practices involved. As the 2009 Cyberspace Policy Review described these competing tensions, "[t]he United States faces the dual challenge of maintaining an environment that promotes innovation, open interconnectivity, economic prosperity, free trade, and freedom while also ensuring public safety, security, civil liberties, and privacy." (White House, 2009, p. 13). 'Cybersecurity,' viewed through an analytical lens, might thus be regarded as a site of techno-political (Hecht and Edwards, 2007; Hecht, 2009) negotiations and contestation over these tensions, as well as the position and legitimacy of the actors articulating these narratives.

Despite its ubiquity in policy documents and US doctrine then, as we shall see through this thesis, what counts as 'cybersecurity' and the boundaries of state responsibility in this matter are still being negotiated and worked out. The shape and form that those negotiations take is also not necessarily as predetermined by material or strategic conditions as the discourses frequently suggest. Later chapters will demonstrate in more detail how a closer look at uses of cybersecurity and the 'cyber' prefix reveal subtle and important distinctions in and within their usages, with important ramifications for the kinds of political responses and possibilities that subsequently emerge. As the

thesis will bear out, 'cyberspace' is not the only thing that has shaped 'cybersecurity' discourses and policies, and the state does not hold a monopoly of their definitions. Many other factors play a role in articulating 'cybersecurity' as a matter of concern: contestation over what counts as 'security' and for whom and what; what laws apply; who claims responsibility; which agency already has resources; institutional mindsets and cultures. As we shall see, all of these things and more have played a part in producing 'cybersecurity' as an institutionalised response to the risks associated with networked communications and computation. First though, the chapter will draw out the parallels and insights already available in the security studies literatures and beyond, as well as situate its contribution there.

1.2 Cybersecurity in the security studies literatures and beyond.

The following section will show why it is important to study the inherent contestability of 'cybersecurity' instead of "distorting it into clarity' (Law, 2004, p. 1) through analysis or method. As referred to above, some academic and policy actors have suggested that the term is so elastic as to be meaningless. However, the term 'cybersecurity' is undeniably a feature of these discourses and debates and has become institutionalised through material-discursive arrangements. Rather than trying to explain this diversity away, the thesis will instead make this apparent 'elasticity' and instances of diversity and contestation the crux of its focus. After all, 'cybersecurity' and its associated concerns have emerged and changed over time, and static definitions do not suit dynamic or emergent phenomena.

There have been many studies that have referenced or cited the lack of conceptual clarity or expansive definitions of cyberspace and cybersecurity. In this first grouping of the literature, academics have recognised the contestability of cyberspace, or the difficulty in pinning down the resultant cybersecurity practices that stem from such definitions. As Ebert and Maurer (2013, p. 1058) wrote, "[d]efinitions of cyberspace are disputed both analytically and politically" while Joseph Nye Jr. reflected that "[t]here are dozens of definitions of cyberspace" (2011: p.122). In a RAND Corporation report also concerned with defining the boundaries of cyberspace (appropriately entitled *Redefining Information Warfare Boundaries for an Army in a Wireless World*), Porche et al. (2013, p. 6) suggested that the many attempts to define cyberspace are a reflection of "[m]ultiple interpretations" of the same entity.

Likewise, Futter (2018) has more recently argued that 'cyber' has become a buzzword that has lost all meaning in its wide-ranging use and lack of conceptual precision. For Rid and Lee (2014), the 'cyber' prefix hampers effective policy because it has been used for political and financial gain by various public and private actors in both security and non-security sectors. Similarly, Betz and Stevens

cite a policymaker who complained that the wider, broader, more inclusive the definition of cyberspace that cybersecurity is concerned with, "the harder it will be to identify what policy is, or should be, surrounding cyberspace" (Betz and Stevens, 2013, p. 148). They suggest that "there is little consensus on the meanings of 'cyber security' and 'cyberspace,' despite attempts to develop common vocabularies" (2013, p. 148), and their article contends that the problem of conceptual clarity undermines the ability of actors in the field (e.g. policymakers and practitioners) to communicate more 'effectively' or efficiently.

However, mirroring the framing of the problem in policy and security circles, a great deal of academic literature tries to 'fix' the terms with substantive definitions. These sources, or the policymakers they are citing, are indicative of a tendency towards substantive views of cyberspace technologies (Feenberg, 2002, p. 5): their arguments are predicated on an assumption of an external and definable technological entity, which just requires more clarity in definition. In mainstream work on cybersecurity, it is largely viewed as a technical formulation, largely absent any cultural or social processes and contexts. These approaches tend to focus on understanding the world from the agents' points of view, but instead this project is examining the structures of meaning that make social actors' perspectives possible and actionable. Technical and instrumental readings of cybersecurity such as those found in policy discourses thus arguably tend to neutralise or discount the material conditions and thick social environments that technologies operate within and by which they are made meaningful (Sassen, 2002).

Other sources have grappled with this breadth of possible definitions of 'cybersecurity' in cybersecurity research and policy by proposing frameworks to create some analytical clarity. An example of this kind of analytically clarifying scholarship is James Shires' (2019) article that seeks to categorise 'cybersecurity' according to three common conceptions, depending on the levels of analysis and focus that policymakers, practitioners and academics employ when referring to the term. Here, he identifies 'national cybersecurity,' with its focus on the functioning of territorially-bound networks and infrastructures as its referent, and criminals and other state actors its threat actors; 'commercial cybersecurity' with its focus on the networks of profit-making entities, and malicious actors taken as any that affect the purpose and functions of the organisation, usually in financial terms; and finally, 'individual cybersecurity' where the devices to be protected are those of the individual, and encompasses privacy rights and communications security (Shires, 2019).

While there is obvious analytical utility for taking some units of analysis as the basis for research, typologies like those outlined above routinely overlook (or seek to impose some analytical order upon) the underlying political processes of contestation and formulation that have gone into the production of cybersecurity discourses and practices without questioning how and why they came

to be articulated as such by state actors. To lesser or greater extents, they either seek to impose static definitions upon dynamic and emergent sociotechnical processes, or alternatively reify the securitising discourses as expressed by state agencies, military actors and commercial interests.

By contrast, this project aims to draw out the political implications of these contests for the state and society's relations with cyberspace by acknowledging the *productive role* of ongoing debates and competing articulations in constituting 'cybersecurity' in the context of US national security. In other words, how we define cybersecurity, decides how we deal with it. Rather than positing a technologically determinist understanding of the technologies of cyberspace, it will emphasise the political structuring of the social world emerging around and through those technologies (Edwards, 1996). Given the centrality of technologies to articulations of 'cybersecurity' as a matter of concern, this highlights the need for an approach that can recognise the constitutive role of technologies beyond giving them an essentialised or deterministic character. As the chapter has already begun to draw out, cybersecurity is at once a technical and cultural formulation, with important consequences for the political possibilities that arise as a result.

Rather than trying to offer a settled definition of what 'cybersecurity' is as it relates to any external or objective reality, this thesis is concerned with the work that this term *does* for those involved in articulating cyberspace as a site of state security and military interventions. Rather than starting out as clearly defined and practiced objects of state governance, 'cybersecurity' and 'cyberspace' have each emerged and iterated contemporaneously over time. Recent glossary definitions notwithstanding, 'cybersecurity' did not start out as a given or clearly defined set of state processes and practices, and efforts to bound 'cybersecurity' have played an important part in setting the parameters (and limits) of the matter of state concern too. Without a recognition of the contingent processes at work, these official narratives and analyses of them in the security literatures may have determinist consequences, not least a naturalisation of definitions of security that favour the state or an apparent inevitability of discourses that frame cyberspace as a warfighting 'domain' for example.

Critical and constructivist analyses of 'cybersecurity' in the security studies literature also draw attention to the lack of conceptual or terminological clarity in cybersecurity discourses, but from a different set of epistemological commitments to some of those outlined so far. Rather than viewing cyberspace and its technologies in substantivist terms, as 'things' with largely determinist effects on society and policy (Kello, 2013; Buchanan, 2016), they have instead picked out the ongoing and iterative processes of the mutual construction of cyberspace and ideas of insecurity. This second grouping of approaches in the literature offers invaluable insights and have brought a concern with cybersecurity into the critical limelight. Their observations about the 'constructedness' of

cybersecurity have a good deal of critical utility in helping to counter determinist narratives about societies' relations with technologies.

One of the earliest articles to take a critical lens to cybersecurity identified that imprecise or contested definitions of cyber belie a split between policy-speak and technical-speak (Nissenbaum, 2005). As one of the formative articles to draw attention to the previously undertheorized consequences of linking 'computer security' and 'national security' from a securitization perspective, Nissenbaum here drew out how two different and overlapping conceptions were at work in this context. Those in the technical community of computer and information security tend to focus on individual systems and networks, while the 'cyber security' discourse focuses on collective and institutional systems. Because of its focus on technologies, these conceptions of 'security' are primarily treated as technical problems, though the article importantly underscores how 'security' is a contested, variable, nuanced and contextual concept, with its varying shades of specialised and cultural meanings (Nissenbaum, 2005). This is an important point in the context of this thesis' later findings, highlighting that not only is the referent object in these conceptions different, but so too are the conceptions of 'security,' with implications for the kinds of political and technical responses that emerge in response.

Conceptualising cyber threats as as-yet-unfulfilled risks that require acts of representation to make meaningful, Myriam Dunn Cavelty (2007, 2013; Brunner and Dunn Cavelty, 2009) has contributed important work in drawing out "what hyphenating 'security' with 'cyber' might imply" (Hansen and Nissenbaum, 2009, p. 1156). Rather than try to dismantle the hyperbolic aspects of cyber threats as though to reach a more accurate underlying reading of some external threat, she seeks to analyse the political mechanisms of threat construction, suggesting that "the imprecision of the vocabulary — which is simultaneously expressive and constitutive of the cyber-threats debate — has a significant impact on the political process." (Dunn Cavelty, 2007, p. 14). This tallies with the work of Tim Stevens (2016), who has drawn attention to the ways that cybersecurity is "elastic in definition and elusive in practice" (Stevens, 2016, p. 23) in its tendency to capture any process interconnected by digital technologies. Stevens also crucially emphasises the importance of recognising the historical context of the relationships between information technology and security and the importance of situating emerging cybersecurity discourses and practices in specific socio-historical contexts (2016, p. 3).

This critical eye upon the intersubjective and 'constructed' nature of cybersecurity and its associated concepts has a great deal of critical utility for this project as a way of capturing the interplay of social and material processes. As Barnard-Wills and Ashenden (2012) point to in their construal of cyberspace as a construction in two senses, it is a physical construction of networked information

technologies, and a social construction shaped by the way that people enact the space to manifest a system of social relations. Similarly, Simon and de Goede (2015, p. 6) argue for the importance of thinking about cybersecurity in terms of its ‘‘ongoing production and intertwining of material and immaterial relations and forces rather than an object or end product” as a way to denaturalise the reification of ‘cyberspace’ as a fifth ‘domain’ of warfare in the mainstream policy discourses. Capturing these ongoing processes of intertwined material and social relations has led scholars such as Collier (2018) to advocate for ‘assemblage’ thinking as “a framework for understanding the dynamic and contested nature of security provision” given the eclectic range of actors and materials involved in producing this thing called ‘cybersecurity.’ This builds on the earlier work of Stevens (2016) who argued for the analytical benefits of viewing “the cyber security assemblage of material and immaterial entities” not as something “static but a web of social and material actors that requires constant negotiation and performance**”** (2016, p. 33)**.**

Even while critical approaches have addressed how definitions of ‘cybersecurity’ are contested and formulated, less has been said about the productive role that these contests and political processes of sense-making in turn play in formulating and producing ‘cybersecurity’ and versions of cyberspace. Shires and Smeets (2017) come closest by identifying that competing definitions of cybersecurity are the result of underlying contest to define cyberspace. Yet, more than just competing or contested definitions, as the next chapter and the thesis as a whole will bear out, ‘boundary work’ is a productive element in social actors’ efforts to make sense of and impose order on this ontologically and analytically ‘messy’ object of ‘cybersecurity.’ As the next chapter will outline in more detail, rather than utilising the concept of the ‘assemblage,’ the proposed framework will utilise and build upon Stevens’ and others’ formative analysis to instead demonstrate how ‘boundary work’ can be thought of as one of the key mechanisms and processes they identify in constituting cybersecurity imaginaries. Accordingly, this project will develop an analytical framework of ‘boundary work’ (outlined in Chapter Two) as the means of recognising these processes of contention and meaning making.

Related to this conception of cybersecurity as a contested and manifold set of practices and concepts, there are also some fundamental questions about what security is in this context, who it is for, and who is responsible for providing it. In this vein, and of particular relevance for this thesis, Jordan Branch has advanced an innovative argument for conceptualising the role of ‘cyberspace’ as a “foundational metaphor” to explain the shaping and constitutive effect the term has had in US security discourses (Branch, 2020). More than simply “a catchy word,” Branch’s analysis of US security policy and military doctrine demonstrates the foundational role that the term has had in conceptualising and orienting the political and security actions pursued by the US government “to manage cybersecurity threats” (Branch, 2020, p. 7). While this study undoubtedly has useful parallels with this thesis given

his insight that, at key moments, "bureaucratic competition over cybersecurity has been shaped by this language—probabilistically, not deterministically" to the point that cyberspace-as-domain terminology helped certain military arguments over others (Branch, 2020, p. 13), his article takes 'cybersecurity' as a finalised set of state security concerns synonymous with 'cyber defence' as an increasingly military focus. To a certain extent, this also naturalises a reading that the concern with 'cyberspace' has produced a natural focus for state actors in the form of (military) 'cybersecurity' policies and discourses, without attending to the full range of actors and interests involved in these bureaucratic struggles that take place *beyond the military's* interests. His empirical evidence base, though very like those utilised within this thesis, have led him to different conclusions as to the importance and shape of other 'bureaucratic wrangling' by state agencies and non-governmental actors too.

Instead, a key finding of this thesis is that while the military's interests and organisational heft have undoubtedly dominated these contests for resources, other actors and 'things' have also played a constitutive part in shaping the US government's policies and practices. Branch's focus on rhetoric and bureaucratic argument in formulating cyberspace as a matter of state concern is invaluable in beginning to capture some of the ongoing political processes, but it does not account for the distinctive ways that technologies, organisational cultures, and institutional arrangements also have a way of 'pushing back' against the rhetorical efforts and political interests of those involved in articulating 'cyberspace' as a site of state security interventions.

As discussed in detail in later chapters of the thesis, US' policies and discourses have not been determined by this metaphor alone, but a whole host of other political, technical, institutional and organisational factors. In distinction to Branch's article then, rather than seeing 'cyberspace' as supporting specific institutional responses in a unidirectional, if probabilistic sense (which in part it has), the thesis will show how 'cyberspace' and 'cybersecurity' have emerged and iterated together, layered with meanings over time, co-produced in relation to a number of other culturally and politically distinct factors including symbolic boundaries, conceptual categories and organisational distinctions.

Building upon but also diverging from the valuable analysis in the security studies literature discussed thus far, I propose to take the analytical and substantive complexity as the starting point for the research. We cannot just dismiss 'cybersecurity' for being difficult or complex: both cyberspace and cybersecurity are taken as real by those actors involved in articulating their effects, policies and agency responsibilities. At the same time, these conceptions of the matters at hand, and ensuing actions by state actors, are affecting the course of these technologies' development and their effects. So how do we capture political and constitutive processes of 'cyberspace' and 'cybersecurity,' without

simply reducing these processes to acts of representation and rhetorical construction on the one hand, or technological determinism on the other? In short, we need a way of studying them that can appreciate the ongoing processes of social construction and recursive feedback between 'cyberspace' and 'society.' In response to this question the chapter will now turn to the role of imaginaries and technologies, and the utility of insights from the STS literatures.

1.3 Technologies, culture, security imaginaries.

As some of the previous discussion showed, policymakers complain about a lack of conceptual clarity, or clearly defined 'boundaries,' for what counts as 'cyber' or cyberspace; citing a need for clearer and more substantive definitions. Policymakers and security actors in the US seek technical fixes to what they see as largely technological problems, with the result that the official discourses surrounding cybersecurity tend to essentialise and also instrumentalise cyber technologies, identifying threats without recognising the ambivalences and contingencies of their technical affordances. Such calls for more precise, or more 'accurate' definitions of cyberspace's essential characteristics are entreated by policymakers and security actors to better 'fix' the problems posed by cyberspace. However, without a recognition of the contingent social processes at work, these official narratives may have determinist consequences on the policies that follow.

Given the ubiquity and integration of 'cybersecurity' with associated ideas of societal values and resilience, we need an approach that can integrate the material, social and cultural landscape into any analysis of its construction and enactment. As studies in the STS literature have convincingly demonstrated, technology "embeds and is embedded in social practices, identities, norms, conventions, discourses, instruments and institutions – in short, all the building blocks of what we term the social." (Jasanoff, 2015, p. 5). Materiality is a key element of cybersecurity discourses and it would be remiss to overlook this: materiality is not just socially or discursively constructed but has a very real constraining or enabling effect (Aradau, 2010, p. 182). Like the long tradition in STS that conceptualises objects as actors (Law, 1992; Latour, 2000, 2005b; Law and Singleton, 2005)[1], such an analysis can therefore show where materiality is *making a difference* (Austin, 2017). Simultaneously, as Markham (2003, p. 1) has underscored, the conscious (and unconscious) discursive framings used to talk about the internet and communication technologies "have actual and meaningful consequences on the shape and perception of these technologies" – as these discursive frames and

[1] Drawing on this STS approach to materiality for example, Graham and Thrift (2007, p. 3) have argued that ""things are not just formed matter, they are transductions with many conditions of possibility and their own forms of intentionality" while for Preda, things and artifacts "need to be seen as social entities that play an active part in the generation, stabilization and reproduction of social order and sociality" (Preda, 1999, p. 349).

metaphors of cyberspace become more embedded and taken for granted, "alternatives are shut out, cut off and left behind." We need an analytical approach that can therefore incorporate these various constituents.

We can better understand the contestations involved in producing 'cybersecurity' once we recognise and draw out the cultural and political shape of the vulnerabilities in question. 'Cybersecurity' represents wider "technological anxieties around impermanence, instability and failure" (Jones-Imhotep, 2017, p. 213), anxieties which in turn produce their own infrastructures and institutional arrangements in a co-constitutive manner. This is not a kind of technological politics that is concerned with the intended effects and designed outcomes of the technologies (MacKenzie, 1993; Hecht, 2009; Bijker et al 2012). Instead, actors are navigating the emergent properties of complex systems, their entropies and "tendencies toward disorder, degradation, breakdown, surprise, even calamity." (Jones-Imhotep, 2017, p. 12).

This thesis will examine the premise that such anxieties are reflective – and constitutive – of visions of desirable futures. These are bound up with what Pretorius describes as a security imaginary, as "that part of the social imaginary that deals with the understanding of the security world and in turn makes security practices possible." (Pretorius, 2008). This has useful parallels to Jasanoff and Kim's work on sociotechnical imaginaries (2015). To paraphrase and repurpose one of their observations, 'cybersecurity' appears to represent "culturally specific collectively held and performed" resistance against undesirable visions of the future, "animated by shared understandings of forms of social life and social order attainable through, and supportive of, advances in science and technology." (Jasanoff and Kim, 2015, p. 22). Cybersecurity politics are thus simultaneously based upon, draw upon, and constitutive of these 'shared understandings' and stabilised or materialised by different technical programs and institutional responses.

As we shall see throughout the later chapters, symbolic boundaries also provide the conceptual tools and 'shared understandings' that groups use to compete over the production, diffusion and institutionalisation of different narratives and principles in their social relations. There are some key boundaries and "codes of intelligibility" (Weldes, 1999) around which the narratives about cyberspace have coalesced, but these boundaries, and the boundaries of 'cybersecurity' as a matter of state concern are also constituted in the process. Importantly, moreover, security imaginaries are enabled or constrained by the already constructed social world, such as particularly evocative discourses of boundaries, powerful organizations (Kinchy and Kleinman, 2003), and what this thesis will call cybersecurity imaginaries. Stevens has suggested that 'cybersecurity imaginaries' both reference and constitute the expectations of communities and can offer a useful analytical heuristic (Stevens, 2016). This project will therefore draw out in more detail how cybersecurity

imaginaries of the networked nation shape and produce cybersecurity as a thing of boundaries specifically in the cultural context of the United States.

Such an approach can therefore work to draw out the specific ways in which discourses, imaginaries and technologies co-constitute each other, all of which is encompassed in what this thesis refers to as 'cybersecurity politics.' As part of the project's efforts to critically assess the claims in military, strategic and security discourses that cyberspace or cybersecurity 'blurs' categorical and symbolic boundaries, this is a conceptualisation that sees technology and culture as mutually interdependent and dialectical (Wyn Jones, 2000, p. 142). As the next chapter will show, this offers some productive parallels to how this project mobilises the concept of boundary work, with all its culturally specific reference points. Rather than a focus only on speech acts and practice, the analysis means to provide a richer account, one that includes the role that materiality and technologies have played in constituting the boundaries and discourses of cybersecurity politics.

The benefits of this approach flow in both directions: Kim and Jasanoff (2009, p. 120) have highlighted that STS research tends to focus on scientific and technological innovation rather than trying to understand more complex relations among knowledge, its applications and power. This is a sentiment echoed by Barry (2001) when citing the shallow conceptions of politics characterised by STS work stemming from the focus that such research often has on labs and particular technologies. As this project will draw out, when the emergence of the concept of 'cybersecurity' is understood as a development that is in progress, one that requires narration and maintenance by those involved, then the analysis in this thesis will have valuable insights to offer both security studies and the STS scholarship. In the time that this thesis has been researched and written, there has been a growing recognition of the benefits that STS frameworks can offer to critical security studies (Barry, 2013; Mayer and Acuto, 2015; Dunn Cavelty, 2018; Stevens, 2018; de Goede, 2020), and as Chapter Two will outline in more detail, this thesis will seek to contribute to this ongoing dialogue. Furthermore, the approach outlined in this project seeks to offer analytical insights for those STS scholars investigating how 'security' is produced too (Orsini et al 2017; Bellanova et al 2020; Evans et al 2020).

In sum then, a key premise for what follows is that 'cybersecurity' is not a static set of discourses and practices but references a multifarious range of technologies, processes and practices, and complex socio-technical arrangements coagulating around and performing this concern. It is also a set of discourses and practices that are contested, both conceptually and politically. The next section will now articulate the research questions that animate this project. By developing a framework that can move beyond determinist or substantivist technological explanations, this framework will also capture the contingent social processes that are going into making these technologies meaningful.

This is so that the thesis can critically examine some of the iterative processes that have been involved in constituting 'cybersecurity.'

1.4 Research Questions

'Cybersecurity' represents a multifarious range of technologies, discourses and practices oriented around security in and through cyberspace and is the touchstone for a great deal of conceptual and political debates. It is not simply a case of the state acting as the security provider or conversely, about accounting for the privatisation of security provision. There is a more convoluted process of legitimation going on in cybersecurity discourses where the responsibilities are dispersed and the boundaries that have constituted many social theories, such as boundaries between public and private jurisdiction, are being mobilised or reconfigured.

The central research question animating this thesis will therefore ask:

To what extent and in what ways are boundaries reconstituted in and by US cybersecurity politics?

The argument in each of the chapters that follow is that the boundaries of 'cybersecurity' reflect the efforts of different entities (not just state agencies) to defend and extend their own organisational and symbolic boundaries. This in turn leads to the overall argument of the thesis that at key moments, 'cybersecurity politics' are symptomatic of efforts of diverse actors to make sense of, but also produce the state's roles and responsibilities in cyberspace and, in turn, to make 'cybersecurity' and 'cyberspace' governable and amenable to the 'classical responsibilities' of the state. As we shall see, these efforts are contested and fraught, and variously draw upon but also reconstitute culturally significant categorical, symbolic, organisational and institutional boundaries. Though by no means exhaustive, the articulation of such boundaries will serve as some of the key moments that each of the empirical chapters later focus on. A key premise animating these chapters is that 'cybersecurity' is therefore emergent as an epiphenomenon of 'boundary work.' Furthermore, 'cybersecurity,' constituted as it is by boundary work, thus emerges as a cultural product of these conceptions of vulnerability, whilst also shaping conceptions of both vulnerability and culturally significant boundaries. The thesis concludes that what 'cybersecurity' *is*, how its boundaries are drawn, depends on the pragmatic utility of any given borders or boundaries for the protection, expansion or denial of political authority and resources.

This argument matters because it will show how efforts at bounding the parameters of 'cybersecurity' are more than simply rhetorical. They are (becoming) institutionalised, enacted and materialised. Later chapters will illustrate how, by becoming so widespread in US security discourses, the different ways of 'bounding' cyberspace implicitly direct: the employment and development of

particular technologies; the viability of certain policies; developmental priorities; and the interplay of social and technical and institutional arrangements that arise as a result. Military actors describing cyberspace advocate for its institutionalisation as a warfighting domain, for example, while Homeland Security actors contest this formulation instead conceiving of cyberspace primarily as an 'ecosystem' and an 'environment.' Each of the empirical chapters will show how efforts to bound cybersecurity are also efforts to contest or defend the boundaries that define those organisations. Rather than being determined by the spatial connotations of the term, different institutional arrangements have evolved at the point of these competing articulations of 'cyber' and 'security,' sometimes successfully and sometimes unsuccessfully. Instead of taking either term as naturalised and uncontested, uses of the terms 'cybersecurity' and 'cyberspace' have iterated and emerged over time and government actors did not (and could not have) sat down and conclusively defined them from the outset. Instead, their meanings and practices have emerged over time, with the result that state efforts to define either term no longer appear so definitive.

Rather than trying to provide a substantive definition of cyberspace or cybersecurity, this thesis thus shows the ongoing processes of bureaucratic, political and technical wrangling that have gone into producing this institutional response to networked communications and computation. This is important because it was not a foregone conclusion that the technologies would determine the form of these national political and technical responses. This thesis will therefore provide the first wide-ranging empirical account of the cybersecurity politics and bureaucratic contestation amongst US federal agencies and institutions, and their interactions with actors and technologies beyond those agencies, to show how all sorts of other (understudied) factors have constituted 'cybersecurity' beyond the metaphorical content of the language of 'cyberspace.' The thesis finds that though the DoD have wielded oversized influence in US cybersecurity politics, there have been some historically resonant boundaries and cultural codes of intelligibility that they have not (yet) been able to reconfigure. The thesis posits that some boundaries (symbolic, institutionalised) have a resonance or resilience in American social and security imaginaries that have (yet) to be reconstituted in or by cybersecurity politics, even while other boundaries have been reconfigured through boundary work.

The later chapters will draw out how multiple (cyber) security imaginaries act as important cultural references in cybersecurity politics. They act as a shorthand for, and invoke, both a way of life as well as signifying a source of profound vulnerability. Indeed a long tradition of historical and sociological studies of technology have underscored how technologies and their vulnerabilities "are thoroughly cultural, and that we can only understand our modern high-tech society by recognising how its dominant cultural values and its technologies shape each other." (Bijker, 2006, p. 62). Cybersecurity politics are therefore simultaneously animated by, draw upon, and concerned with producing, this idea of an American national 'self.' References to such imaginaries act like a collective

story that actors tell themselves to make sense of the past, present and future. Readings of technological anxieties are getting 'written into' the initiatives discussed in each of the chapters. The thesis and introductory chapter are not evaluating whether or not these narratives about existential threats to American ways of life are objectively true, or whether they are entirely hype, or 'merely' strategic or instrumental political communications. What is important, and what animates this thesis, is the ways that most of these actors appear to believe that these narratives are true, that they 'make sense' amongst them, and therefore animate and contextualises their boundary work and initiatives.

This thesis is therefore about the *politics* of cybersecurity, rather than treating security as a concern that takes place above politics (Hagmann, et al. 2019). What follows is a detailed account of the politics and politicization of (cyber) security understood as being "controversially debated in a public arena, without foregone conclusions as to how they are going to be handled," as Dunn Cavelty and Leese (2019, p. 50) put it. As they go on to point out, this feature has received decidedly less attention in the security political literature than securitization and technification. While the project of critical security studies has a strong history of analysing and deconstructing the security complexes of the liberal state, it has often had a limited engagement – conceptually, disciplinarily, and practically – with questions of security policy and how to capture those emergent processes such as those outlined so far in the discussion of cybersecurity. A recent renewal of research interest into security politics is helpful in this regard (Hagmann et al, 2019; Neal, 2019; Dunn Cavelty and Wenger, 2020). In the context of US cybersecurity, official efforts of definition and negotiation are not restricted to arenas of high politics, or formal and public settings: as the chapter outlined earlier, cybersecurity debates are characterised by a wide range of state and non-state actors involved in defining the bounds of state action in cybersecurity, each involved in shaping 'the truth' about certain threats and security (Huysmans, 2006, 2011; Leander, 2008). It is important to study these political efforts, because these debates also have real-world effects in constituting specific material and discursive arrangements.

Throughout this thesis, what I will call 'cybersecurity politics' in the United States can be understood as an arena of contestation and antagonism between competing articulations of the problems that the state is thought to face in managing its relationship with 'cyberspace.' 'Politics' in this sense refers to the intersubjective efforts of people to make sense of change-processes in the world, which play a constitutive part of efforts that go into the making of social realities. Here, 'cybersecurity politics' are not just rhetorical and discursive efforts to build support for preferred courses of action in 'formal' arenas or places of politics, such as Congressional hearings and judicial processes, but also capture the assembly and mobilisation by social actors of heterogenous elements of people and technologies towards concrete ends (Jasanoff and Kim, 2015; Jones-Imhotep, 2017). Unlike many approaches to the topic outlined in the literature review above that focus on the politics of dominant or powerful actors, such a conceptualisation of cybersecurity politics can thus pay critical

attention to voices of practitioners and privacy advocates and companies and lawyers and non-government actors too, both consenting and dissenting of official state agency imaginaries. Such an analysis is also attentive to the roles that boundaries, technologies and broader security imaginaries also play in constituting cybersecurity.

It is my contention that a focus on the political *processes* involved in demarcating cybersecurity (discussed in more detail in Chapter Two) can grant the researcher important insights into the political and cultural assumptions animating this context. The extent to which cybersecurity touches so many peoples' lives underscores the importance of challenging deterministic accounts of technology's relations in and through society. Looking at cybersecurity through the lens of boundary work can grant security scholars new interpretive insights, whilst also shedding analytic light on the interests and political economy at work in cybersecurity imaginaries. Throughout the later chapters the thesis will thus ask how 'cybersecurity' is constituted, and by critically examining to what extent boundaries are reconstituted in and by 'cybersecurity politics,' it will ask what difference it is making. To make these arguments, the thesis will be structured as follows.

1.5 Thesis structure

Chapter Two will lay out the theoretical framework and outline the methodology for demonstrating these arguments. Cybersecurity is said to challenge a number of long-held consequential distinctions, and because it encapsulates such a broad range of actors and activities, the efforts to 'fix' its boundaries and associated processes of meaning-making are captured and denoted here by the concept of 'boundary work.' Political actors, both governmental and those non-governmental actors with whom they interact, undertake strategic as well as unconscious categorisation work to make sense of the world around them and their role in matters of (state) cybersecurity. Important scholarly work has looked at how boundary work informs the development of national identities and material boundaries of the nation (Anderson, 2006; Mayrl and Quinn, 2016), but security studies have, for the most part, not yet engaged with this work. Outlining such an approach is one of the main contributions that this project seeks to make.

Drawing on the concept of 'boundary work' from the STS literature (Gieryn, 1983, 1999; Jasanoff, 1987; Kinchy and Kleinman, 2003; Langley *et al.*, 2019), Chapter Two will begin to draw out the importance of making a closer examination at the ostensibly apolitical management of these technical issues. Following Langley et al (2019, p. 706), boundary work is defined as "*purposeful individual and collective effort to influence the social, symbolic, material and temporal boundaries, demarcations and distinctions affecting groups and organizations*." The utility of this definition is that it offers a relational or processual and constructivist account of boundaries as continually becoming

and fluctuating, subject to human agency and configurations of materiality (Langley and Tsoukas, 2017). This is also a form of analysis that can account for the ways that the cybersecurity discourse is rooted in and intertwined with material elements and technical instruments (Mayer et al. 2014). Technologies (and their vulnerabilities) do not present themselves to us in unmediated ways. As a set of practices and discourses, it requires work on the part of those who articulate cybersecurity and technological vulnerability to solidify them as a 'matter of concern' (Latour, 2005a).

'Cybersecurity' is thus a work in progress, constantly emerging and iterating as a set of practices and discourses. Part of cybersecurity's concerns are shaped and produced by material and technological 'possibilities' too. There is an important sense in which the practical and discursive efforts of actors are predicated on the affordances of the technologies involved. While the 'technological anxieties' are referenced and produced in culturally bound ways, they also reference and depend upon the material infrastructures in question: as Dunn Cavelty (2018, p. 27) warns, "without a close reading of the technological (im)possibilities shaping these activities," understanding their long-term political and constitutive effects is difficult, and challenging their dominance becomes impossible.

Each chapter starts with a vision of insecurity in which actors have variously worked at, *for*, or *through* boundaries to contest, configure or collaborate with each other (Langley *et al.*, 2019). Because these phenomena and categories are the outcomes of various social and political processes, Newman (2003, p. 134) argues that we are in need of a "solid theoretical base" that allows us to understand the socially contingent processes of bounding and categorization. Here, I suggest boundary work is the 'solid theoretical base' that can help us to trace the *processes* of bounding. It can examine these categories not as intrinsic or essential, but as the "result of boundary making narratives and practices that reify, naturalise […] the category as a thing-in-the-world." (Jones, 2010, p. 266) As Jones highlights, boundaries must be constantly re-fixed and re-iterated to reify the perception that they are permanent. These are ongoing social processes of fixing, or what he calls "*bounding*, because without boundaries nothing could ever be anything" (Jones, 2009, p. 180, emphasis in original).

Starting from the premise that boundaries and categorical distinctions are not essential things 'out there' in the world, but an emergent product of boundary work, what follows in the case studies in each of the chapters will showcase moments where boundaries are invoked, challenged or reconfigured in order to 'bound' cybersecurity. Cybersecurity is thus taken to be a 'thing of boundaries' in the sense articulated by Abbott, who argues that it is "wrong to look for boundaries between pre-existing social entities. Rather, we should start with boundaries and investigate how people create entities by linking those boundaries into units. We should not look for boundaries of

things, but things of boundaries." (Abbott, 1995, p. 857). This premise animates all of the analysis that follows.

Each empirical chapter is consequently oriented around illustrative moments and locations where previously 'invisible' or uncontroversial artefacts, technical incidents, materials and symbolic and social boundaries have become the focus for political debate. I have selected my case studies because they exemplify key themes or 'boundaries' that were consistently referenced by actors involved in articulating cybersecurity in these instances. So much of the cybersecurity discourse articulated by security actors suggests that all kinds of consequential boundaries are blurred, challenged or rendered obsolete by cyberspace, and that cybersecurity is a novel kind of problem that poses "fundamental challenges to traditional political concepts" (Stevens, 2016, p. 28). In cybersecurity politics, claims like these that imply 'the state' is in crisis are often implicitly invoking a 'time before,' the equivalent of the old saying of 'in my day…' (for a review of this perspective, see Migdal and Schlichte, 2016). In fact, the logical conclusion of the research in this thesis will reinforce the literature that has shown the state has never really been a stable edifice, that it has always been a socially contingent and emergent set of granular processes (Sassen, 2008; Mayrl and Quinn, 2016).

At a more modest level of analysis for the purposes of this thesis though, the project will assess how cybersecurity politics represent the efforts of political actors to make sense of, and impose some order upon, the complexity of networked communication technologies. The analytical lens of boundary work allows each of the chapters to critically assesses the vested cultural, political, and organisational interests at work in claiming that cybersecurity is about patching or spying, claims about who cybersecurity is *for*, who is responsible for *doing* it, and how far cybersecurity *goes*.

Boundary work in cybersecurity politics is the strategic practical action different vested interests undertake, with each chapter's analysis starting with a vision of insecurity from which a preferred solution 'naturally' flows. Thus, in each of the later chapters we will see different kinds of boundary work, depending upon the goals, motivations and purpose of the people or initiatives in question. The framework outlined by Langley et al. (2019) sets out a typology of three broad categorisations of boundary work, Langley et al characterise three types of boundary work from their review of the literature on boundary work: competitive, collaborative and configurational boundary work. Competitive boundary work, or work *for* boundaries, involves defending, contesting and creating boundaries for people to distinguish themselves from others and define an exclusive territory (Langley et al, 2019). This boundary work often acts as a mechanism "for acquiring resources or reproducing power, social position and status" (Langley et al. 2019, p. 8). We will see this form especially in Chapter Six's analysis of the controversy between civil society and the government's use

of software vulnerabilities for example, and in Chapter Four's analysis of the 'turf battle' between the Department of Defense (DoD) and the Department of Homeland Security (DHS).

Collaborative boundary work, or work *at* boundaries, involves negotiating, embodying or downplaying boundaries (Langley et al., 2019). This is so that people draw on those distinctions and thereby (re)negotiate, downplay or realign boundaries in interaction with others as a strategy to collaborate, coordinate or to achieve an objective. We will see this form especially in Chapter Three for example, where actors instrumentally hail but also seek to downplay historically resonant distinctions to make a political and procedural case for new organisations or new policy responses.

Finally, configurational boundary work, or work *through* boundaries, involves arranging, buffering and coalescing boundaries. This is when people work from outside existing organisational or social boundaries "to design, organize or rearrange the sets of boundaries influencing others' behaviours" (Langley et al., 2019: 8). This is often involves manipulating habits of differentiation and integration to reconfigure the bounds of organisation, usually with the intention of instigating particular kinds of collective action (Langley et al., 2019). We will see this form especially in Chapter Five's analysis of the federal arguments for public-private collaborations to produce cybersecurity as a collective good. Though these forms of boundary work are not mutually exclusive to each other, and different instances of each appear in all the chapters at different moments, it is helpful to outline this typology of boundary work here to explain the terminology used in my analysis later.

It is the contention of this project that by paying attention to 'boundary work' undertaken by social actors and stabilised by organisational and technical programs, we can critically assess those claims. As the empirical chapters will show in more detail, in some cases historically resonant distinctions are so ingrained or resilient that they cannot be sidestepped or reconfigured by cybersecurity politics. This kind of approach offers critical security scholars a tool to contextualise security politics and to counter exceptionalist discourses or neologisms. This framework may also help move STS-influenced boundaries research on from the development of specific sites and practices, to look at "…one of the most fraught and consequential contemporary sites of boundary making… how the state itself is bounded" (Mayrl and Quinn, 2016, p. 2). While some scholarly work has looked at how boundary work contributes to the development of state formation, national identities and the materialised borders of the nation or state (Anderson, 2006; Carroll, 2012), remarkably little research has been undertaken regarding the constitutive effects of boundary work in the name of state security, and the ways it embeds or stabilises security imaginaries. Chapter Two will therefore set out the theoretical and methodological rationale for the chapters that follow.

In the first of the empirical chapters, Chapter Three will begin the story of how military (cyber)security imaginaries have played a constitutive part of debates concerned with institutionalised

and organisational boundaries demarcating between peacetime and wartime activities. This narrative has most explicitly been articulated throughout attempts to institutionalise 'computer network operations' or 'cyberspace operations,' practices that have prompted debates about how to draw distinctions between its constituent elements of 'exploitation,' 'defence' and 'attack' (Committee on National Security Systems, 2015; NICCS, 2019; Office of the Chairman of the Joint Chiefs of Staff, 2020). Such categorisations, and the tools and techniques of such computer network operations, were initially developed in the intelligence community. However, these tools and techniques (or 'capabilities') have not fitted neatly into pre-existent notions of historically resonant distinctions governing peacetime and wartime activities on the one hand, and distinctions governing intelligence and military activities on the other. Efforts to establish *military* cyber capabilities have therefore triggered alternating phases of collaborative and competitive boundary work to fit these tools and techniques (or 'capabilities') into pre-existent notions of historically resonant distinctions governing peacetime and wartime activities and distinctions governing intelligence and military activities.

As part of the military's efforts to determine its roles and responsibilities in national 'cybersecurity' in distinction to that of the intelligence agencies, it has articulated a doctrine that suggests the development of distinctively 'military' cyberspace capabilities are the result of a 'natural trajectory' of cyberspace, technology or international politics. For example, in the words of Richard Harknett, the first scholar in residence at U.S. Cyber Command (CYBERCOM) and the National Security Agency (NSA),

> It is, thus, not a choice, but a structurally and strategically driven imperative to reorient U.S. cyber strategy around continuous action. The states that master persistent engagement will not only be more secure in cyberspace, they will also position themselves to enhance their national power relative to others. (Fischerkeller and Harknett, 2018 n.p.)

Contrary to the overdetermining 'structurally and strategically driven' narrative suggested here, this chapter will instead argue that 'persistent engagement' is also the product and expression of boundary work that has sought to demarcate CYBERCOM from their progenitors in intelligence agencies and practices, to establish authority and autonomy for the new command. By critically examining documents, strategies, policies, official discourses, promotional materials, and specific programs and initiatives, this chapter will show how only as CYBERCOM has taken shape has the realization evolved that 'persistent engagement' is the strategy that best justifies the military command's existence.

The debates in Chapter Three matter because as we shall see, they are concerned with establishing how far 'cybersecurity' goes, whether the threats and vulnerabilities the nation faces merit action by intelligence agencies or more hostile military actions, and about 'fixing' or *working for* the bounds of 'cybersecurity' accordingly. The chapter finds that while distinctions surrounding

international legal definitions of 'wartime' cyber actions have been fairly settled since 2012, what counts as legitimate 'peacetime cyber operations' or cyber operations 'below the threshold of war' in the context of the United States has gradually shifted or enlarged as a result of these imaginaries and initiatives. In fact, the chapter argues that the bounds of permissible 'peacetime' or 'grey zone' military cyber actions have been expanded both as a condition for, and a condition of, their efforts to articulate the distinctiveness of CYBERCOM from its technical and organisational progenitors in the intelligence community. This chapter offers a challenge to many existing academic approaches that focus on technical and strategic aspects as having causal explanations, to instead show a more fraught process of social, bureaucratic, legal, cultural and technical efforts to produce the state's and military's role in 'cyberspace.'

A very different vision of 'cyberspace' and 'cybersecurity' emerges in Chapter Four. There are always multiple imaginaries in a society and across federal organisations, and as we shall see, these play an important role in shaping programs and policies, so that military cybersecurity imaginaries of cyberspace as a domain no longer appear so hegemonic (Smith, 2009). This is why this chapter will analyse the DHS' imaginaries as a counter to the military's (cyber)security imaginary. Thus, as part of their competitive boundary work, or work *for* boundaries to articulate and advocate for the extent to which 'cybersecurity' should be a military or homeland security matter, federal actors have differently amongst themselves emphasised its 'internal' or its 'external' characteristics and features, and reinscribed boundaries demarcating between 'homeland security' and 'homeland defense,' according to their specific interests and organisational cultures. In the US, the military has traditionally been responsible for activities outside of the state's territorial bounds, while civilian agencies have responsibilities for security activities deemed domestic and 'internal'. While specific organisations were given (high-level, policy) cybersecurity responsibilities early on based on the longstanding territorial division of labour between civilian agencies and the military, working out how to enact those responsibilities for cybersecurity amongst federal actors has been a slow and fraught process, apparently challenged by the global and interconnected features of cyberspace. This chapter argues that in their efforts to *work for* boundaries to distinguish their vision of cybersecurity from that of the DoD, a risk-based approach to cybersecurity gradually emerged and was constituted in various initiatives as a productive strategy for DHS advocates. Competitive boundary work strategies were key to DHS actors being able to 'domesticate' and 're-territorialise' cybersecurity by shifting the focus onto managing the nation's internal vulnerabilities through a risk-based framing. The advent of 'homeland security' has prompted some writers to argue that it is now impossible to maintain any rigorous distinction between the 'internal' and 'external' dimensions of US security policy (Bigo, 2001). However, Chapter Four finds that in some areas of 'homeland security,' representatives of DHS have worked hard to reinscribe and police those distinctions through competitive boundary work in their

efforts to defend the credibility and legitimacy of their cybersecurity roles. The chapter finds that DHS sought to reproduce and reinscribe such spatialised boundary distinctions in their initiatives, rather than reconstitute them.

The debates in this Chapter matter because they are concerned with establishing who 'cybersecurity' belongs to, which state agencies should have what roles and responsibilities, and contests over the power to define those parameters. Despite the recurrent and essentialised narratives about the borderless 'nature' of cyberspace, this chapter will show how by 2018, government actors and agencies had mostly managed to reassert how cyberspace fits into or maps onto existing schema and jurisdictions long used to distinguish between 'internal' and 'external' security: the competitive boundary work analysed in this Chapter will show how DHS inscribed or 'mapped' a territorialised and spatialised understanding of cyberspace into their cybersecurity activities and policies, but with very different emphases to those of the military. In this case of the Department of Homeland Security's cybersecurity remit, both 'cybersecurity' and 'homeland' are categories whose boundaries are organisationally and materially contested. Here, boundary work has sought to embed competing imaginaries into technical and organisational infrastructures and has also helped define priorities and allocate resources for carrying out different tasks related to cybersecurity. In this sense, while military actors had tried to produce a vision of the homeland by enacting and managing the 'external' boundaries of that homeland, and so constitute a cybersecurity oriented around external threats, in the end the DHS' boundary work was more successful in producing and enacting links between contested boundaries of 'homeland' and 'cybersecurity.'

Chapter Five moves the analysis beyond the politics of state security agencies to critically examine the role that non-governmental actors have played in constituting cybersecurity as a matter of concern. This chapter shows how through a mixture of collaborative and configurational boundary work, boundaries between 'public' and 'private' have been simultaneously problematised and reinscribed in cybersecurity politics as a way for government actors to articulate their vision of cybersecurity. Here we will see that as part of efforts to expand or enlarge the bounds of cybersecurity and to make space for private sector involvement, state actors first articulated an imaginary of insecurity in which their lack of insight into networks posed an existential threat to national values, social orders, and technological futures. This chapter's analysis of federal strategy and vision documents leads it to argue that government actors have undertaken *configurational* boundary work to orchestrate and produce collective action in the name of 'cybersecurity,' based upon their stated desire of "extending cybersecurity" (White House, 2010, p. 5) and constituting it as a 'shared responsibility' for the whole of society (Carr, 2016). This is an important element of the cybersecurity discourse, given that these incremental and recursive cybersecurity politics are also a reflection of broader "fundamental conceptual and political debates regarding the evolving nature of security

governance" (Bossong and Wagner, 2016, p. 266; Bures and Carrapico, 2018). As we will see, cybersecurity politics do not represent an essentialised shift of power from state actors to non-government entities, but instead signify a more diffused (and sometimes contested) unbundling and reconfiguration of political authority.

The debates in this chapter matter because by linking boundaries of 'public' and 'private' in particular ways, two different conceptions of cybersecurity (and who it is *for*) emerged as a result: a focus on the security of citizens, and the security of corporations. Rather than 'cybersecurity' emerging as the result of a series of technical features or fixes, we can see how (similarly to Chapter Four) the initiatives in this chapter demonstrate how technical features can be said to both produce and challenge boundaries, which then inform the development of subsequent features and boundaries. In this instance, government and corporate actors would draw on and *work at* distinctions between 'public' and 'private' as resources in their efforts to legitimise private sector attribution reports. This boundary *work at* those distinctions would work to downplay and thereby reconfigure conceptions of 'private' roles in cybersecurity, whilst also constituting an imaginary of cybersecurity in the favour of the security and interests of corporate referents. Meanwhile, in the case of encryption technologies, government configurational boundary work to orchestrate security at the interface of distinctions between 'public' and 'private' show how they are not always successful in embedding their boundary work in initiatives and legislation, with dissenting competitive boundary work by private sector actors constituting cybersecurity imaginaries that favour the citizen instead. The different boundary work strategies analysed in this chapter indicate how governmental or state discourses are not so hegemonic or totalising as they may first appear: the success of competitive boundary work strategies of corporate actors like Apple show how state actors may not be able to automatically rely on their political authority nor mobilise the most resources to always stabilise their boundary work.

Like the chapters before it that have shown how different characteristics are ascribed to cybersecurity at different times, depending on the interests and background of the speaker, Chapter Six finds that 'disclosure' has been used as part of competitive boundary work strategies to demarcate and work *at* the political and operational bounds of 'cybersecurity.' From 2013 onwards, a series of cyber breaches and international cybersecurity incidents prompted criticisms from diverse commentators outside of the US government. They challenged the rationales and legitimacy of the government's use of software and hardware vulnerabilities in the course of intelligence and law enforcement missions. As we shall see, mobilising boundaries of 'disclosure' was intended to preserve the autonomy of intelligence and law enforcement agencies that would otherwise be politically curtailed in their use of these technical and operational tools. While the chapter argues that the Vulnerabilities Equities Process (VEP) has set procedural and practical parameters on disclosure, *working for* boundaries in order to protect the autonomy of government agencies to use

vulnerabilities, it will also show first how official discourses have adapted to dissenting narratives in order to defend the political legitimacy of the government's conceptualisation of cybersecurity. As in the previous chapter, this again highlights how state security discourses may not be so totalising that they cannot be contested.

As opposed to the internal turf battles amongst different state agencies as outlined in Chapters Three and Four, or the configurational boundary work in Chapter Five, the competitive boundary work of federal actors analysed in this chapter is directed towards policing and maintaining boundaries with those *outside* the government. This chapter will demonstrate how 'disclosure' has been used as the basis for claims to legitimacy by different communities. In the case of Federal actors defending these practices, disclosure was used to *work for* boundaries between lawful and illegal uses of vulnerabilities, and to draw boundaries between 'national security' and 'cybersecurity.' Meanwhile, critics of the government's claims would undertake competitive boundary work to challenge the government's claims, methods and rationales for weighing whether to retain or disclose vulnerabilities.

The debates in this Chapter matter because they are concerned with setting parameters on what cybersecurity *means*, whether cybersecurity is concerned with prioritising the patching, or exploitation, of vulnerable or insecure technologies. The competitive boundary work analysed here has been an important part of both slowly re-constituting 'disclosure' as a practice, as well as defending the US government's 'cybersecurity' credibility. In contrast to Langley et al's (2019) broad typology then, this chapter reaffirms that boundaries may be negotiated, embodied or downplayed without necessarily stemming from intentional strategic intended to facilitate collaboration – they can be reconfigured in the name of competitive strategies too. As this chapter will show, 'vulnerabilities' are not just technical, they are social and human too, made up of a uniquely non-fungible interplay of technologies, people and processes, raising important questions about determinist narratives that claim these state practices are inevitable responses to the technologies. This chapter will demonstrate that implicit within the debates surrounding 'disclosure' of vulnerabilities are concerns about the technological and networked future, with all its potential vulnerabilities and unknown risks. Boundary work analysed in this chapter is therefore concerned with making technologies legible in ways that support 'classical' responsibilities of the state, whilst also defending the autonomy of government agencies to undertake operations in cyberspace.

Taken together, these chapters will lead Chapter Seven, and the thesis overall, to conclude that that what cybersecurity 'is,' how its boundaries are drawn, depends on the pragmatic utility of any given borders or boundaries for the protection, expansion or denial of political authority. With this analytical lens we will see how cybersecurity is emergent, a thing of boundaries, and boundary

work has been concerned with getting different (often incommensurate) versions and imaginaries of cybersecurity to 'hang together' (Mol, 2010). An analysis of the military (cyber)security imaginary is the first of the analytical chapters because a great deal of the controversy and contention in the subsequent chapters follows from (or seeks to contest) the widespread spatialised articulations of cyberspace as a warfighting 'domain.' By leveraging their continued post-Cold War investments in agencies such as the NSA, and by bringing together the service branches' scattered cyber components, the DoD has been able to wield an outsized influence on the shape of cybersecurity politics thanks to the enormous resources they are able to bring to bear. As a more recent case in point of the investment the DoD is able to obtain compared to other Federal agencies, the 2020 budget proposal asked for more than $9.6 billion for Defense Department cyber operations, compared with just over $1 billion for civilian Federal cybersecurity efforts (Boyd, 2019; Executive Office of the President; OMB, 2019). This gives imaginaries of cyberspace as a warfighting 'domain' all the appearances of a hegemonic discourse, one in which its technological and structural 'nature' determines that the military treat it as such (Branch, 2020).

However, in each of the chapters that follow Chapter Three, we will see how the DoD has not had an unquestioned ability to set the parameters of the matter at hand. The counter-imaginaries of DHS, civil society, intelligence agencies, law enforcement are important, but they are often overshadowed by the scale and influence of the Pentagon and its military branches. The structure of the thesis can be thought of as telling a story of the iterative back-and-forth between these imaginaries. If we are to open the space for alternative conceptions of cybersecurity than one based on approaching cyberspace as a domain of warfighting or with the state as the main referent, then the chapters take this order as a way to demonstrate how state cybersecurity and initiatives have emerged processually, at the point of boundary work amongst and between different interest groups. This is important because it shows that despite state discourses that suggest that cybersecurity is overdetermined by technologies or strategic imperatives, a critical analysis of actors' strategies instead helps explain how these visions of cybersecurity variously iterate from – and sometimes must accommodate – competing visions and boundary work. Security imaginaries are generally studied as top-down and pre-determined by state actors, so examining cases where those visions are contested or dissented – as in the analytic chapters that follow – can help explain the emergence or persistence of official framings as they encounter practical or political obstacles and alternative imaginations.

This is important because while there has been a good deal of critical discourse analyses of cybersecurity and threat constructions, less has been said about the overarching narratives that form the basis of (state) cybersecurity imaginaries. Moreover, by taking a case study approach and comparing across different agencies of the state, as well as those outside of the government (e.g. in Chapter 6), we can begin to pick out the key themes as well as the points of contention across these

narratives, to show how there is more to cybersecurity than common perceptions of technological determinacy. I hope to supplement the critical analyses of the technical elements of cybersecurity practices and programs to show more than just substantive and technical definitions, but some underlying (and culturally-specific) rationales for the form that cybersecurity politics have taken in the US. Furthermore, by addressing the different (competitive, collaborative, configurational) boundary work strategies, we can begin to critically reflect on the conditions and resources that informed how some strategies may have been more successful than others, highlighting the contingency (and vested interests) of some of those otherwise seemingly totalising discourses. Statist discourses of security are a prominent example of powerful discourses (Weldes *et al.*, 1999), but the analysis in this project can begin to show the limits of those powers.

Rather than trying to 'fix' cybersecurity with substantive definitions then, the analyses in these chapters of the arrangements of people, organisations, institutions and technologies will critically engage with the ways that 'cybersecurity' is an emergent phenomenon, constituted by boundary work embedded in heterogenous initiatives and programs. Chapter Seven will then conclude with a discussion of the wider implications of this research, drawing out how charges and counter-charges in US cybersecurity politics, articulations of specific boundaries, distinctions of how it 'fits' into one category rather than another category have each signified how boundaries stand in for and also help produce choices of one future over another. Cybersecurity politics in this context thus become about fixing the bounds of cyberspace so that they conform to (but also at times challenge or reconfigure) ideas about the state as security provider, and the state's relationship with cyberspace.

1.6 Conclusion: Bounding cybersecurity.

Despite being a conspicuous and ever-expanding focus for security actors in the United States then, what counts as 'cybersecurity' or how it is practised by state actors is still being negotiated and contested. Through an analysis of the 'cybersecurity politics' involved in constituting it as a matter of state security, the overall argument of this thesis is that key actors engage in forms of 'boundary work' to 'fix' the boundaries of 'cybersecurity' as part of their efforts to stabilise state practices in this matter, and to contest and police their own symbolic and organisational boundaries in turn.

It is not simply the boundaries of 'cybersecurity' as a practice that are being variously contested, negotiated and constituted within US cybersecurity politics though. As we will see, there are some metaphors and boundaries in US cybersecurity politics that repeatedly surface or get problematised, where moments of controversy prompt actors try to settle and fix conceptual, political, organisational and institutional boundaries. By focusing on the ways that such boundaries are articulated, problematised and mobilised in cybersecurity politics, the thesis will provide important

critical insights into the political and cultural assumptions animating this context. We will see how such boundary distinctions are culturally specific, acting as productive cognitive and political frameworks for actors to make sense of new concepts and phenomena. The thesis will thus show how in some important ways, efforts to 'bound' cybersecurity are constitutive of boundaries and institutionalised arrangements in those contexts, worked and re-worked in a recursive and iterative manner. Using the analytical framework of 'boundary work' discussed now in the next chapter, this project will illustrate how and why these contests over 'cyber' matter politically and technologically. As the thesis will demonstrate, technologies, consequential categories, institutional responsibilities, political authority and national identity are also constituted and challenged in and through these debates.

Chapter Two: Boundary work, imaginaries and methods

2.0 Introduction

This thesis' central research question asks to what extent, and in what ways, boundaries are reconstituted in and by cybersecurity politics. By looking at cybersecurity in terms of boundaries and boundary work, this research question directs our attention to the processual characteristics of security practices in the US as a way to de-essentialise those discourses. Rather than taking cybersecurity as a singular object, this thesis will sketch out the messy, contingent, fraught processes of negotiation, enrolment, persuasion, and contestation that go into making a difference and into making things happen in the name of 'cybersecurity.'

While the introductory chapter went some way to explaining its conception of 'cybersecurity politics,' this chapter will spend more time outlining what it means by 'boundaries,' and its analytical and methodological framework for assessing the extent to which boundaries are made or (re)constituted. First, it will set out how efforts to 'bound' or 'fix' definitions of cyberspace represent efforts by state actors to make it amenable to state security interventions. Then, through a discussion of the interplay of discourses, practices and imaginaries with institutions, organisations and materiality, this chapter will then explain what I mean by (re)constitution. The approach taken in this thesis is that 'culture' can be triangulated in terms of practice, discourse and materiality (Carroll, 2006). Drawing upon this conception of culture, the second section will then explain how it conceives of 'boundary work' as a practice that is both derived from and productive of culturally and temporally specific arrangements of people and things, or in other words, as a triangulation of practice, discourse and materiality. Building upon this conception of boundary work, a discussion of the relationship between security imaginaries and boundary work will explain the rationale for the chapters' structures. Finally, the chapter will draw out how I mobilised this analytic and methodological framework, to support the contention in this project that the concept of boundary work can also advance a distinctively processual and relational view of security imaginaries in general, and cybersecurity in particular.

2.1 Cybersecurity is complex, performative, emergent.

Concerns about 'cybersecurity' are an embodiment of tensions between national imaginaries of technological success and innovation on the one hand, and large-scale technological vulnerability on the other. A key contention of this project is that boundary work in cybersecurity politics thus becomes about 'fixing' the bounds of cyberspace so that they conform to (but also at times challenge or reconfigure) ideas about the state as security provider, and the state's relationship with cyberspace.

Here, we can trace a constant and ongoing tension in official discourses wherein the perceived benefits of increased opportunities afforded by the 'open internet' and increased flows of information and capital, are pitted against the perceived risks associated with reliance upon large scale and ubiquitous networked communications technologies. As the previous chapter demonstrated, cybersecurity politics are a key site for government and non-government actors in the US to negotiate how 'cybersecurity' therefore maps onto established jurisdictional boundaries and agency and federal divisions for security responsibilities.

With all of these definitions circulating in US discourses, it is tempting to try and explain away the differences, to look for more accurate or more 'realistic' readings of the thing in question. As we saw in the last chapter, this is the crux of the problem for many of the state actors, who complain about cyberspace's exceptional novelty or the ways that cyberspace and thus cybersecurity blur historically resonant lines and boundaries. As a researcher, it is also tempting to simplify the conflicting readings, both for pragmatic reasons and for analytical neatness. No doubt there are some aspects of cybersecurity politics that are amenable to positivist methodologies: perhaps attack distributions, or the implementation of statutory federal cybersecurity requirements, or defence spending on cybersecurity programs could be analysed with such accounts.

However, in the case of this thesis' research question, such an approach misses the political consequences that stem from efforts to bound cybersecurity. Those essentialising and substantive accounts of cyberspace and cybersecurity discussed in the previous chapter try explaining the differences away and indicate a form of perspectivalism. Such approaches imply that studying different perspectives can *explain it away* by imposing order and terms, while I am arguing this leaves out important (and in this case, constitutive) disorder present in the attempts to bound cyberspace (Law 2004), what this project has designated as 'cybersecurity politics.' Such 'methodological auditing' would miss some of this complex political reality, with deleterious effects of potentially naturalising securitised readings of networked communication technologies.

In the case of US state security actors, we can view a lot of the narratives and policies concerned with securing cyberspace as ways of extending pre-existing practices to other arenas of social reality. The same can be said of the widespread use of particular institutionalised metaphors (Branch, 2020): defining cyberspace as a 'domain' of warfighting meant that policymakers and military actors have sought to fit cyberspace operations into patterns of 'traditional military activities' and 'deterrence', looking for regularities that fit military instruments and methods. Various groups will make sense of a new concept in diverse ways, anchoring it to different concepts depending on their familiar framings (Riesch, 2010). At the same time, and as Chapter Three will bear out in more detail, the production and stabilisation of 'cyberspace' as a 'domain' is entangled with, and mutually

constitutive of, military organisational cultures and instruments (Jasanoff, 2004, 2015; Evans et al 2020). Unlike the frameworks of the DHS that favour cyber 'ecosystems' and 'infrastructures' in Chapter Four (CISA, 2020a), or corporate and advocacy frameworks that favour dealing with cyberspace in terms of 'public health' and cyber 'hygiene' in Chapter Six (Lapointe, 2011; Chappellet-Lanier, 2017; Slupska, 2020), thinking and representing the challenges of cyberspace through conceptual frameworks of 'domains' and 'war' produces different bounds for 'cybersecurity.' In the case of cybersecurity then, contests to define its bounds are performed and enacted differentially by each of the organisations, agencies and groups involved in describing it.

By posing the problems of cyberspace and cybersecurity in specific ways, different groups have thus produced and institutionalised (sometimes competing) social and technical ensembles, those "heterogenous elements assembled and directed toward coordinated and concrete ends" (Jones-Imhotep, 2017, p. 8). In this sense, 'cybersecurity' becomes both a means and an end: it is a disparate set of practices, discourses, organisations and technologies variously enlisted, enrolled or accumulated with the implicit (or sometimes explicit) end project of realising particular imaginaries of desirable futures. These aggregated social and technical elements have in turn made particular readings of cyberspace more durable. One example of this is the institutionalisation of cyberspace as a domain of warfighting, a sociotechnical 'method assembly' (Law, 2004) in the form of a military command (CYBERCOM) co-located with the National Security Agency (NSA).

Rather than trying to overcome or explain the competing security rationales at work in US cybersecurity politics, there may be good reasons why we should follow this messiness and apparent incommensurability. These realities are real enough because they have consequences. Of course, conceptualised in this way, 'cybersecurity' signifies such an expansive empirical matter that simply noting that it is noncoherent or showing evidence of competing rationales is not a remarkable insight (Law, 2017). The important thing is to show why and where this complexity and boundary making is making a difference. In the case of the research question animating this project, paying attention to the ways that social actors try to impose some order on the dynamic phenomena of global networked communication technologies helps us to denaturalise state security discourses. In other words, drawing out the mess shows us how things could have been otherwise, how 'cyberspace' could be more than a domain of warfighting, but also an ecosystem, an infrastructure, a global commons; and that 'cybersecurity' could be more than military defence and the state as the referent, but also the security and rights of individual citizens or communities. In other words, paying attention to the complexity and efforts to impose order helps us draw out alternative narratives. This does not necessarily equate to relativism: after all, not all statements become accepted, not all readings of cyberspace become institutionalised and concretised. There is resistance, instances where 'stuff'

pushes back against representations, where actors are not able to assemble a sufficient weight of authority and evidence and resources to make their case.

The approach in this thesis is therefore concerned with capturing those ongoing contingent processes that make some realities or experiences more widely accepted (or 'black-boxed') than others. Exploring the work to make vulnerabilities and (in)security meaningful in cybersecurity politics — undertaken by multiple actors — with its narratives and counter-narratives, will help illuminate the ongoing and unfinished processes by which the state's role(s) in cybersecurity are being constructed and legitimised. This rest of this chapter is therefore concerned with laying out ways for us to study and methodologically pay attention to the empirical complexity of US cybersecurity politics and its productive dynamics.

2.2 'Cybersecurity' as a 'thing of boundaries.'

One of the recurring themes in state actors' efforts to define 'cybersecurity' as a matter of national security are official admissions that the state alone cannot address the threats posed by these networked technologies because the claim that cyberspace exceeds traditional boundaries. A report by RAND in 1996 articulated the issue in terms that would feature in subsequent congressional and popular debates up to the present day, stating that "traditional distinctions" such as "public versus private interests, warlike versus criminal behavior—and geographic boundaries, such as those between nations as historically defined, are complicated by the growing interaction within the information infrastructure." The report suggested that these "boundaries […] are porous" rendering such traditional distinctions "less meaningful" (Molander et al, 1996, p. xiv). A focus on such 'porous boundaries' would continue to trouble policymakers. As Representative Ike Skelton described the issue before a House Armed Services Committee hearing more than a decade later, "[c]yberspace is an environment where distinctions and divisions between public and private, government and commercial, military and non-military are blurred." (in US House of Representatives, 2010, p. 1). In short, despite various efforts at fixing substantive definitions, cyberspace, in many ways, seems to exceed and evade those definitions. For state actors, this has provided significant contention and debate. Cybersecurity politics are thus the forum and form that these concerns about bounding cyberspace take place.

For these state actors then, security of and in cyberspace is portrayed as an expansive and unstructured set of problems. However, a closer look at the ongoing politics of its definitions reveals political and engineering efforts to redefine the problem as more structured. Different actors seek to 'fix' the boundaries and meanings of cyberspace: the boundaries of cyberspace need clarification, settling, fixing; while, simultaneously, cybersecurity policies and politics represent the efforts to 'fix'

or repair such problems and ambiguities at a general level and/or to address specifically identified 'cyberthreats' such as crime, espionage and the actions of other state actors.

As the empirical vignettes in the thesis so far have illustrated, and as the project more broadly will bear out, cybersecurity politics are repeatedly invoking and mobilising a range of symbolic, cultural, social and institutional boundaries. These are "conceptual distinctions made by social actors to categorize people, practices, materials and even time and space," and they are also the "tools by which actors and groups struggle over and come to agree upon definitions of truth and reality" (Lamont and Molnár, 2002, p. 168). Cultural and symbolic boundaries are something that we reference and build on an everyday basis, and the classification processes that we engage in to split some things and join others along conceptual lines can appear both natural and inevitable, as though these processes are a reflection of some essence of the thing themselves. But as Lamont and Molnár highlight (2002: 176), this kind of 'boundary work' matters because it constitutes the systems of classification that emerge to bring social and political order to our lives. This project contends that cybersecurity politics are exemplary of these dynamics.

So how should we study these processes of boundary construction and categorisation, how does the concept of boundary work help address the recurring problematisation of boundaries in US cybersecurity politics? Sorting and classifying the world around us may be an instinctive and cognitively useful practice, but the ubiquity of these social practices can also serve to obscure the sometimes mundane and quotidian processes that went into the classifications. As Bowker and Star (2000, p. 319) write: "[c]lassifications are powerful technologies. Embedded in working infrastructures they become relatively invisible without losing any of that power." This study therefore uses the concept of 'boundary work' to examine how actors enact, control and contest consequential distinctions. This work can be traced in the ways that actors instrumentalise their definitions of the 'technical' fields of computer security and information security as separate from politics, and the ways in which a range of longstanding conceptual distinctions are mobilised and constituted in the contests to define (or bound) cyberspace as a state security concern. The next part of the chapter will now draw out the descriptive value of boundary work, before going on to set out its explanatory value.

2.2.1 Boundary work

The concept of boundary work was initially developed by Gieryn (1983), Holmquest (1990), and Taylor (1994, 1996) among others. Originating in the sociology of scientific knowledge (or what has become known as Science and Technology Studies [STS]), the concept was first used by Gieryn (1983) to describe the efforts of scientists to establish their epistemic authority and differentiate (demarcate) science from other knowledge practices. For Gieryn — wrestling with the problem of

defining science without resorting to describing it terms of the 'scientific method' — boundary work was the strategic practical action that scientists undertook to promote the distinctiveness of their work from 'non-scientific' fields, in an effort to defend and legitimate their specific form of epistemic authority. Boundary work thus focused on the processes and rhetorical strategies that make up such processes of demarcation. In other words, boundary work is about power relations: the power to speak, the power to define the matter of concern, the power to set social and political agendas (Bourdieu, 1991).

Gieryn's approach focused on 'public science' and the kinds of jurisdictional claims that scientists would make in public and political settings. Descriptive analysis of these rhetorical and ideological struggles for legitimacy and jurisdiction therefore focused on the public articulations made by actors. Gieryn (1999) focused on explicit credibility contests in the public domain, more than the habitualised practices of actors' professional and everyday lives. While much sociological research has argued for the important ways in which everyday interactions and boundary work serve to shape and constitute the professional contours of groups (Abbott, 1998, cited in Allen, 2000; Persson, 2010), Gieryn's spatial metaphor with its focus on public domain articulations and negotiations has useful parallels to my analysis of state security efforts to 'bound' 'cybersecurity' and its attendant spatial conceptions of cyberspace. While his was a focus on the rhetorical strategies used by scientists, Gieryn's framework has descriptive value in detailing the processes involved at these moments of ideological demarcation. According to Gieryn, "[e]ssentialists *do* boundary work, while constructivists *watch* it get done by people in society" (1995, p. 394, emphasis in original). Using this sensitising and descriptive concept, we can watch boundary work getting done in US cybersecurity politics, helping to direct our analysis of official statements, policy documents, congressional testimony and media coverage.

As well as its descriptive value, boundary work also has explanatory value. For Gieryn and other approaches, boundary work in the social sciences is concerned with the social functions of people's words and practices, charting how they build symbolic boundaries, and how communication works across those boundaries (Riesch, 2010). Boundary work represents the efforts of different social groups to give themselves legitimacy and authority in the blurry space between these groups. Boundary work can also play a role in helping these different worlds cooperate (Star and Griesemer, 1989; Jasanoff, 2009). Gieryn's discussion of scientific boundary work characterised the objectives of expansion, monopolisation and protection of the autonomy of science. As we will see in the way these three broad objectives are visible in the boundary work in later chapters, boundary work has wider implications since these practices are generic features of social and political groups establishing their credibility. This was something he later acknowledged, recognising that his framework could have utility in the analysis of other social domains (Gieryn, 1999, p. 34). What animates this thesis is not

merely the *description* of official boundary work but understanding the processes by which these interpretations are constructed, promoted and accepted. In the case of cyberspace and cybersecurity, these bounding processes can have profound effects on how we organise and understand the world, as well as on how some issues get politicised or prioritised over others.

Defining the bounds of 'cyberspace' and 'cybersecurity' are the overall themes in the later chapters, but another motif that features in cybersecurity politics are efforts to demarcate 'security.' As the chapters later will demonstrate, efforts to define cybersecurity are shot through with, and oriented around, contestation over what counts as 'security,' and for whom and what, thereby prioritising the interests of some actors and conceptions of security at the expense of others. As security scholars have long demonstrated, claiming to 'speak security' is a claim to represent the existential interests of people and communities and as such carries considerable normative weight. The distribution of a great deal of resources rest on those claims too. But like efforts to distinguish science from non-science, it is not possible to define 'security' by making reference to some essential nature 'out there' that it possesses. After all, social constructivists have long argued that 'security' is what agents make of it, and that security can be studied as a 'structured field of practices' where some people and collective actors are more privileged to speak and construct security issues than others (Buzan et al, 1998, p. 31; Huysmans, 2002; Williams, 2003; Vuori, 2008; Berling, 2011; Balzacq, 2014; cf. Bourdieu, 1991). For example, in securitization theory, power is thought to be "derived from the use of 'appropriate' words in conformity with established rules governing speech acts" (Balzacq, 2005, p. 171) and that those who 'speak security' do so because they already possess some institutional or organizational capital to do so (Huysmans, 2002). While security may be "a strong legitimator" or clearly related to justifications of legitimacy as some have argued (Vuori 2008: 68; Balzacq, 2014), the capacity to 'securitize' depends on the position from which the security claim is made (Huysmans, 2002). Rather than explicitly examining how that capacity to speak has been attained or is actively maintained, securitisation frameworks focus on how those securitisation efforts are institutionalised 'downstream.' A boundary work approach flips that around, to see how 'speaking security,' demarcating an issue as 'security' or not, is akin to mobilising 'science' in Gieryn's original formulation.

Thus, when we take a boundary work approach to studying cybersecurity politics (and beyond), we can begin to see how political authority does not stem from some essential characteristics of 'security' that automatically confers that authority. Gieryn (1999) demonstrated that 'science' is not one thing: its boundaries are drawn in different ways at different times depending on the context and interests of those demarcating its parameters, and different characteristics are emphasised at the point of those efforts. Similarly, the selective ascription of this or that characteristic to cybersecurity cannot be explained by what (cyber) 'security' really is, but only by the instrumental use or interests it may serve to draw them in that way, not only for the allocation of resources, but also for the

protection, expansion or denial of political authority. Claims to political authority thus rest on boundary work. While some actors may be better positioned to do boundary work than others (Pereira, 2019), the analytical framework can also show us how boundary work is in turn a constitutive part of efforts to produce (or maintain) credibility and political authority. That capability to 'speak security' emerges in part as a product or epiphenomenon of boundary work. The chapters that follow will show how ideas such as 'the state' and 'security' are examples of the kinds of distinctions that can have profound social implications, and the boundary work that actors undertake that invoke these boundaries also serve to constitute them, in incremental and recursive ways.

The idea of boundary work therefore resonates as a way of denaturalising the categories that are being articulated by US state actors and beyond in the context of cybersecurity. According to Bijker, boundary work is not just about demarcating 'science,' but is "the work done by scientists, policy makers, civil servants and politicians to distinguish politics from technology and then to relate the two again in specific terms." (Bijker, 2006, p. 690). This apt spatial metaphor can be extended to other disciplines where we see actors actively working to separate distinct matters of knowledge and define authority for those domains of practice and inquiry. As Chapter Five will exemplify, boundary work acquires a special salience when technical experts (such as computer scientists or threat intelligence companies) seek to extend or monopolise their areas of expertise, or to defend their autonomy (Kinsella et al 2013, p. 284). This is why boundary work has utility for describing the ideological or practical demarcations of other professions or organisations, outside of the demarcation of science, including the demarcations involved in formulations of cybersecurity.

Boundary work is not purely rhetorical or discursive though. While boundaries are cognitive functions rather than natural phenomena, they become concretised and habitualised (as well as contested and reformulated) through practice, and serve to organise people's thinking as well as social relations (Lamont and Fournier, 1992; Starr, 1992; Gieryn, 1999; Fuller, 2003). Though Gieryn's emphasis was on rhetorical strategies and discursive processes, boundary work is thus manifest (and constituted) in more concrete arrangements too. However, Riesch (2010) suggests that early scholarship on boundary work does little to lay out exactly what boundaries are supposed to consist of, other than metaphoric and symbolic distinctions. How does boundary work become concretised, accepted, successful, institutionalised, black-boxed? How is it made *durable*: more than just rhetoric? What cultural 'hinterlands' precede these discourses for them to become possible? In the next section I therefore set out how boundary work is more than just strategic rhetorical action, to lay the groundwork for the arguments of later chapters, which examine the manner in which boundaries are (re)constituted.

2.2.2 Boundary work and triangulating culture

This section will explain this conceptualisation of culture and technology in more detail, but it draws upon the work of scholars such as Weldes (1999), Wyn Jones (2000) and Carroll (2009) in their recognition of the dialectical interactions of technology and culture and, as this chapter will draw out, boundary work. The approach taken in this thesis is that 'culture' can be triangulated in terms of practice, discourse and materiality (Carroll, 2009), and this is relevant because 'boundary work' is both derived from and productive of culturally and temporally specific arrangements of people and things. In other words, boundary work draws from, but also constitutes, culture. This is important to underscore because despite his focus on the 'Cultural Boundaries of Science' (Gieryn, 1999), Gieryn offered no theory of culture (Swedlow, 2017).

As we shall see, articulations of boundaries in cybersecurity politics invoke and constitute a range of symbolic, conceptual, institutionalised, and social boundaries. Here, the assortment of boundaries articulated in the context of US cybersecurity politics provide the conceptual tools that groups use to compete over the production, diffusion and institutionalisation of different narratives and principles in their social relations. Importantly, moreover, it is enabled or constrained by the already constructed social world, such as particularly evocative discourses, powerful organizations, sets of practices, or what Law (2004) would describe as 'method assemblages' (Kinchy and Kleinman, 2003; Carroll, 2009). This requires some unpacking.

Mirroring the work of Bowker and Star (2000), though boundaries may be cognitive practices to begin with, they argue that pragmatically, "things perceived as real are real in their consequences" (Thomas and Thomas, 1917, cited in Bowker and Star, 2000, p. 53). What separates a profession or conceptual distinction from others is whatever people do to make it separate, such as using specific language, institutional organisation or professional links (Evans, 2009). Boundary distinctions can also become engrained through technocratic politics (Huysmans, 2011, 2014), whereby agencies quietly and routinely deal with an issue in a way that engrains the distinctions between 'state' and 'non-state,' or between 'peacetime' and 'wartime' for example. Operational procedures and technocratic discourse can operate independently of instances that are visibly politicised or publicly problematised in elite boundary work (Zajko, 2015), with protocols and procedures working to *enact* those boundary distinctions. Distinctions can thus become 'solid' through the ways they are lived or performed, instantiated in buildings and objects, protocols and organisations, practices and procedures. This conception of 'concretisation' and 'materialisation' resonates with the valuable insights of materialist scholars in STS who have long underscored the ways in which the 'social' and the 'technological' are

irrevocably co-constitutive of each other[2] (Barad, 1998; Leonardi, 2012; Latour and Woolgar, 2013; Jasanoff and Kim, 2015). It is in this sense that boundary work may always be potentially performative, and the conditions of this performativity and its subsequent concretisation are reliant on this whole host of material, political and social conditions (Austin, 1962, cited in Pereira, 2019). This project therefore means to interrogate the actual conditions of this performativity through its later analysis of the different kinds of (competitive, collaborative, configurational) boundary work.

However, not all boundary work is successful, and not all boundaries are stabilised to the same degree. This is where it is useful to be able to triangulate between practice, discourse and materiality. If boundary work is evident at the level of rhetorical strategies and expressions (a methodological point I will return to shortly), and those expressions draw upon historically resonant discursive reference points, the position of the speakers and the salience of their efforts are also shaped by institutionalised practices and technologies. Not only are some actors positioned more readily to mobilise resources in their boundary work (Pereira, 2019), what these actors see and advocate for is shaped by their cultural context and organisational setting. Thus, while Gieryn emphasised the ideological motivations of boundary work, this may not always be intentional and strategic, and not always in the control of 'insiders,' but may instead be habitual or ingrained in organisational practices (e.g. Bourdieu, 1980, 2014).

While initially this description of boundary work appears to have parallels to approaches that focus on bureaucratic politics (Weldes, 1998; Halperin and Clapp, 2007), there are some important differences in the ways that boundaries are conceptualised by this project in terms of the role that materiality and practices play beyond strategic intentional actions. Boundaries are enacted through practice, and this relationship between understanding and practice is continual, reciprocal and constitutive (Pretorius, 2008). Boundaries may also be enacted or performed through technologies and programs – that is, technologies can be the platforms that shape possible political behaviours as much as they offer particular pathways or affordances (Hutchby, 2001; Srnicek, 2013). As a result, the concretised, organisational and institutional arrangements can help shape and lend durability to some boundary work. At times, it may even give some boundary work a sense of path dependency. For example, if actors treat cyberspace as a warfighting domain, that is how they will organise their response to it, which further engrains those habits of thought and practice. However, while boundary work may draw upon and shape these technological materials, it can also 'butt up against' the material (im)possibilities of some material formations and technologies, illustrating how the sociocultural

[2] As Andrew Feenberg points out, "Concretizations construct alliances among the actors whose various demands are materialized in a single object. That object operates across the boundaries of different social groups, each interpreting it in accordance with its own conception of its needs, each incorporating it into its own world." (in Felt *et al.*, 2017, p. 653)

capital that some actors are able to mobilise in their efforts are not the only factors that may determine the stabilisation or acceptance of their boundary work.

More than just rhetorical strategies then, boundary work can always be potentially performative in the sense that it can be constitutive of particular socio-technical arrangements (Barad, 1998) and in so far that it can make various institutional arrangements stick or cohere and reproduce. Cybersecurity politics (and its attendant contestations over specific readings of 'cyberspace') thus offer valuable insights into how "the material world [simultaneously] derives meaning from culture and performs culture" (Hecht, 2009, p. 11). In this sense, 'cybersecurity' and 'cyberspace' are not just technical 'things' but are indicative of the ways in which people, practices, materiality and culture mutually co-constitute one another. Each of these emerge at the point of political and cultural processes of meaning-making. In other words, cybersecurity is emergent at the point of these iterative process of boundary work. It is not a singular object or thing, but dependent upon the context, the speaker, the practices at any given time.

So far, this chapter has outlined some basic presuppositions. Firstly, boundaries between technology and science, society and politics are culturally meaningful. How those boundaries are drawn or mobilised works to materialise cultural anxieties about vulnerability and insecurity stemming from reliance on complex and ubiquitous networked communication technologies. Secondly, technology's relationship with society is not deterministic, but is co-constructed and iterative, mutually informing and producing each other. The discussion so far has also helped to foreshadow what boundaries may be made of, and the extent to which they can be said to be (re)constituted. The constructivist approach being proposed here is therefore concerned with tracing the distinctions that constitute these boundaries, and the work of producing and reproducing those distinctions (Crotty, 1998). The thesis will supplement this framing with an explicit examination of how materiality is enrolled into and constitutive of these narratives (Hecht and Edwards, 2007). As the next section will illustrate, boundary work, when viewed as a cultural practice (as both a culturally-shaped practice and the enactment of culture, in a reciprocating, iterative, emergent manner) can also help us show the productive role that boundary work may play in constituting security imaginaries.

2.2.3 Boundary work and security

Earlier, we saw how the United States is one of the foremost nation states articulating a strategic use of cyberspace and cybersecurity in their official security discourses. However, as the introductory chapter before this laid out, the question of what counts as 'cybersecurity,' and how it is practised by state actors in the US is still being negotiated. To make representations of insecurity meaningful security actors must necessarily draw on a set of shared points of reference. Thus, official

representations of 'cyberspace' frequently invoke the ways that it challenges, or bypasses, categorical boundaries and escapes established categories of thought and practice. These articulations draw on a range of ideas and concepts that already have some cultural significance and meaning.

Later, we will see how actors variously invoke and constitute historically resonant distinctions that are thought to distinguish: peacetime from wartime activities, domestic from external security responsibilities, and public and state roles from those of private or corporate actors. Such boundary distinctions serve as 'codes of intelligibility' (Weldes et al., 1999): typically referenced by people and state actors to situate the challenges said to be posed by networked and digital technologies partly to impose some order on the emergent complexity of networked communications technologies, but also to stake organisational claims and contest the credibility of respective roles and strategies.

Boundary work in the sense developed in this thesis has useful parallels with Nick Srnicek's framework of 'cognitive mapping,' or James Scott's work on legibility constituting a central aspect of statecraft (Scott, 1998; Srnicek, 2013). It thus emerges at the point of efforts by actors struggling to make sense of how to organise governance practices, struggles which are themselves shaped by a mental and cultural schema of 'the state': invoking the category of 'the state' triggers pre-existing security and social imaginaries of what the state is and how it relates to other objects and actors (Pretorius, 2008; Mayrl and Quinn, 2016). Boundary work is a form of making society, cyberspace, and cybersecurity legible in ways amenable to state governance.

Boundary work is continual, processual and emergent, but as part of these state efforts to make cybersecurity legible, it also plays a constitutive role in producing security imaginaries. In this way we can begin to identify the parallels between boundary work as a cultural practice, discussed earlier, and the role that cybersecurity politics are playing in drawing upon but also (re)constituting those ideas and beliefs about the state as a security actor. Following these ideas, we might say that historically resonant ideas about the traditional place of the state as the main provider of security can provide the basis for the boundary work undertaken in the context of cybersecurity. Different actors involved in the practice of cybersecurity mobilise particular imaginaries, symbolic boundaries and shared ideas of the state's traditional role as security provider to contextualise their own behaviours and to stake out legitimate roles for different actors in producing cybersecurity. State actors and private sector actors are amongst those who undertake boundary work to find ways of cooperating and staking a space in the blurry areas between state and non-state cybersecurity responsibilities.

Viewing boundary work as a key constituent in the messy and historically contingent processes by which state and non-state actors situate themselves in the context of 'cybersecurity' can also help us examine the processes by which such boundaries are produced. In this sense, boundary work is one of the 'nitty-gritty' political processes of sense and meaning making, or as was argued in

the previous chapter, one of the "mechanisms and processes that enable [cybersecurity's] continued assembled existence" (Stevens, 2016, p. 33). 'Cybersecurity,' viewed through the analytical lens of boundary work, can thus be regarded as a site of techno-political negotiations and contestation over these tensions and the position and legitimacy of the actors articulating these narratives and imaginaries. In this way, boundary work as a descriptive and explanatory framework complements Kim and Jasanoff's articulation of imaginaries as "the performative dimensions of a society's self-reproduction" (Jasanoff, 2015, p. 6). Boundary work is thus a performative dimension of these security imaginaries.

Each of the chapters that follow start with a vision of insecurity. Whether it be a military strategic imaginary of (cyber)security, or DHS imaginaries of ecosystems, or administration imaginaries of limited disclosures, or liberal civil society imaginaries of cybersecurity for individual rights, or corporate imaginaries of cybersecurity for intellectual property rights, the chapters that follow (and society more broadly) contain multiple visions and conceptualisations of cyber (in)security. Like a 'script' or a 'frame' in other contexts (Rein and Schön, 1996; Jasanoff, 2005), imaginaries of insecurity can work to foster demand for frameworks that can be used for guiding change, directing policy attention and resources (Pfotenhauer and Jasanoff, 2017). Articulating a vision of insecurity makes some actions politically possible or imaginable. The security imaginaries concept draws our attention to how the world is consequentially envisioned in particular ways, at particular times, by actors who have the capacity to actualise these ideas (Smith, 2009). Unlike frames or scripts, these are distinctly future-oriented practices, and are rarely singular: a focus on 'futures' in the plural reflects the processes of contention and dissent involved in the different ways that cybersecurity is envisaged in the chapters that follow. As part of the project's counter to technologically determinist narratives, this pluralist stance recognises the ways that multiple actors across multiple levels and spaces are involved in making and remaking, producing and reproducing such security imaginaries (Delina and Janetos, 2018). The concept of boundary work discussed so far has already alluded to the importance of the resources that actors can mobilise in support of the goals. We will see later how not all actors are equally capable of articulating and realising those goals.

This project therefore contends that security imaginaries are shaped by boundary work, and boundary work is shaped by (security) imaginaries. As the discussion of culture and boundary work alluded to above, while imaginaries are distinctively future-oriented, they are also a product of, and constrained by, historically produced cultural, technical, scientific or political conditions and historically resonant cultural and symbolic boundaries (Smith, 2009). Certain ideas, security frameworks, metaphors and boundaries can thus present "historical echoes in the present" in the words of Douglas Porter (cited in Smith, 2009, p. 478). By turning to security imaginaries in this way, we can critically examine the ways that competing imaginaries by different actors are bound up with

hopes for the future as much as they are "bound up with the hard stuff of past achievements" including material infrastructures, networked communications technologies, the security state, or the "normative infrastructures" of legal precedence, constitutional principles and political structures (Jasanoff, 2015, p. 22). By examining how particular imaginaries emerged or prevailed, the project is able to critically examine how these visions or projects (how treating cyberspace as a warfighting domain, or as a matter of risk assessments, or as a matter of exploiting software vulnerabilities) came to be understood as the best, or most suitable, or most 'natural,' even while appearing apolitical or value neutral.

In the case of this project, it is important to differentiate between two distinct elements to the conceptualisation here of boundary work. The discussion so far has argued that first of all, boundary work can serve as an analytic concept, that it has descriptive and explanatory power. Then, it has outlined how boundary work should also be understood as a constitutive reservoir for power and action, a rhetorical strategy as well as a performative and concretised element of state making. The question then becomes a practical or methodological one. How do we recognise boundary work? How do we identify it, in what ways can we show that it is more than instrumental rhetorical strategy? What are its components, and how can we be sure that we are not performing our own versions of methodological auditing and boundary work? In the following section, the chapter will provide an account of what this analytic framework looks like in research practice.

2.3 A methodology informed by 'STS' and boundary work.

As the thesis has discussed so far, while there appears to be a consensus amongst security actors that cyberspace is a significant matter of national and homeland security concern for the United States, agreeing upon its operational, procedural, and political bounds has been an animating feature of cybersecurity politics. Boundary work is characterised by (and surfaces most clearly at) moments of contest and competition over resources, authority and legitimacy, often triggered by moments of technological disruption or breakdown. Throughout the materials studied for this project, it was possible to trace ruptures in these discourses and points of contestation. As later chapters will show, these are moments where previously 'invisible' or uncontroversial rules, distinctions and technological artefacts have become the focus for political debate (Dunn Cavelty and Wenger, 2020). This thesis argues that this boundary work reflects the efforts of security actors to draw the bounds of cybersecurity to reflect, defend and extend their own organisational and symbolic boundaries.

These moments are when boundary work become particularly visible to the researcher. It is a key process by which participants make claims about the stakes and strategies involved, and by which they contest the weaknesses and resources of their opponents, drawing and redrawing distinctions to

do so. Pinch and Leuenberger (2006, p. 2) have suggested that such sites of contestation can facilitate an investigation of "the metaphors, assumptions and political struggles embedded within science and technology." Each of the chapters that follow therefore contain illustrative case studies (Law, 2017) that exemplify moments of contestation in cybersecurity politics during which consequential political distinctions, metaphors and assumptions are problematised by actors. Investigations of the relations between science or technology and society in STS have a long history of using case studies as a way of gaining insights into much broader patterns of culturally-specific relations between structure and agency, technologies and people (Sismondo, 2010; Law, 2017). Though the use of case studies tend to be of an ethnographic kind in STS, their use there is intended to emphasise the diversity of science and technology, thereby showing the variation across those cases as a demonstration that there is no single way of making knowledge or no universal meaning of a technology (Beaulieu et al 2007; Wyatt and Balmer, 2007; Law, 2008), an approach this project seeks to replicate. By no means exhaustive, each of the chapters coalesce around themes drawn from official discourses and programs, where distinctions such as 'public and private', 'domestic' and 'external' security, 'secrecy and disclosure' and 'wartime and peacetime' are invoked as framing mechanisms, boundaries that are said to be reconfigured or in need of policing in cybersecurity politics. Illustrative case studies, of the sort that structure each of the following chapters, are thus part of the project's overall strategy of de-essentialising state-centric (cyber)security discourses, showcasing the iterative processes of meaning-making involved in producing those narratives.

Such distinctions do not represent ontological categories: they are the product of negotiation, contestation, and institutionalisation. Connections between meanings and legitimacy require articulation and interpellation, what Muppidi (1999, p. 126) refers to as "the politics of meaning fixing." This thesis argues that efforts to 'fix' the bounds of cybersecurity through boundary work are demonstrative of these kinds of politics, whereby actors struggle to impose their own meanings. Rather than taking it to be a self-evident entity, we can and should study how actors are linking boundaries (such as 'internal,' 'external' security; 'public,' 'private') into things designated 'cybersecurity.'

Boundary work is a central strategy for convincing audiences of the legitimacy of a speaker's position, and for making some positions more credible or durable as 'facts.' These efforts can be both tacit or instrumental, depending on the context and the speaker. It is therefore important to reflect critically on the reasons why actors may take the positions they do, given the impossibility of resolving controversies by simple reference to the 'facts' at hand (Rip, 1986; Walters, 2014). For example, actors who have pre-existing credibility within a certain realm may monopolise their authority by correlating an issue to areas that they already control, leveraging their authority in one area to expand it into

another (Gieryn, 1995, pp. 424, 429). Referencing concepts such as 'national security' is one strategy for making a claim appear more central to key traditions (Sismondo, 2010).

In addition, because boundary work is most visible at moments of contestation, this points to how incomplete such processes are. These boundaries are a work-in-progress. This is a critical point: because category distinctions such as 'public' and 'private,' or 'internal' and 'external,' need constant maintenance and patrolling by the actors involved, this is evidence of their incompleteness and that they can be contested too (Jones, 2009). As Jones highlighted, boundaries must be constantly "re-fixed and re-iterated" to reify the perception that they are permanent. These are ongoing social processes of fixing, or what he calls "*bounding*, because without boundaries nothing could ever be anything" (Jones, 2009, p. 180, emphasis in original). Looking for boundary work offers us a means to investigate the ways that actors in the cybersecurity discourses use broader cultural resources to help with sense-making and anticipation in this domain. Boundaries and longstanding conceptual distinctions are some of the 'prime cultural resources' in question, but so too is the concept of 'cybersecurity' constantly constructed and enacted.

As the discussion so far has laid out, the concept of boundary work is both a constituent part of these discourses and practices, but it is also an instrument by which the analysis can trace the contingent and contested processes in formulating statist readings of cybersecurity. In their review of boundary work literature, Langley et al (2019) demonstrated how varied and eclectic the methods used by boundary work researchers are. Boundary work can thus be thought of as an analytical framework and a theoretical disposition rather than a prescriptive methodology or methods. The discussion will now therefore outline the methodological points that follow this project's reading of boundary work.

2.4 Methodology, sources and sites

Between the empirical complexity and the political stakes involved in articulating 'cybersecurity' as a matter of concern, boundary work offers a window into these ongoing processes of meaning making: a critical tool that directs us to identify moments where we can trace the ambiguities and fissures in the discourses and practices that constitute cybersecurity. Such an approach does not mean to advocate for a particular change or specific political outcome, but rather means to demonstrate existing cracks in the discourses and practices, to show their contingency and the potential for thinking and acting differently. The challenge is therefore to develop a method that allows for an engagement with the people, places and things through which cybersecurity are constituted as such, in a context marked by the increasing prominence of military and state involvement in constituting cyberspace as a thing to be secured.

My aim[3] was therefore to develop an analysis that could expose the "ambiguities, incoherence or cracks" (Squire, 2013, p. 56) in cybersecurity discourses and practices, to de-essentialise them without losing the rigour and precision needed for a critical project of cutting into statist efforts of 'bounding' and enacting cybersecurity. However, my data collection did not start out with the boundary work framework already in mind. To begin with, my research and gathering of sources was preoccupied with trying to define cyberspace because this appeared to be at the heart of the contention in defining cybersecurity practices and responsibilities. I collected congressional hearing transcripts with 'cyber' in the title, I sought out investigative reporting and books on matters related to cyber, I trawled through current affairs and technical magazine reports on cybersecurity and the latest developments. My academic literature review was substantial, but like my efforts at pinning down how political actors and professionals were defining cybersecurity, academic literatures were no more definitive in helping me to pin its essential characteristics.

My object of concern, cybersecurity, thus seemed to be 'essentially contested' (Baldwin, 1997), whilst also containing incommensurate elements or concepts. To begin with, this made me question my methods. I must have been missing something, or not applying my analysis in a rigorous enough manner. All of the sources that I collected, all of the empirical evidence, only left me feeling more dazzled and overwhelmed by the complexity, detail, and contradictions before me. How could I practically study cybersecurity, something that was predicated upon securing something (cyberspace) that was declared simultaneously a technological set of processes, a metaphor, a domain, a physical infrastructure, a cultural artefact and a product of discursive representations, or even just 'made up'? Further, how could I realistically hope to capture the technological processes that by their nature happen at levels beyond human cognition? These same complexities and combinations of technological and social elements motivated the literature, as much as it did the actors in the empirical sources I was gathering.

My methodological difficulties therefore seemed to be reflecting a sign of difficulty in the real world. As we shall see in the next chapters, cybersecurity debates suggest that the challenges posed by cyberspace would be better fixed, and better dealt with or addressed, if the space could just be better mapped, itemised, and quantified, or if the technologies could just be more carefully integrated, if the lines of responsibility could just be more clearly defined in this space, if its boundaries could more clearly be related to existing structures. In other words, if cyberspace could just be *bounded*. This kind of view is more or less implicit in the whole range of statements, debates, quotes and coverage that made up my empirical data. This is not just a matter of representation, of a

[3] This section takes the form of a first-person account because I want it to serve as a reflexive account of the methodology, as a means to reflect on my active participation in producing the analytic framework and to make the rationale for the choice of my chosen methods explicit too (Braun and Clarke, 2019).

correspondence between the representations and the thing to be secured. To put it another way, for the actors regularly using the terms cyberspace and cybersecurity, these are real 'things', even if they disagree exactly what they are or how to define them. With a closer look at the discursive and cultural patterns framing these technologies we can trace processes of actors trying to negotiate with competing and sometimes incommensurate frames of reference.

Given the complexity and political contestation surrounding cybersecurity, I did not want my methodology to reflect positivist or reductionist scientistic commitments. Instead, I approached the data in an inductive manner. Boyd-Barrett (2006, p. 22) argues that 'national cultures' are "representations 'constructed' by state agencies, social elites and media" and are therefore detectable in public records. These representations from public records therefore form the basis for the analysis contained hereafter. The raw research materials of US cybersecurity politics are analysable and represented in the languages of strategy and doctrinal documents, legislative hearings, policy reports, congressional records, expert testimonies, legal briefs, political speeches and the work of public intellectuals, all provide accessible and indicative resources for analysing cybersecurity politics. These formed the basis for my empirical investigations, and were the materials that I compiled to form my own corpus of materials. While these official texts tend to be biased towards the articulations of elites, the extensive grey literature and technical reports generated by industry also repaid careful study because these sources are publicly available and will be the same materials that security elites, policymakers and technical experts refer to and enrol in their representations (as Chapter Five will attest to). These sources can serve as a key barometer of the topics or issues that policymakers and the media consider relevant or are spending time debating (even whilst acknowledging their biases and political contexts) (Stevens, 2020).

As well as the global influence that the US has in cybersecurity discourses, the focus on the US was also for pragmatic methodological reasons: a lot of material is publicly accessible online, making it a potentially productive selection of material. Thus, a major rationale for the use of secondary sources and digitally available materials was because my project was aiming to understand shared processes of meaning making at the national or cultural level rather than processes undertaken by specific individuals. Compiling a large selection of publicly available data sources would give me (partial) access to those 'common-sense' or widespread framings and discourses, whilst also affording me some longitudinal and historical context. In this sense, I was *curating* my sources, rather than collecting them. Appendix 1 provides a detailed list of institutional repositories that engaged with.

However, the importance of this US case study is also in its potential for advancing some theoretical and conceptual contributions. Firstly, as in other matters of 'security' that may be essentially contested, my boundary work framework for analysing the fraught domestic political

processes of defence and security policymaking in the US may have wider generalisability. It has broader analytical purchase for understanding security policies in other national contexts, as well as its potential generalisability for investigating fraught relations amongst non-government actors involved in devising 'cybersecurity' policies and practices, such as standards organisations, civil society, infrastructure operators and corporate security firms amongst others. In this sense, this case has some conceptual and theory-building value for understanding what 'security' is or means, through a critical analysis of the specific case of 'cyber' security. Secondly, and in common with other critical constructivist security analyses, my case study selection has a specific goal: while the US may indeed have a global influence in cybersecurity discourses, the analysis that follows in the later chapter shows that these discourses may not be as hegemonic as they first appear. It is precisely because the US appears so powerful and the discourses so seemingly totalising that I have chosen to analyse their cybersecurity politics through the lens of boundary work, to show the contingency of even the most seemingly materially powerful military and intelligence agencies.

With all of this empirical data to process, it then became a matter of unpicking the complexity, of finding ways of telling the story at hand. To begin with, I conducted a form of 'reflexive thematic analysis' (Clarke et al., 2015; Braun et al., 2017; Braun and Clarke, 2019). Having collected thousands of documents, reports, hearing transcripts, media reports, grey literature and official policy documents, I then tried inductively reading those documents and coding broad themes with NVivo software. As I worked my way through all the empirical data that I had been able to collect entirely via cyberspace – fitting, given the subject matter – I began to see sets of themes and boundaries repeatedly rehearsed and problematised in the debates. These sets of boundaries (which form the themes discussed in the empirical chapters to follow) happened to resonate with other sets of boundaries that are amplified and rehearsed in my own "theoretical hinterlands" (Law, 2004, p. 111). Law's discussion of theoretical hinterlands echoes Braun and Clarke's suggestion that these themes do not lie passively 'in' the data waiting to be retrieved by the researcher: they are creative and interpretive stories about the data "produced at the intersection of the researcher's theoretical assumptions, their analytic resources and skill, and the data themselves" (2019, p. 594), hence my desire to use this chapter to critically reflect on these processes.

In other words, the data began to resonate with the political sciences, sociology and security studies theories that I was trained in and that themselves had long studied these consequential categorical distinctions of public and private, domestic and external security, peacetime and wartime and secrecy and disclosure. While the literature has provided some valuable insights into the production of such binaries, I will not spend much time reviewing them as they relate to each chapter as they often start from different epistemological assumptions about these distinctions. As the discussion in this chapter has already detailed, this thesis is investigating how cybersecurity politics

are informing national cultures and vice versa, and it does not want to reify the boundaries it is investigating as though they are elemental categories. Rather than taking the public and private as organising categories in international relations for example, Chapter Five will draw out the productive and constitutive effects that invocations and performance of these boundaries can have.

After this initial inductive review of the data I had so far curated, the analytic method of boundary work offered a productive approach that would go beyond formal techniques of discourse analysis, because it offered a more interpretive means of identifying the symbolic, linguistic and material elements that are crucial to the production of recurrent themes, tropes and national identity politics (Evans *et al.*, 2020). Once these patterns began to resonate, I was then able to find additional empirical material that could be understood as further repetitions of these same patterns, becoming progressively easier to navigate the overwhelming detail before me. I recognise this necessarily means that I have left a lot out and under-represented those elements of the state debates that do not fit the patterns. The cases chosen for each of the chapters in this thesis are insufficient to capture every aspect of a messy and complex world of technological relations. For example, once I had started analysing my data through the lens of boundary work, I had initially wanted to develop a line of critique about distinctions constantly referenced in discourses from the early 2000s between 'virtual' cyberspace and 'real' materiality. However, as I questioned and queried the assumptions I was making in interpreting and coding the data (Braun and Clarke, 2019), this was a thematic line I ended up abandoning because it was not a theme that animated the more recent debates, morphing instead into the debates discussed in Chapter Four. Thus, while it makes no claims to being a comprehensive account of all the boundaries animating cybersecurity politics, this project shows how focusing on the moments of contention that animate each empirical chapter works to capture some snapshots into a constantly developing situation.

At the same time however, studying contemporary security contexts poses its own methodological challenges, given the secrecy that so frequently obscures the 'facts of the matter' (Walters, 2014; Kearns, 2017). Instead, these apparent difficulties acted as a methodological strategy in their own right for this project. In the chapter oriented around boundaries of disclosure for example, rather than striving for the 'truth' or the transparency of official revelations, the choices about what actors do and do not disclose was taken as an indication of salient political struggles and representations in action. Put another way, this chapter studies how actors talked about what they weren't talking about. While a range of questions arise from drawing attention to "the material context in which certain security practices become possible" (Lundborg and Vaughan-Williams, 2015, p. 15), through the framework outlined in this project we can also investigate how otherwise silent or invisible actors and things become visible at particular times and places. Once I had collected the empirical data, the analytical approach as I have outlined so far meant asking certain kinds of

questions of the material. Dunn Cavelty (2018) has cogently highlighted the analytical insights available from approaches that can interrogate why some technologies trigger political debate or popular attention, whilst others stay in the background, uncontested or invisible. The interesting critical point is not to simply focus on how particular incidents came to pass at the technical level, but rather to ask how the intangible or invisible workings of these technologies get "made thingy" (Rankin, 2014, p. 664) at specific times and places.

Despite the secrecy that ostensibly covers these contexts, and the difficulties posed by restricted access, by asking these kinds of question the analysis can capture the dynamics that are helping to constitute cybersecurity in specific relational ways. Rather than taking cybersecurity as a singular object then, 'obscured' by secrecy, tracing the ways that people, practices and materials are arranged and mobilised at different times can help us attune to the complexity while also scrutinising the efforts required by different actors to produce the cyberspace and approaches to cybersecurity in question (Law and Singleton, 2005). After all, this project contends that what cybersecurity *is* depends on the boundaries drawn and the motivations of the actors.

The boundaries articulated here are not always explicit: nor are the statements available in public necessarily going to resonate easily with my boundary framing. An extra layer of interpretation was therefore required to make broader sense of the boundaries being articulated in cybersecurity politics, to contextualise their history and cultural significance, something provided by the concept of security imaginaries (Pretorius, 2008; Jasanoff and Kim, 2009, 2015; McNeil *et al.*, 2017). While primary sources such as policy documents, strategy statements and the statements made by officials give us an insight into perceptions of the security world and the instrumental or rhetorical strategies at work, they take place in a much wider cultural background that also need to be incorporated into the analysis (Pretorius, 2008). State actors are not the only groups articulating the national culture and imaginaries that animate cybersecurity politics. Jasanoff has suggested more recently that such imaginaries are not confined to nation-states or their official representatives, they can also be expressed by organised groups including companies, professional groups and social movements (Jasanoff, 2015, p. 5). A cultural approach to security imaginaries therefore necessitates a wide selection and range of sources beyond official policy documents and statements, something borne out in the proceeding chapters.

In each of the chapters we will see competing visions of desirable futures, centred around varied articulations of security for whom, what, and how, with many different actors involved in articulating those imaginaries. Multiple imaginaries of desirable technological futures can thus be at work in any one context, thus highlighting that moments of contention – and reflecting on the social positions of those articulating those counter narratives – can offer a window into these processes

(Jasanoff and Kim, 2009; Smith, 2009). As such, this is another rationale for my focus on ongoing processes of contestation, quarrelling, competition for resources and in-fighting amongst different government agencies, as much as debates with those outside of government, rather than isolated controversies.

In parallel to the conception discussed earlier in this chapter of the ways that boundaries are materialised or concretised, these imaginaries can also be 'locked in' by the material commitments, funding decisions, and policy priorities of different agencies and institutions (Mikami, 2014, cited in McNeil *et al.*, 2017). The organisations, institutions, buildings, programs and initiatives that enact cybersecurity are also 'readable' like documents and discourses in this sense, available to us at sites where the enactment of cybersecurity are made 'durable.' I therefore looked at the emergence of cybersecurity policies in the US as one way to gauge the relationship between the imaginaries and policy outcomes. Many studies in security analyse rhetoric and metaphors and have shown how discourses construct meanings, so that interpretive social repertoires are formed in media, policy and science. These repertoires shape conceptions of what technologies are supposed to be, and how they are thought to be legitimately governed (Konrad *et al.*, 2017). However, a lot of the analysis in the chapters that follow also focus on localised programs or initiatives, to unpack them as evidence of acts of investment and statements revealing commitments to particular futures (Borup *et al.*, 2006). Each of my chapters analyses how these kinds of questions – 'how far does it go' (Chapter Three), 'who does cybersecurity belong to' (Chapter Four), 'who is cybersecurity for' (Chapter Five), and 'what does cybersecurity mean' (Chapter Six) – are questions that are implicitly reflecting but also shaping visions of the future. The policies, programs and initiatives that follow are indirect materialised assessments of emerging technologies and desirable futures. Collective expectations can be expressed and traced in strategic discourse, but they are also materialised through investments in particular technologies or policies or programs. When these programs are analysed as statements about future development or conditions, we can thus start to understand the expectations and assumptions animating those programs (Konrad *et al.*, 2017) and the imaginaries that are embodied by such cybersecurity programs.

This is where my narrative account becomes important. Actors in the stories compare with "somewhere and somewhen" in formulating their responses to the matters at hand (Jasanoff, 2015, p. 24). It is up to me as the researcher to draw out and demonstrate the comparisons across time and across policy sectors to help demonstrate the moments of contestation and coherence, and the analysis that follows draws out patterns in temporal and spatial comparisons. I therefore adapt a case-study and narrative style in the chapters to draw out these moments and show how they have changed over time and across the broader trajectory of cybersecurity politics over the last thirty years. As Abbott (1995) urged above, mine is not an essentialist account of boundaries, but a narrative about how actors are using boundaries to make (sense of) entities or concepts.

Boundary work thus offers a valuable heuristic for exploring the work and effort that goes into keeping objects (like cybersecurity and statist readings of 'cyberspace') relationally stable (Law and Singleton, 2005). This project is about studying how actors 'gather' these different realities, how they tell stories to make it cohere (Law, 2004). These are the detailed political processes that go into producing categorical distinctions of 'state,' 'public' and 'private,' 'internal' and 'external' security, 'peacetime' and 'wartime' and 'disclosure.' Rather than taking cybersecurity as a singular object then, these case studies will show the messy, contingent, fraught processes of negotiation, enrolment, persuasion, and contestation involved in actualising different security imaginaries and different characteristics of cybersecurity that are articulated in support of those imaginaries. Using the sensitising heuristic and analytical technique of boundary work to guide analysis of official statements, policy documents, congressional testimony and media coverage, this thesis will investigate how cyberspace and cybersecurity are constructed and contested, and how state actors are continuing to articulate and perform 'the state's relationship with cyberspace. As a first step in this direction, the next chapter will now tell a story of how military (cyber)security imaginaries have played an important and constitutive role in shaping cybersecurity imaginaries of the United States.

Chapter Three: 'Two hats' and the demarcation of boundaries between peacetime and wartime cyber capabilities

3.0 Introduction

When General Paul Nakasone successfully navigated his confirmation hearing before the Senate Armed Services Committee in March of 2018, he was to be put in charge of two agencies simultaneously, much as his two predecessors had. He would be placed in command of one of the world's most well-funded signals intelligence agencies, the National Security Agency (NSA), whilst also assuming the command of the US' dedicated military cyber operations unit, Cyber Command (CYBERCOM)[4]. The arrangement for NSA and CYBERCOM to share their leadership has been in place ever since CYBERCOM was established in 2009. This had been proposed as a means for the new military command to leverage the hacking capabilities and technical infrastructure that the NSA had already developed (e.g. Lynn, 2010; US Senate, 2015d, p. 75). However, in this chapter we will see how military and intelligence actors are increasingly trying to extricate such military cyberspace capabilities from their intelligence heritage. As we shall see, phases of *collaborative* and *competitive* boundary work analysed in this chapter are about articulating conceptualisations or visions of how far cybersecurity *goes*; whether it is a matter of peacetime operations or wartime activities, and the ways that security imaginaries subsequently direct policy and funding.

This chapter will argue that the establishment of CYBERCOM and this 'dual-hat' arrangement has both triggered and emerged from boundary work concerned with demarcating long-held symbolic and procedural boundaries in US law and tradition: namely, distinctions governing peacetime and wartime activities, and between intelligence and military activities. Contrary to the widespread narratives about the "structurally and strategically driven" emergence of military cyberspace capabilities discussed in Chapter One (Fischerkeller and Harknett, 2018 n.p.), this chapter will show how the establishment of CYBERCOM demonstrates the extent to which 'cybersecurity' has also been shaped by military imaginaries and their boundary work and vice versa.[5] Instead, this chapter will

[4] He would also be in charge of the Central Security Service (CSS) and the Defence Information Systems Agency (DISA), but the label 'dual-hatted' generally acts as a shorthand to refer to the simultaneous command of NSA and CYBERCOM.

[5] In the latest edition of Joint Doctrine on cyberspace operations, the document notes that it "distinguishes between cyberspace security and cyberspace defense actions," but that these are not distinctions "made in DOD and USG cybersecurity policy, where the term cybersecurity includes the ideas of both security and defense." (US Department of Defense, 2018, p. 2.6). This also aligns with the thesis' argument that 'cybersecurity' is a broad (and contested) term.

argue that CYBERCOM's doctrine of 'persistent engagement' has emerged to play an institutional role for justifying the military command's existence, a means of demarcating themselves from their progenitors in intelligence agencies and practices, and for establishing authority and autonomy for the new command.

To substantiate this argument, this chapter will begin with an analysis of the military cybersecurity imaginary that emerged out of a combination of broader military strategic imaginaries of cyberspace on the one hand, and the technological and organisational experiences of relying on intelligence organisations to develop the military's skillsets on the other. So that a military cyber command appeared inevitable and the only rational response to 'structural and technological imperatives' and threats, in this imaginary articulations of consequential boundaries and categorical distinctions such as 'offence' and 'defence,' military and intelligence, and thresholds historically used to demarcate between 'peacetime' and 'wartime' therefore initially animated the collaborative boundary *work at* such boundaries that sought to give the NSA time and resources to develop its hacking capabilities. As we will see, the imaginary was a product of "more than a decade's worth of institutional change" that according to CYBERCOM's historian Michael Warner had "firmly linked" the DoD's "defensive and offensive capabilities" with that of the NSA (Warner, 2015, p. 133). Then in Part Two an analysis of the debates surrounding the dual-hat leadership and co-location of CYBERCOM with the NSA at Fort Meade will show that, more than just a question of technical feasibility, 'military cyber capabilities' are emerging as a result of political, instrumental and organisational contestation. The boundary work analysed in Part Two leads into the argument of Part Three, where to advocate for the autonomy of the new command, advocates for distinctively *military* cyber capabilities have undertaken competitive boundary work through initiatives and doctrine intended to *work for boundaries* that could distinguish the command from its tools and cultural progenitors in the intelligence community, exemplified by the emergence of the doctrine of 'persistent engagement.'

Overall, the chapter finds that efforts to defend and extend organisational boundaries have shaped technological capabilities as much as technological capabilities have shaped organisational boundaries, with the result that at a tactical and technical level, the DoD has expanded the range of permissible military activities below the threshold of war. The bounds of 'cybersecurity' have thus been expanded to legitimise and institutionalise military action beyond DoD networks. First though, the chapter will critically analyse how the military's imaginary of insecurity was articulated so that CYBERCOM became the political and practical solution.

3.1 Part One: Military imaginaries of (cyber) insecurity

In this section we will see how advocates for increased military cyber capabilities (and its associated allocation of resources) gradually produced a shift in the ways that cyberspace and cybersecurity were understood, imagined and implemented as a specific kind of problem space – or 'domain' – that the military could and should play a role in. The imaginary was both a product of, and a condition for, the establishment of the new unified military command. Though its roots can be traced back to the 1970s (Gray, 2006; Metz, 2006), over the course of some ten years starting in the late nineties, military strategy documents and vision statements solidified this imaginary of cyberspace and the military's role in 'cybersecurity,' thereby working to simultaneously inform and direct subsequent policy and funding priorities and organisational initiatives. As this section will show, the analytic concept of a military (cyber)security imaginary emerged from broader military and strategic imaginaries but developed in tandem with organisational and technological developments at the NSA. Though this concept articulated the rationales for the military's computer network operation capabilities in terms of 'structural and strategic imperatives,' Part One will demonstrate the boundary work embodied in but also triggered by the development of this military (cyber)security imaginary. In turn, as also discussed below, this would have important consequences for the doctrine and organisations that emerged later.

3.1.1 A genealogy of the military (cyber) imaginary

The story of the military (cyber)security imaginary began by security actors establishing that the American nation was confronted by daunting challenges and vulnerabilities arising out of the 'Information Age.' This narrative would emphasise that in order to fulfil its traditional mission of 'defense of the Nation' (Chairman of the Joint Chiefs of Staff, 2000, 2006), the military would need to undertake rapid and fundamental innovation and 'transformations,' hailing specific characteristics thought to be inherent to the technological environment. According to this narrative, the military was having to develop new concepts and capacities for coping with broader technological changes brought on by networked communication technologies. As a formative document in articulating this vision of the future, the *Joint Vision 2020* for example set out a coherent and succinct explanation of how military leaders thought conflict would evolve in the light of new technologies, articulating a vision for directing institutional priorities in light of the 'Revolution in Military Affairs' and America's strategic context at the turn of the millennium (Chairman of the Joint Chiefs of Staff, 2000; Czelusta, 2008). Citing "the ongoing information revolution," this document argued that technological change in the "information environment" would create not only profound quantitative but also qualitative changes in the conduct of military operations by 2020, necessitating new ideas, operational concepts and

capacities (Chairman of the Joint Chiefs of Staff, 2000, p. 61). To achieve the "overarching focus of this vision" of "full spectrum dominance," so the logic went, the "pace of technological change, especially as it fuels changes in the strategic environment" was a situation that required "infusion of new technology and modernization and replacement of equipment." (Chairman of the Joint Chiefs of Staff, 2000, p. 60). While this was never intended as a concrete policy document, the framing here of the operating environment would pave the way for the subsequent strategy documents that were intended to direct the development of specific initiatives.

It is possible to trace a narrative thread running through the vision documents and strategic declarations outlining collective 'visions' of the future that the military, and by extension the nation, was thought to be facing. As the 2006 National Military Strategy for Cyberspace described the matter, this US was now operating in "a global environment characterized by interdependence, uncertainty, complexity, and continual change" where cyberspace was both crucial to "the prosperity and security of our Nation" as much as it was a source of continuing vulnerability from adversary actions and systemic breakdowns (Chairman of the Joint Chiefs of Staff, 2006, p. 1). This narrative thread was still present by 2010, where one pamphlet by the Army Training and Doctrine Command explained in a section entitled 'Framing the Problem' that the…

> …operational environment (OE) has changed dramatically. The technologic convergence of computer and telecommunication networks; astonishing rates of technologic advancements; global proliferation of information and communications technology (ICT) and its consequent effect in social networks and in society impact the OE" (US Army, 2010, p. iii)

This "technological revolution" represented "a condition of perpetual turbulence without traditional end states or resolution," with profound effects on traditional military doctrinal frameworks (US Army, 2010, p. iii). At the core of the military imaginary of cyber insecurity then was the belief that faced with a global environment and a future of "interdependence, uncertainty, complexity, and continual change" (Chairman of the Joint Chiefs of Staff, 2006, p. 1), the challenges posed by cyberspace would therefore require specific solutions.

A stated desire to develop 'information operations' as a "core military competency" (US Department of Defense, 2003) therefore developed out of a specific conceptualisation of the information environment and a broader doctrine of 'military transformation,' championed by the likes of Secretary of Defense Donald Rumsfeld and the Bush administration (Czelusta, 2008). In the context of this broader vision, the oversight panel for the 2003 *Information Operations Roadmap* were charged with developing a "concrete set of action recommendations" in which they set out the DoD's vision and 'roadmap' for developing the military's nascent capabilities for computer network operations into a "robust warfighting capability" and 'core competency' (US Department of Defense,

2003, p. 7). This document was animated by just three 'key assumptions' and programme priorities, one of which was that networked 'C4ISR' (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) was envisaged as a "critical enabler to transform the forces" in an "increasingly transparent battlespace" (US Department of Defense, 2003, p. 4). While these visions were hailing the transformational capacity of military capabilities for information operations, they also articulated a recognition of the increased vulnerability that came from reliance on networked 'C4ISR.' These capabilities were therefore envisaged as a fundamental prerequisite for transforming the forces to keep up with (as much as produce) a changing battlespace. So long as the recommendations in the report were "aggressively implemented" it was argued that this would lead to several "enhanced capabilities for the warfighter" including "the protection of networks with real defense in depth strategy," and a "robust offensive suite of capabilities to include full-range electronic and computer network attack" (US Department of Defense, 2003, p. 7). In sum, the 2003 Roadmap was directing the development and consolidation of hacking capabilities (amongst others) that they felt the military were lacking and which the military's future was dependent upon. Thus, while the 2003 Roadmap set out the vision of the future and the intention of developing these capabilities, the process for achieving that vision would require more than a program of acquisitions.

Having made a case for the 'necessity' of information operations capabilities in response to an information revolution, the challenge was to establish the extent to which these capabilities could fit into extant military organisational structures and legal remits, and how the military would have to transform to accommodate them. Invoking a long history of the United States' reliance on technological innovation "throughout the industrial age" in order to "succeed in military operations," the innovations that would be required of the military to remain effective were more than just technological: this shift would require both organizational and conceptual innovation too (Chairman of the Joint Chiefs of Staff, 2000, p. 62). "[A]dvances in information capabilities" were envisaged as "proceeding so rapidly that there [was] a risk of outstripping our ability to capture ideas, formulate operational concepts, and develop the capacity to assess results." (Chairman of the Joint Chiefs of Staff, 2000, p. 61). Military actors needed new operational concepts and orienting frameworks to deal with these changes.

The military cybersecurity imaginary thus emerged in the context of broader conceptual and strategic articulations of transformation. A formative element of this conceptual shift was seeded in 2004. As part of his remit for realising this transformative doctrine, and described as the 'godfather' of 'network centric warfare' concepts, while he was Director of the Office of Force Transformation in the DoD Admiral Arthur Cebrowski propagated the idea for treating cyberspace as a global domain akin to the sea and air in an article entitled 'Transformation and the Changing Character of War' (Cebrowski, 2004; Metz, 2006). As we shall see later, conceptualising the operational environment as

a ‘domain’ would eventually become an ‘intuitive’ framing for those in an American military culture, and it would help shape the policies and initiatives that followed. At this stage, ‘Information Operations’ was an umbrella term that incorporated ‘computer network operations’ alongside other conceptual components such psychological operations and communications security. As time passed though, this framework would gradually disaggregate in doctrine and strategy statements into its component parts, so that information operations and ‘PSYOPS’ were increasingly understood as a separate entity to computer hacking and communications security.

As the next section will now show, this gradual shift in conceptual frameworks was wrapped up in the instrumental and practical work that was going into the development of computer network capabilities in the NSA.

3.1.2 Downplaying boundaries to establish military cyber capabilities

For the military to fulfil the vision it had articulated in the 2003 *Information Operations Roadmap* to develop ‘information operations’ and computer network operations into a “robust warfighting capability” and a “core military competency,” they had already recognised the facilitating role that the intelligence community, particularly those at the NSA, would have to play to make that happen (US Department of Defense, 2003, pp. 29–30). The 2003 Roadmap and the DoD therefore proposed that they would need to fully “leverage the Intelligence Community’s capabilities, including its knowledge of the threat space and access into adversary systems” (DoD historian, cited in Wiener, 2016, p. 282). These capabilities were predicated on technical knowledge and experience that the intelligence community, and NSA in particular, had been developing since the Cold War. During his tenure as Director of the NSA between 1999 and 2005, General Michael Hayden and his predecessor Ken Minihan had recognised that if the NSA was to remain relevant and funded after the Cold War, they needed to carve out a new niche for the agency (Kaplan, 2016).

To lobby Congress for the resources to develop these capabilities at the NSA, from the very earliest articulations of the need to conduct operations in cyberspace, advocates for NSA’s interests would emphasise the commonalities between the tools of the intelligence community and those the military would need. This was because, as NSA director Hayden later explicitly reflected, “U.S. law is pretty clear about the distinctions between espionage and war fighting” (Hayden, 2016, p. 136). Such historically resonant and legally constituted distinctions between espionage and war fighting were thus offered as part of the rationale for emphasising technological similarities in the tools that the NSA was developing.

By downplaying distinctions on technological grounds and working *at* boundaries, they wanted to give themselves the political space to develop hacking tools without apparently transgressing those legal and normative distinctions. A description given by the former director of the NSA from 1996 to 1999, Ken Minihan, was indicative in this regard. He was described by many sources as a formative character in the NSA's shift from passive to active signals and data collection and the development of 'computer network operations' (Kaplan, 2016; Hayden, 2016; Wiener, 2016). Minihan went so far as to describe the overall concept of computer network operations as made up of "90% CNE [computer network exploitation], 5% CNA [attack] and 5% CND [defence], *as the difference between exploitation capability and attack capability is nominal*" (cited in Wiener, 2016: 128 emphasis added).

Differentiating between 'attack' and 'exploitation' capabilities are important in this context because the differences have been embedded in US traditions governing organisational and institutional boundaries between peacetime and wartime activities. According to those distinctions, the military traditionally conducts attacks and the intelligence community traditionally does not[6], so actors were having to work out where these hacking capabilities could or should fit within those conceptual and organisational frameworks. As part of his efforts, as head of the NSA, to give his organisation the time and resources to develop the expertise and ownership of these capabilities, Hayden recognised the historical resonance and institutional importance of such distinctions when he later recounted his time at the NSA, where they apparently 'knew'…

> …that defense, exploitation and attack were technologically and operationally indistinguishable even though they were separated in legal authority, funding streams and congressional oversight – the result of putting new (digital) wine into old (eighteenth century, actually) bottles. (Hayden 2016: 142)

In other words, by working at boundaries as part of their objectives to lobby congress to generate some political and institutional space to develop these capabilities at the NSA, they were working to fit the technically indistinguishable capabilities into 'old bottles' that had long determined the separation of these different activities, downplaying such boundaries.

Downplaying such distinctions thus became a strategic practical action intended to defend the NSA's autonomy and credibility as a post-Cold War signals intelligence agency. According to Bill Black, a deputy director at the NSA after the Cold War, the NSA had undertaken a series of initiatives and reorganisations that "centered around technology" intended to establish "NSA's role as the dominant

[6] These are of course not mutually exclusive distinctions, when considering covert action and counter-intelligence, but the question here was where cyber operations could or should fit in this framework.

provider and 'understander' of that technology." (cited in Lardner, 2002, p. 19). This meant that over time, the NSA had been able to develop hacking capabilities that Hayden described later as…

> …action designed to disrupt an adversary's network or, in its most extreme form, take over the network in order to use it to create some level of physical destruction. NSA still had not authority to do that; it was limited to defending American information and stealing other people's (Hayden, 2016: 141)

Over time, the NSA built up the technology and expertise for hacking that crossed into 'some level of physical destruction,' but these capabilities exceeded their traditional remits as an intelligence agency. Having developed some of the tools and skillsets, these hacking capabilities thus needed a home. They were a "CNA function that Fort Meade could perform but didn't have legal authority to do" (Hayden 2016: 142). This is something the NSA apparently recognised early on: archival documents from the NSA from the late nineties "revealed that whatever the nature of the new phenomenon [offensive cyberspace operations], possible responses to it may not fit easily within either mission or within the legislation and regulations that defined NSA." (Nolte, 2012, p. 26). While the NSA's hacking capabilities apparently exceeded the agency's legal remit, by working *at* the boundaries of espionage and military distinctions, Hayden and others would undertake *collaborative* boundary work that would negotiate and blur those institutionalised boundaries between espionage and offense in order to coordinate the DoD's and NSA interests.

For the NSA to defend its position as the dominant 'provider and understander' of that technology, Hayden and the commander of Strategic Command (STRATCOM) would therefore come up with a mutually beneficial arrangement for both organisations. A restructuring by Secretary of Defense Donald Rumsfeld in 2002 designated STRATCOM as the unified combatant command to be responsible for developing the military's cyber capabilities, alongside its other command responsibilities for strategic deterrence, global nuclear strike capabilities and operating the DoD's Global Information Grid. However, it was the NSA that was a premier source of technical expertise for those capabilities – according to Hayden, General James Cartwright who was commander of STRATCOM at the time would therefore come to Fort Meade and talk with him often as a means of expediting this new responsibility for STRATCOM, where they apparently "agreed that he could devolve his authority and responsibility for cyber-attack to Fort Meade and dual-hat me as his action arm under the unwieldy title of commander, Joint Functional Component Command-Network Warfare (JFCC-NW)." (Hayden 2016: 142). Effectively, the Director of NSA now had the authority for both exploitation and attack activities. "The combined team at Ft. Meade would access and conduct reconnaissance of a target based on my authorities as DIRNSA [Director, NSA] and then, on order, could manipulate or destroy the target based on Cartwright exercising his combat authority through

me […] essentially offering NSA's resources to enhance DoD cyber combat power at little cost to the Services." (Hayden 2016: 142). The NSA had developed the offensive capabilities, but in order to legitimise their use, Hayden and others would have to foster specific organisational responses that moved their practice beyond the bounds of the intelligence agency through a mixture of collaborative and configurational boundary work strategies.

Reconfiguring such institutionally and organisationally engrained distinctions had taken some intentional and careful manoeuvring on the part of Hayden and his colleagues in the early days of establishing these cyber capabilities. He went on to describe how they navigated Congressional concerns:

> Our technique was to bring the members [of Congress] into our confidence and our "ask" was to give this unusual relationship of Title 10 (war making) and Title 50 (espionage) authorities a little space and time to mature before we had to explain all the fine print (a lot of which didn't exactly exist yet). What we were doing did not fit nicely into the congressional oversight structure. It blended activities, some of which were traditionally overseen by the intelligence committees and some of which were traditionally overseen by the Armed Services Committees – and nothing is as jealously guarded on the Hill as jurisdiction. (Hayden, 2016: 136)

By asking Congress to give the NSA and STRATCOM 'a little space and time to mature' and to work out how cyber operations would fit into congressional jurisdictions, this combination of collaborative and configurational boundary work would instrumentally downplay distinctions between 'defense, exploitation and attack' to give the NSA time to defend the allocation of resources to the development of these new capabilities. As an example of boundary work that saw the potential for working *through* boundaries, the alignment of NSA with STRATCOM simultaneously advanced both STRATCOM'S capabilities and NSA's authorities, to the benefit of both leaders.

Contrary to narratives discussed in the Introductory chapter and in the first section of this chapter about external structural characteristics of the technologies forcing the development of military 'cyber' capabilities then, in some important ways, the organisational and institutional development and shape of these capabilities was also the product of efforts to fit them into notions of historically resonant distinctions governing military and intelligence activities. Mixed up with broader military strategic imaginaries discussed earlier, and the organisational interests of developments within the NSA discussed here, as we shall see in the next section, the military (cyber)security imaginary shaped, and was in turn shaped by, more than just the 'technological operating environment.' By 2009 the DoD increasingly sought to set the terms by which 'cyberspace' was to be conceived of as a 'domain,' with its attendant spatial connotations as a terrain to be

maneuvered through and secured, so that the establishment of a new military cyber command would appear to be the best solution to the challenges expressed in the military (cyber)security imaginary.

3.1.3 Cyberspace 'blurs boundaries'

Eventually, the formalisation of the military's cybersecurity imaginary was triggered by, but also framed within, the articulation of an organisational 'solution' in the form of a new dedicated command to be based at Fort Meade. The arrangement to gather the military branches' disparate 'information operations' units together in one place and to physically co-locate them with the NSA was formalised by the U.S. Secretary of Defense directing the Commander of Strategic Command in 2009 to establish USCYBERCOM. CYBERCOM would be made up of service elements from the U.S. Army, Navy, Air Force and Marines, whilst being co-located in the NSA's building at Fort Meade, Maryland. The leadership of this new military command would be given to the director of the NSA. Although he was already head of the NSA, the Defense Information Systems Agency and the Central Security Service, this meant that General Keith Alexander was described as a "dual-hatted" commander of these intelligence agencies at the same time as a military organisation.

According to the narratives accompanying CYBERCOM's establishment, the challenges and vulnerabilities posed by this complex, uncertain and continually changing global environment would be expressed in terms of the ways that several conceptual, institutional, and organisational distinctions were challenged. Though by no means an exhaustive list of issues, such challenges were most often represented as three different categorical issues. Informed by the collaborative and configurational boundary work that had facilitated the development of these hacking capabilities at the NSA, these boundaries would be problematised in terms of: structurally determined 'offence-dominance;' difficulties of distinguishing between espionage and attacks; and difficulties of separating military from non-military remits. As we shall see, the difficulties of 'categorising' cyberspace operations and the military's roles and responsibilities were thus shaped by military and strategic cultures as much as they have been a product of organisational manoeuvres at the NSA. The proceeding section of the chapter will show how CYBERCOM can be understood as both a condition for, and a condition of, this imaginary, and the boundary distinctions that the imaginary invokes.

The first set of central attributes that have repeatedly been picked out in the military (cyber)security imaginary was the conviction that for "structural reasons, the U.S. government's ability to defend its networks always lags behind its adversaries' ability to exploit U.S. networks' weaknesses" (Lynn, 2010 n.p.). Hailing this asymmetry in offence and defence would underwrite calls for the military to develop new strategies. After all, the logic went, in "an offense-dominant environment, a fortress mentality will not work. The United States cannot retreat behind a Maginot Line of firewalls

or it will risk being overrun" (Lynn, 2010 n.p.). Furthermore, this was conceived of as a profoundly unstable and 'volatile' cyberspace, something that "constantly changes, [thus] making some targets transitory and defensive operations challenging." That defensive lines could no longer be drawn, that cyberspace "[t]ranscends commonly defined organizational and geopolitical borders," (Chairman of the Joint Chiefs of Staff, 2006, p. 3), presented the military imaginary with an existential threat to its own cohesion as an entity. When cyberspace was conceived of as something that "[lacks] geopolitical boundaries […] the electromagnetic spectrum allows cyberspace operations to occur rapidly nearly everywhere" (Chairman of the Joint Chiefs of Staff, 2006, p. 1), the information-age identity of the networked military was thus threatened by not being able to defend itself from the transgressions, infiltrations and incursions of adversaries into its networks. In this imaginary, they could no longer defend their cohesion or their network borders (Brunner, 2013). Conceived in such a way, this 'structural imperative' was invoked to argue that "speed and agility matter most," and to "stay ahead of its pursuers, the United States must constantly adjust and improve its defenses." (Lynn, 2010 n.p.). Such language of speed, agility and being pursued by adversaries in this way was thus invoked to signify how drawing bright distinctions between 'offense' and 'defense' was a challenge in such a 'quickly shifting terrain.'

At risk in this imaginary were ideas of American exceptionalism and military advantage: the very resources and infrastructural investments that had hitherto assured their dominance were now being cast as potential sources of vulnerability. This was part of a longer narrative arc discussed at the start of the chapter in which the period after the Cold War signified a shift and post-9/11 erosion of military power (Gray, 2006; Metz, 2006). Subsequently, this narrative arc was explicitly referenced by the authors of the 2017 National Security Strategy when they lamented that from the late nineties, Americans had taken "our political, economic, and military advantages for granted [while] other actors steadily implemented their long-term plans to challenge America and to advance agendas opposed to the United States" (VEP Charter, 2017, p. 2). As such, although the 2006 military vision document noted that "the United States currently enjoys technological advantages in cyberspace, those advantages are eroding," and this was reason to devote "significant effort" to changing its military organisation and concepts (Chairman of the Joint Chiefs of Staff, 2006, p. 9). Despite this narrative about their military advantage being eroded by the potential for adversary actions in this interconnected cyberspace, America has consistently spent as much as the next eight or even ten countries combined on defence, and its military remains the only one that can sustain global operations (Lohaus, 2018; PGPF.org, 2020). Yet, for those articulating a vision of an insecure nation and an insecure military dominance, these narratives were presented as the rationales for urgent action to naturalise the solution of a new military command that could unify the military's offensive and defensive 'cyber' capabilities.

The second set of categorical distinctions challenged in military cybersecurity imaginaries were those used to classify thresholds for military action and distinctions between espionage and attacks, and translating the ideas of 'traditional military activities' (TMA) into this context. For those describing the challenges posed by cyberspace, "… what constitutes an attack is not always clear. In fact, many of today's intrusions are closer to espionage than to acts of war." (Lynn, 2010). This was echoing the arguments that Hayden had already been making before Congress. Invoking these distinctions carried a significance because in the U.S., such distinctions are embedded in legal authorities and congressional oversight and reflected in the institutionalised activities that the military or the intelligence community can each undertake. While intelligence is conducted by military organisations, espionage is an activity that takes place during peacetime and so long as it remains covert is often normatively (if not legally) 'tolerated' internationally.[7] These difficulties were again articulated in terms of structural qualities of cyberspace - "given that information technology is evolving rapidly, policymakers are left with little historical precedent to inform their expectations," (Lynn, 2010 n.p.). Deputy Secretary of Defense Lynn was here making the case here for the necessity and appropriateness for the Pentagon to present policymakers with useful conceptual frameworks and with flexible strategic responses, and in the years that followed, boundary work to demarcate military and intelligence attributes and activities would be a recurring feature of cybersecurity politics.

The third set of categorical distinctions that have resonated throughout these debates and narratives were the difficulties of drawing distinctions between military and non-military remits and spaces. While the Joint Chiefs of Staff had described 'cyberspace' as a 'domain' of warfighting as a doctrinal matter in their 2004 National Military Strategy (subtitled "A strategy for today; a vision for tomorrow"), this document intimated the shift in conceptual approach underway, from viewing air, sea and space as "international commons" to conceiving of them as warfighting domains (U.S. Department of Defense, 2004). However, at the same time as this general shift there was a simultaneous emphasis on the difficulties of disaggregating 'military' cyberspace from other "portions" of cyberspace (Chairman of the Joint Chiefs of Staff, 2006, p. 1), something that would animate the turf battles between the DoD and other Federal agencies discussed in the next chapter. More immediately though, because cyberspace was distinctive for being a "man-made domain" and furthermore, "… [c]reated, maintained, owned and operated by public, private and government stakeholders and exist[ing] across the globe," security of these networks was not in the sole control of the military nor within national territorial bounds (Chairman of the Joint Chiefs of Staff, 2006, p. 3).

[7] As international legal scholar Richard Falk (cited in Lotrionte, 2015, p. 473) reflected, "[t]raditional international law is remarkably oblivious to the peacetime practice of espionage. Leading treatises overlook espionage altogether or contain a perfunctory paragraph that defines a spy and describes [their] hapless fate in the event of capture." (See also Navarretef and Buchaní, 2019; Georgieva, 2020)

As Arquilla and Rondfeldt had articulated in their formative 1993 RAND paper *Cyberwar is Coming*, the "rise of global information networks" would set in motion forces that would "… challenge the hierarchical design of many institutions", redrawing "… the boundaries of offices and responsibilities" and expanding the "spatial and temporal horizons that actors" would have to organise around (Arquilla and Ronfeldt, 1993, p. 26). For military actors concerned with trying to articulate how the military's roles and responsibilities could, or should, be translated into 'cyberspace,' this would prompt them to demarcate categorical distinctions of military and non-military remits, and 'public' governmental duties from 'private' or corporate roles in securing the reliable operation of these networks. While the security imaginary of cyberspace had helped them conceptualise networked communication technologies in particular ways, it also generated new problems of categorical definitions and institutional organisation.

There are variations in the visions that military advocates and speakers offer, but rarely do they stray from technocratic and instrumental precepts of cyberspace that underwrite but also motivate a vision of cyberspace as a 'domain' of warfighting. In the years leading up to CYBERCOM's establishment, this 'domain' narrative helped them understand and translate 'cyberspace' technologies into familiar terms, to help them understand how those technologies could fit into, but also potentially reshape the organisational responses that became politically possible. When conceived of as a territorialised domain, a series of boundaries and thresholds were imagined to be challenged by cyberspace and for defining the military's role in the security of cyberspace. As we shall see in Part Two of the chapter, each of these categorical distinctions would later form the locus for boundary work when CYBERCOM's credibility and legitimacy became the source of contention.

Given this overall framing of risk, vulnerability and novelty, we can read the military (cyber)security imaginary as a reactionary story, but one that is also trying to make sense of broader technological and social changes through a very specific military cultural lens. To be sure, the positive aspects of these visions are present too when actors highlight the ways that cyberspace is an embodiment of "the free flow of information that fosters growth and intellectual dynamism" and of specific normative values of "freedom, liberty, prosperity, intellectual property, and personal information" as the commander of CYBERCOM later would put it (Rogers, 2015, p. 2). But in this military imaginary, these values and qualities tended to be portrayed as the things at risk, rather than as the source of potential solutions to the challenges thought to be posed by an increasingly networked 'information age.' When American capacities for innovation were cited in this imaginary, it is was a pool of resources that the military could draw upon, not as something that could displace the need for a military response (Chairman of the Joint Chiefs of Staff, 2000, 2006).

When we consider the military cybersecurity imaginary as a project oriented around viewing cyberspace in terms of a warfighting domain, then it begins to coalesce as a military project in which the best course of action is to undertake internal reorganisations to better 'fit' to this domain and to secure extra resources to do so. The work of establishing and promoting this conception of networked communication technologies in terms of boundary-blurring risks and threats served to cultivate frameworks that could be used for guiding change (Pfotenhauer and Jasanoff, 2017). As a result, specific organisational and doctrinal changes became more politically imaginable. As William Lynn explained in his announcement of the new military cyber command, this meant that to "…address this risk effectively and to secure freedom of action in cyberspace, the Department of Defense requires a command that possesses the required technical capability and remains focused on the integration of cyberspace operations." (Lynn, 2010 n.p.). When conceived of in terms of risks and threats, and the need to "secure freedom of action" in such spatial terms, the proposal of a new military command that centralised the disparate service components' offensive and defensive network operations became the 'logical' solution. According to CYBERCOM's 'origin stories' then, the command was a natural response to structural imperatives, but a closer reading of the controversies and cybersecurity politics that have followed in the wake of CYERCOM's establishment will show that putting the imaginaries of insecurity to work has been a politically fraught and bureaucratically contested endeavour.

3.2 Part Two: Controversy and Contention

The recurrence and persistence of debates surrounding the dual-hat leadership and co-location of CYBERCOM with the NSA at Fort Meade discussed now shows that, more than just a question of technical feasibility, military 'cyber capabilities' emerged because of political, instrumental and organisational contestation: in other words, because of boundary work that sought to defend the new command and distinguish it from its progenitors in the intelligence community. While earlier efforts described above focused on collaborative and configurational strategies, in the following sections we will see more frequent instances of working *for* boundaries to defend CYBERCOM's boundaries and their conception of their conceptual and operational 'terrains.' The core of these controversies have been centrally concerned with drawing distinctions between espionage conducted by the intelligence community on the one hand, and 'traditional military activities' (TMA) and 'attacks' on the other. These were competing conceptualisations or visions of how far cybersecurity should *go*; whether it was to be a matter of peacetime operations or wartime activities, and about articulating imaginaries in ways that could subsequently direct policy and funding. To convince its detractors that CYBERCOM was good value or politically viable, actors would advocate for the necessity of rearranging

the organisation to make military imaginaries of cybersecurity possible and actionable. However, efforts to fit this new command within culturally and historically resonant distinctions have in turn informed the range of policies and doctrines that have emerged – namely, 'persistent engagement.' In other words, organisational boundaries have (been used to) shape 'cybersecurity' as much as 'cybersecurity' has in turn (been used to) shape organisational boundaries.

3.2.1 Controversy and boundary work after Snowden

Boundary distinctions that had until 2009 been downplayed and minimised by advocates of the co-location of CYBERCOM with the NSA increasingly became the locus for those wishing to contest the arrangements from 2013 onwards. These contests, working *at* boundaries, would be articulated in two main forms: concerns about too much power being vested in one individual, and cultural and organisational clashes between the two organisations.

Despite the pragmatic technical and financial reasons offered for this co-location and 'dual hat', each of the three individuals placed in charge of this outfit since then have had to justify the unusual arrangement. As discussed earlier, the dual-hatted commander of the military's and the NSA's capabilities would span two distinct set of intelligence and military authorities and challenge several other consequential distinctions. As the first to hold the position, General Keith Alexander described the dual-hatted command as an "imperative" measure in view of the technical characteristics of the space. In defending the position to a Special Hearing before Congress following the Snowden disclosures, Alexander was asked to respond to "…widespread concern about an appropriate balance between national security and the privacy rights of American citizens" and to speak to whether there was "…wisdom in avoiding giving one person virtually unprecedented power as the head of both a unified command and a civilian intelligence agency" (Sen Mike Johanns, US Senate, 2013a, p. 69). In response, Alexander doubled down on the claims of technical and organisational convergence, arguing that the "dual-hat relationship facilitates" the transfer of knowledge about the "global cryptologic platform" and "… ensures that the Commander can maintain situational awareness and respond when required in an extremely high-paced, complex, technical environment—while applying to both jobs a single ethos of protecting privacy rights" (Alexander, in US Senate, 2013a, p. 69). Such a position would enable him to maintain situational awareness over both sets of military and civilian concerns, implying the position would grant him a transparency into operations rather than compartmentalising them.

While Hayden, Cartwright and others had quietly managed to arrange the dual-hatting of STRATCOM forces and the director of NSA, by the time that CYBERCOM was established as its own sub-unified command, questions of appropriation and oversight became unavoidable as it now needed official Congressional approval. In Congressional oversight hearings, Alexander and others

were thus asked to justify the dual-hatted role because it was thought to challenge boundaries traditionally demarcating oversight of civilian intelligence agencies from unified military commands. To allay the jurisdiction, oversight and funding concerns of Congress, CYBERCOM's advocates would also invoke those distinctions to emphasise how each organisation would be able to 'leverage each other' to fulfil national security requirements. This was intended to convince congressional committees that this was a wise use of resources at a time of budget cuts and sequestration. As both the Commander of STRATCOM, and the first dual-hatted commander of CYBERCOM and NSA together described it, the "very nature of the cyber space architecture" was such that "both organizations need expertise, tools, accesses, high-performance computing resources, situational awareness of friendly and adversary activity, and intelligence to identify potential adversaries, their tools, and their methods. Sharing such capabilities results in far lower costs than attempting to replicate them." (Haney and Alexander, in US Senate, 2014b, pp. 64–65). From the very earliest articulations of the need to conduct operations in cyberspace CYBERCOM's advocates would thus emphasise the ways that the technology was prompting an organisational response, rather than the organisational response (developed and housed at NSA) shaping the technological capabilities.

According to this reasoning, there were pragmatic reasons for advocating that these distinctions not be rigidly demarcated and policed by Congress for the time being: the dual-hat arrangement would allow "CYBERCOM and NSA to seamlessly synchronize, integrate, and coordinate their independent capabilities towards common objectives." (Haney, in US Senate, 2014b, p. 64). That it was described as 'seamless' was intended to signify to Congressional audiences how little those distinctions should be allowed to impede the operational effectiveness of these organisations, given the organisations' apparent common objectives. Highlighting the overlap in missions, tools, operating space and skillsets also acted as a reference point for advocating that they did not wish to recreate "a mirror capability" for the military that the NSA was already so competent in as that "would not make operational or fiscal sense" (Adm Rogers, in US Senate, 2016b, p. 414). Instead, the dual-hatted commander described to Congress how "the best, and only, way to meet our Nation's needs today" and "to exercise good stewardship of our Nation's resources" was to "leverage the capabilities (both human and technological) that have been painstakingly built up at Fort Meade." (Adm Rogers, in US Senate, 2016b, p. 414).

Continuing those pragmatic political arguments, and despite the earlier articulations that emphasised how the absence of territorial boundaries in cyberspace were a problem that challenged 'traditional' strategic imaginaries, those liminal qualities of cyberspace would continue to be judiciously downplayed to rationalise the co-location of the military and intelligence organisations. As Alexander described it to the Washington Post, "[w]e all operate on the same network. You create more problems by trying to separate them and have two people fighting over who's in charge of

putting it all together." (Gen Alexander, cited in Nakashima, 2013 n.p.) Advocates such as Alexander had gone some way to creating the authorities to mature and use these capabilities by instrumentalising claimed technical convergence and the claim that they 'all operate on the same network.' While such a role was intended to enable the DoD "to leverage NSA's capabilities" in order to fulfil CYBERCOM's missions (US Senate, 2013a, p. 69), this arrangement also posed as a challenge for distinguishing between the NSA's capabilities and CYBERCOM's warfighting missions. This would present particular problems for the advocates of a 'robust military capability', which manifested – as the next section will illustrate – as a failure to entirely 'translate' these hacking capabilities out of their origins in intelligence communities and into military imaginaries of distinctive strategic and tactical capabilities. These tensions began to surface around this time in debates about organisational cultures and establishing the distinctiveness of cyber space operations from intelligence operations through the framework of 'traditional military activities.'

3.2.2 Drawing distinctions between military and intelligence cultures

Despite successfully establishing the new military command, Congress were not the only people who had to be convinced of the merits of the dual-hat and CYBERCOM by its believers. Advocates for the intelligence community's interests as well as different branches of the military were also expressing misgivings about the arrangement. These concerns were most frequently expressed in terms of the credibility of CYBERCOM's efforts to demarcate its distinctiveness from its progenitors in the NSA. As a result, cultural and organisational boundaries between the intelligence community and the military command were re-emphasised and policed through competitive boundary work strategies. Drawing distinctions between military and intelligence cultures took place in at least three interrelated ways, namely: outlining how intelligence and military operations were said to have fundamentally opposing objectives; demarcating the differences between the tools and technologies needed to undertake those missions; and by highlighting the different measures of success characteristic of military or intelligence cultures. As one of the three boundaries that the military (cyber)security imaginary had problematised (discussed in Section 3.1.3), the convergence between intelligence and military technics and resources would now come to be a point of contention.

Firstly, those who were contesting the co-location arrangement would underscore how intelligence and military operations had fundamentally opposing objectives. This was articulated as a tension between intelligence and military missions and cultures. As an active duty Army cyber operations officer assigned to CYBERCOM described the matter, the original motivation for the arrangement was to allow the military command to leverage the NSA's expertise, capabilities and experiences (Schoka, 2019). While he suggested that the responsibilities of the two organisations

frequently overlapped in the cyber domain, he also described their fundamentally opposing missions (Schoka, 2019). These tensions were echoed by a former Pentagon Chief of Staff to Defense Secretary Ashton Carter who suggested that…

> …[a] lot of what we ran into during the Obama administration involved the IC [intelligence community] bucking at plans strung up by Cyber Command because they worried about intel gain-loss. The missions of Cyber Command and NSA should be complimentary, but too often they are competitive and collide with one another. (Rosenbach, cited in Bing, 2018)

While earlier collaborative boundary work to establish the co-location of military and intelligence operatives had initially downplayed those distinctions between intelligence and military mission objectives on technological grounds, when it came to putting those military capabilities into practice, tensions between the two organisations started to be articulated as a competition. As one former member of the NSA characterised the tensions that were beginning to surface, policing and navigating these organisational and cultural boundaries made for an "endless squabble. It was the difference between intelligence officers, who are in this for the long term, and the military officers, who are paid to plan for attacks." (Anonymous administration source, cited in Sanger, 2018, p. 45). The differences in the two organisations were also referenced by James G. Stavridis, former supreme allied commander of NATO, and Dave Weinstein, a strategic planner at Cyber Command:

> Not only do the organizations have starkly different cultures, their missions are vastly different, even contradictory. There is, indeed, an overlap between military and intelligence missions in cyberspace. But it was a mistake to assume that they would complement, rather than impede, each other. (Stavridis and Weinstein, 2013)

Thus, the different cultures were invoked and policed here to contest the ongoing co-location, on the basis of culturally meaningful distinctions between how intelligence operatives and military operatives define themselves and their missions. For those wanting a distinctive military capability, as Stavridis and Weinstein did, then highlighting the 'starkly different cultures' and their concerns about NSA's ability to gain priority in operational planning over CYBERCOM's attack (rather than espionage) goals was intended to build a case for the separation of the two organisations as a means to secure greater operational freedom and access to resources for CYBERCOM. These 'starkly different cultures and missions' were also policed in relation to the second difficulty that boundaries between military and intelligence cultures were said by the dual-hat's detractors to pose to organising for distinctively military and 'offensive' cyber operations.

Secondly, as one of the three boundaries that the military cybersecurity imaginary had problematised (discussed in Section 3.1.3), articulations of 'structurally-determined offense

dominance' would now come to be a point of contention. In other words, actors would cite putatively essential characteristics of the technological environment as part of their competitive boundary work to emphasise distinctions between military and intelligence tools. The 'intel gain-loss' cited by Rosenbach above referred to the calculation that intelligence officials weigh before every operation, whereby the use of a capability runs the risk of revealing its tools and techniques, but with the potential advantage of new intelligence in exchange. As the DoD's Joint Publication on cyberspace operations described it, this is a unique "technological challenge" for using cyberspace capabilities that rely "on exploitation of technical vulnerabilities in the target [that] may reveal its functionality and compromise the capability's effectiveness for future missions." (US Department of Defense, 2018, p. x). Different mission objectives therefore had different tools and risk calculations. Rear Admiral Bill Leigher was instrumental in setting up the Navy Fleet Cyber Command (which became a sub-component of CYBERCOM) and explicitly described the tensions between different measures of success and the tensions in the objectives of espionage versus CYBERCOM missions:

> If you're collecting intelligence, it's foreign espionage. You don't want to get caught. The measure of success is: 'collect intelligence and don't get caught.' If you're going to war, I would argue that the measure of performance is 'what we do has to have the characteristics of a legal weapon in the context of war and the commander has to know what [it does when] he or she uses it'. From an NSA perspective, cyber really is about gaining access to networks. From a Cyber Command point of view, I would argue, it's about every piece of software on the battlefield and having the means to prevent that software from working the way it was intended to work [for the adversary] (Leigher, cited in Tucker, 2017).

Leigher's point here about fundamentally opposing missions and 'measures of performance' was painting a picture of an incompatible cultural difference between intelligence and military organisations. Furthermore, co-locating the two (sometimes competing) organisations meant that CYBERCOM had a deeply ingrained organisational reliance on NSA tradecraft and structure, making it difficult for each organisation to realise their respective missions (Schoka, 2019). While technical commonalities were cited as reasons to organise a military branch for offensive cyber operations to begin with, for those advocating for cyber operations as a 'core military competency' (rather than an intelligence competency), legitimising and defending the autonomy of military operations in cyberspace has therefore been challenged by those who cite these internal cultural distinctions.

Thirdly, such different measures of success between intelligence and military officers were also invoked by those wanting to actualise distinctively offensive cyber operations, also alluded to by Leigher. These differences were said to be embodied in the design parameters of their respective tools and techniques. One of the early rationales for developing military cyber capabilities was with a view

to developing technologies the military could exploit that fell short of kinetic weapons, but that built off the infrastructures that the intelligence community has already built. During his years in command of STRATCOM, General James Cartwright had come to appreciate that "…the tools available to a president or nation in between diplomacy and military power were not terribly effective" leading him to develop studies into 'speed of light means' including 'electronic warfare and cyber' (Cartwright, cited in LaGrone, 2012 n.p.). At the same time, he would draw bright lines between intelligence and military capabilities by emphasising essential qualities that he thought characterised the military, stating that "DoD is in the business for offense – that's essentially what we are." (Cartwright, cited in LaGrone, 2012 n.p.).

According to this logic, the military is 'in the business of offense,' and military service cultures have a preference for visible and quantifiably measurable effects (White, 2019, p. 377). Highlighting distinctions that would signify the 'offensive' traits of cyber capabilities would come to be a productive and instrumental set of distinctions for those wanting to defend CYBERCOM's credibility as a warfighting entity. This rationale was evident in a statement made by the executive director of U.S. Cyber Command Shawn Turskey in July 2016. In speaking to private sector security and software vendors at a Department of Homeland Security business conference, he stated that "…we will continue to work with the intelligence community for offensive means and offensive operations. *But as the United States Cyber Command, we need totally separate tools and infrastructure to conduct our operations*." (cited in Bing, 2016, emphasis added). Unlike intelligence tools and capabilities, military operations historically prefer tools with distinctive technological characteristics: in this instance, they needed to be "loud" (ibid), again invoking the analogies with military kinetic effects. This was an effort to articulate how CYBERCOM's tools were at odds with the stealthy capabilities favoured by their colleagues in the intelligence community.

Despite the desire and ingrained habits of military officers to use traditional 'kinetic' frameworks to organise and judge cyber operations by, there were limitations to this framework (McGhee, 2016). While he was head of CYBERCOM, Admiral Michael Rogers told Congress that "we've built a good framework in the kinetic world" and that such frameworks offered "a good departure point for" cyber operations: "the same things that have conditioned my life in the kinetic world as a serving military officer […] that's the kind of point of departure for me intellectually in the cyber world." Like Turskey, Rogers was here invoking the culturally conditioned frameworks that were intuitive to military actors, as a way to demarcate how cyber operations fitted within those 'kinetic' frames of reference. Despite the desire to impose distinctions from the military's intellectual and cultural frameworks, cyberspace operations do not easily translate into those kinetic frameworks Rogers was referencing here. This was because, as one CYBERCOM operative points out, unlike a bomb or munition, the "efficacy of a weapon system" in cyberspace operations hinges upon its ability to

operate secretly (Schoka, 2019). This makes it harder to 'demonstrate' or prove the 'indefinite effectiveness' of those military capabilities, when, according to CYBERCOM's 2018 *Command Vision'*, the "underlying technologies and protocols of cyberspace," are a "fluid environment of constant contact and shifting terrain." (CYBERCOM, 2018, p. 4)

The competitive boundary work for boundaries analysed thus far suggests that cyber operations are capabilities that do not fit established bounds of kinetic operations: tools and opportunities are short-lived, and effects potentially reversible (Borghard and Lonergan, 2019), meaning that military actors and advocates for CYBERCOM's autonomy have sought to make the case for how they fit into recognisable (military) frameworks. The tools and operations appear to make for a unique operational environment. As one military officer in charge of the army's information technology and computer systems described it: "…it's the only place where you're going to run your business [operations] and you're also going to fight a cyber war on the same infrastructure simultaneously." (Wang, deputy Chief Information Officer, cited in Pomerleau, 2016). Cyber operations are therefore not neatly analogous to the kinds of kinetic operations that the military are so often judged – and judge themselves – by, highlighting the work that has had to go into demarcating how these tools and capabilities fit into historically resonant institutional, organisational, cultural and political bounds. As the rest of this chapter will show, these different measures of success have shaped as much as they have constrained the kinds of capabilities the military has sought, informing the articulation of the doctrine of 'persistent engagement.'

3.2.3 Demarcating 'traditional military activities'

As one of the three boundaries that the military (cyber)security imaginary had problematised (discussed in Section 3.1.3), boundary work would now seek to underscore how frameworks for 'traditional military activities' could be mobilised in support of CYBERCOM's efforts to defend its credibility, re-creating boundaries for CYBERCOM to define an exclusive organisational and operational territory for themselves. TMA is a well-established historical constituent of distinguishing between wartime and peacetime activities for U.S. actors in other areas. It would therefore be invoked as a set of categorical distinctions that could be a productive resource for CYBERCOM's supporters wishing to expand the parameters for legal military actions in and through cyberspace. To begin with, Congress recognised the importance of giving CYBERCOM time to demarcate its capabilities. As one hearing's opening statement reflected:

> U.S. Cyber Command, or CYBERCOM as it has been called, has been tasked with conducting the full range of activities needed for the Department of Defense [DOD] to operate effectively in cyberspace. Of one thing I am confident: Cyberspace will be a big part of future warfare.

> That means we can't afford to get this wrong. The establishment of CYBERCOM is a critical milestone for our Nation's defense. Cyberspace is an environment where distinctions and divisions between public and private, government and commercial, military and non-military are blurred. (Chairman Ike Skelton, in US House of Representatives, 2010, p. 1)

While they initially spoke of the way that distinctions and divisions were blurred, demarcating the military's role in cybersecurity would require CYBERCOM's advocates to articulate how it would either reinforce or challenge these distinctions and divisions, particularly where the distinctions of 'military and non-military' were concerned in the case of CYBERCOM. This can be illustrated through the appropriations hearings that have focused on defining how cyber operations fit within definitions of "traditional military activities" (TMA), as part of strategies to distinguish and legitimate the military's cyber operations from those of the intelligence community. Over the course of successive National Defense Appropriations Acts, lawmakers with oversight of the Armed Services have consistently sought to expand the military's role in cybersecurity by seeking clearer language on TMA. In the 2012 National Defense Authorization Act (NDAA), Congress sought to clarify this definition for the Command:

> "The conferees recognize that because of the evolving nature of cyber warfare, there is a lack of historical precedent for what constitutes traditional military activities in relation to cyber operations and that it is necessary to affirm that such operations may be conducted pursuant to the same policy, principles, and legal regimes that pertain to kinetic capabilities." (US House of Representatives, 2012, p. 686)

While the Secretary of Defense had established a military cyber command in 2009 with the rationale of it being an imperative response to an evolving technological environment, demarcating how its activities should fit into the historical precedence set by military activities has been an ongoing and contested process. Contrary to instrumentalist narratives about 'the evolving nature of cyber warfare' driving institutional responses in the military, a whole other set of political and conceptual issues have also played a significant role in the DoD's efforts to defend the new command's autonomy and legitimacy. In this case, lawmakers were stating that cyber operations should fit within those historical bounds of 'traditional military activities' as a means of legitimising their continued development by CYBERCOM.

Demarcating how cyber operations relate to traditional military activities was a strategy undertaken by advocates of CYBERCOM because the command's policy and appropriations authorities were at stake. The first attempt at clarifying how cyber operations fit within 'TMA' did not survive the 2012 conference committee for the bill, and the bounds of the matter had yet to be settled by the time of the conferees' report for the NDAA of 2019 either. Echoing these earlier concerns, the

conferees noted that "…one of the challenges routinely confronted by the Department is the perceived ambiguity" of whether military cyber operations "qualify as traditional military activities as distinct from covert actions" (US House of Representatives, 2018, p. 2223). For the conferees, they could "…see no logical, legal, or practical reason for allowing extensive clandestine traditional military activities in all other operational domains (air, sea, ground, and space) but not in cyberspace" (US House of Representatives, 2018, p. 2223). This point intended to set out how CYBERCOM's activities would fall within their jurisdiction, whilst also making political space for the command to extend the parameters of its activities, by making the equivalence with 'other operational domains' explicit.

The then commander of CYBERCOM, General Nakasone, relatedly acknowledged in Congressional hearings that the unique characteristics of the space were a significant factor in the difficulties they were having in deciding how cyber operations fit within the historic bounds of TMA. As a "very, very young and maturing force" in CYBERCOM, Nakasone agreed that "…being able to define traditional military activities has sometimes been hard." Despite the Conferees' argument for the equivalence of other domains, Nakasone pointed to the limitations posed by the materiality of cyberspace: "Not having borders is something that […] really isn't applicable in the other domains, minus space" (Nakasone, in US Senate, 2018, p. 54). That this was still a matter for debate ten years after CYBERCOM's establishment suggests the extent to which the technical qualities of these operations are still triggering boundary work to demarcate how they fit within long-held categories to differentiate wartime and peacetime activities.

The discussion so far has sought to demonstrate the extent to which it has not been just the operating environment of cyberspace that has shaped the establishment of military cyber capabilities. CYBERCOM has been both a product of, and a condition for, a whole strategic and cultural security imaginary as much as a 'natural' response to exogenous technological factors. Contrary to the widespread narrative that cyberspace technologies are overdetermining the organisational response, the analysis in this section has suggested a more complicated trajectory has emerged over time. As legal advisor for Special Operations Command North pointed out, the "current reality is that *offensive cyber operations are difficult*" (McGhee, 2016, p. 47 emphasis added), and this has been reflected in efforts by advocates for CYBERCOM's independence to articulate how the new command maps onto historically resonant categories that U.S. actors have long used in other contexts to differentiate between peacetime and wartime activities, or between military and intelligence activities. As the final part of the chapter will now demonstrate, this has meant that to justify and make military cyber capabilities intelligible in terms of these historic distinctions, state actors have simultaneously shifted the institutional, organisational, legal, and social boundaries that they operate within too. At the same time, cyber operations have also worked to reconstitute some of those boundaries, with the result that they have expanded the military's role in cybersecurity from 'defense of the network' to a more

extensive doctrine of 'persistent engagement,' a doctrine which has in turn acted as a means of distinguishing themselves from the intelligence community.

3.3 Part Three: (Re)constituting boundaries and actualising the imaginary

As part of the DoD's efforts to make the military cybersecurity imaginary a reality, making a credible and autonomous military cyber capability has been a challenge. In the analysis that follows, the chapter will show how boundary work has played an important part in constituting 'persistent engagement.' This section will draw out how persistent engagement has emerged as the best way for CYBERCOM to differentiate the command from the intelligence community and its tools, again working *for* boundaries that would distinguish CYBERCOM from its progenitors in the intelligence community. At the same time, while CYBERCOM has devised a doctrine in response to the ways that its advocates had articulated historically resonant boundaries and pre-existing schema to defend the autonomy of the new command, as we shall see now, conceptions of the bounds of legitimate peacetime activities 'below the threshold' of war have gradually been reconstituted over time too, expanding the permissibility of military actions beyond DODIN networks that were not politically possible in 2009.

3.3.1 Boundary distinctions shaping 'Platforms' and 'Architectures.'

Two technical programs illustrate the military's efforts to reconstitute those distinctions in the command's favour. One of these initiatives is the 'Unified Platform,' or UP. The idea for the UP was first mentioned publicly in the 2015 DoD Cyber Strategy. Despite CYBERCOM developing some capabilities in conjunction with the NSA, it was indicative of the military's desire to disarticulate the command from its progenitors at the NSA when the document reflected that the military "must have the technical tools available to conduct operations" of its own (US Department of Defense, 2015, p. 18). This proposed "network of computers, servers, data storage, and analytic capabilities" (Gen. Cardon, in US House of Representatives, 2015a, p. 105) was claimed as a necessary prerequisite for the military's cyber operations because of the 'incorrect assumptions' that had motivated their colocation with the NSA to begin with. As one Senator reflected in a hearing that year:

> When Cyber Command was established, NSA leaders asserted that military and intelligence operations in cyberspace overlapped almost entirely and argued that Cyber Command for efficiency and effectiveness should make use of the infrastructure, planning systems, and tools that NSA had already developed. NSA expected that a military command would operate much the same way that a signals intelligence agency would in cyberspace. *Five years later,*

> *we know that these assumptions were incorrect. Cyber Command needs separate and different tools, infrastructure, training ranges, planning systems, TTPs [tactics, techniques and procedures], and command and control capabilities from those that NSA* has developed for its own use. (Reed, in US Senate, 2015d, p. 75, emphasis added).

Here we have an example of peacetime and wartime boundaries, or distinctions differentiating intelligence and military actions, being invoked as a constraint on the range of political and technical programs available to CYBERCOM. For Reed and others, this 'assumed commonality' between intelligence and military operations that had led to their colocation initially were now no longer such credible claims when judged by those distinctive 'military' standards discussed earlier.

While earlier episodes of collaborative and configurational boundary work had emphasised technical commonalities to establish CYBERCOM on practical and organisational grounds to begin with, as time passed this arrangement increasingly caused contention in mapping onto existing expectations of institutionalised and cultural boundaries between intelligence and military operations. When members of Congress compared military operations, with their expectations of 'loud' tools and capabilities, to the intelligence agency's emphasis on "high-end—and therefore expensive and hard-to-develop—technical tools and tradecraft" specifically designed to be untraceable, they were left unconvinced of CYBERCOM's distinctive merits (advance questions from Chairman Levin, US Senate, 2014c, p. 514). The Unified Platform was therefore proposed as a way for CYBERCOM to reinscribe distinctions between intelligence and military operations that had previously been technically and organisationally downplayed and blurred.

The Unified Platform (UP) was both the result of the military cybersecurity imaginary, and a precondition for future efforts at demarcating "military operations that are unique and distinguishable from the Intelligence Community" (Rosenbach, in US Senate, 2014c, pp. 413–4). Historically resonant distinctions between peacetime and wartime, and between military and intelligence activities, have been implicitly reflected upon as a means of understanding the military's roles in national cybersecurity. Much as Representative Thornberry had asked the Commander of STRATCOM in 2010 to clarify "the role of the U.S. military in cybersecurity, computer network attack, defense, and exploitation", he was also asking when "America act[s] under Title 50 authorities, and at what point Title 10?" (Thornberry, in US House of Representatives, 2010, p. 101). The UP was intended to help demarcate these very issues and responsibilities. According to the official description, it was envisioned as enabling the 'cyber mission forces' "to conduct full-spectrum cyberspace operations in support of national requirements" (US Department of Defense, 2015, p. 18) and was crucial to enabling these operations (Adm. Tighe, in US House of Representatives, 2015a, p. 105). The title of the Congressional hearing ('*Cyber Operations: Improving the Military Cybersecurity Posture in an*

Uncertain Threat Environment') similarly invoked the links between cyber operations and the military's ability to more clearly articulate its posture and responsibilities in cybersecurity. In other words, the UP was described as a key component to the military's ability to fulfil its historic role of defending the nation in this new space.

If the UP could actualise the military vision for capabilities differentiated from the intelligence community's, this would solidify the military's future funding and research efforts. Having declared their intention to develop a UP program, in September 2016 the military command was finally granted its own acquisitions authorities, giving it limited permission to identify and purchase the tools and resources that it would need to develop its own distinctive tools and capabilities (Pomerleau, 2017). After the 2015 DoD Cyber Strategy, it took three years for the Department to release the draft UP request for proposals for their suppliers, and in that time boundary work that invoked distinctions governing peacetime and wartime activities would also shape the capabilities sought through these funding authorities. This can be illustrated by the case of "Operation Glowing Symphony." One of the few cyber operations to be disclosed to the public, a dedicated task force at CYBERCOM undertook Operation Glowing Symphony in 2016 to interrupt ISIL's ability to disseminate its propaganda (Martelle, 2018). CYBERCOM operators hacked the online accounts of computer administrators, deleted content and changed the administrator passwords to block their access (Cox, 2018). However, according to an anonymous senior defence official cited by the Washington Post four months later, CYBERCOM "has not been as effective as the department would expect them to be, and they're not as effective as they need to be. They need to deliver results." (cited in Nakashima and Ryan, 2016). Statements like this were intended to publicly pressurise CYBERCOM's leadership into producing more tangible 'results' that the administration, and Secretary of Defense Ash Carter in particular, could hail as signs of success in their campaign against ISIL (Carter, 2017). That CYBERCOM was described as not being 'as effective as they need to be' reflects the enduring influence that distinctions between intelligence and military operations discussed earlier can have. 'Delivering results' was invoking the standards set by kinetic operations traditionally undertaken by the military. According to Joshua Geltzer, who was the senior director for counterterrorism at the National Security Council until March 2017,

> In general, there was some sense of disappointment in the overall ability for cyberoperations to land a major blow against ISIS. There were folks working hard on this stuff, and there were some accomplishments that had an impact, but there was no steady stream of jaw-dropping stuff… There was no sort of shining cybertool. (Geltzer, cited in Sanger and Schmitt, 2017).

The disappointment in this operation's 'effects' and the tendency to judge military operations by standards set in other domains meant that funding authorities would be used to develop distinctive

military capabilities or 'cybertools' that more closely aligned with these distinctions. By these standards, the operation failed to offer a credible proof-of-concept for distinctive military operations. The Secretary of Defense at the time later reflected:

> It never really produced any effective cyber weapons or techniques. When CYBERCOM did produce something useful, the intelligence community tended to delay or try to prevent its use, claiming cyber operations would hinder intelligence collection. (Carter, 2017, p. 33)

Intelligence operations were thus said to be setting limitations on the measures of effectiveness of military operations. The search for distinctive 'cyber tools' would therefore be facilitated by the acquisitions authorities granted for the UP.

Over the three years that the UP was being discussed within the DoD, imperatives to develop capabilities distinctive from the intelligence community would also be invoked to shape a broader initiative, called the Joint Cyber Warfighting Architecture, or JCWA. According to CYBERCOM's dual hatted commander Gen. Paul Nakasone in testimony before the Senate, operational lessons learned from Glowing Symphony informed their acquisition priorities, including the "geographically distributed set of redundant and reliable infrastructures […] as well as a virtual arsenal of capabilities (comprising both open-source and high-end tools)" (Nakasone, 2019b, p. 12). In this testimony, he described the Joint Cyber Warfighting Architecture not as "a fixed future state, but rather an adapting set of capabilities continually evolving along with technological change, operational outcomes, and shifting threats" that would help the DoD make critical investments in those tools that would help them "fight and win in conflict." (Nakasone, 2019b, p. 12)

While adversary action was cited as a key reason for developing the strategy of 'persistent engagement', here we can see the way that frustrations with the distinctiveness of 'wartime' capabilities had informed the acquisition priorities embodied in the initiatives of the UP and the later JCWA. The JCWA was now viewed as an overarching initiative of which the UP was a component (Nakasone, 2019b), but both initiatives have been part of the military's efforts to reinscribe or reinforce distinctions between military and intelligence operations.

Boundary work that polices and institutionalises these organisational and operational distinctions between the military and intelligence are likely to be an ongoing feature of efforts by security actors to defend the credibility of CYBERCOM. The JCWA was recently described as a key initiative in helping to react to the actions of competitors, with one General describing their "need to constantly innovate in this space because our adversary gets a vote" (Gen. Gingrich, in CYBERCOM, 2019, p. 7). However, he went on to suggest that unlike in previous years where the command was focused on developing capabilities in the near term and modifying those already in its possession, the

JCWA would be working on program objectives through to the year 2025 (CYBERCOM, 2019, p. 8). More than just reacting to adversary actions then, these capabilities will likely be shaped into the future by culturally specific and overarching political pressures to distinguish military capabilities based on distinctions governing wartime and peacetime activities.

3.3.2 (Re)constituting 'traditional military activities'

At the same time as these technical and organisational programs, appropriations legislation was construed by CYBERCOM's political supporters in Congress as one of the ways that they could shape a clearer articulation of the military's role in cybersecurity and their military capabilities. The Conferees' report that accompanied the National Defense Authorization Act (NDAA) for 2019 expressed their frustrations that traditional military activities had been clearly defined in other domains but that cyber operations were still undefined (US House of Representatives, 2018, p. 2223, cited earlier). For Congressional lawmakers, efforts to more clearly define how cyber capabilities fit within the bounds of TMA would serve two purposes. First, it would ground these capabilities more firmly within the remit of the Armed Services oversight and appropriations streams. Over the ten years that CYBERCOM has been operating, budgetary constraints and sequestration have been a constant feature constraining spending on other programs, and yet cybersecurity has been one of the few areas to receive constant funding increases across government, but especially the military. This was something that Senators and Representatives would have had a political interest in securing for their districts. Second, expanding the bounds of TMA to incorporate cyber capabilities would give congressional lawmakers the ability to use their appropriations authorities to politically shape those capabilities and national declaratory policies. Lawmakers have political and bureaucratic interests in maintaining the distinctions between armed services and intelligence. The conferees used the Armed Services NDAA and the accompanying report to force the Executive to make legislative and authoritative room for the military cyber force to realise its potential capabilities, demonstrating how boundaries have shaped capabilities as much as adversary action or technical features of the space have.

Because the NDAA language declared that cyberspace operations constituted traditional military activities, Congress had successfully redrawn those boundaries to fit the military's cyberspace capabilities into longstanding distinctions demarcating military activities. As a collaborative boundary work strategy, this expansion of boundaries was an important move, as without it CYBERCOM had previously had to "…declare or make very overt any of our operations, and acknowledge that it's being done by the DOD and the USA -- not very conducive to being successful inside the cyber domain." (Maj. Gen. Moore, cited in Lopez, 2019 n.p.). These expanded boundaries have contributed to

improving the military's ability to conduct cyber operations. Eric Rosenbach, former chief of staff to the Defense Secretary, described how with offensive (cyber) operations during the Obama administration, he could "…count on one hand, literally, the number of offensive operations that we did at the Department of Defense." (cited in Sanger and Perlroth, 2019, n.p.). By 2018 and 2019, a report by the DoD's weapons tester, the Director Operational Test and Evaluation office, suggested that it had collaborated with developers and testers for more than a dozen offensive cyber events in fiscal year 2019, contrasted with "more than 10" in fiscal 2018 (cited in Pomerleau, 2020, n.p.). By expanding the possible activities for what counts as actions below the threshold considered armed aggression, lawmakers have helped CYBERCOM undertake more offensive operations, so that 'persistent engagement' is a result as much as a precondition for those operations.

This boundary work was concretised when CYBERCOM's 2018 *Command Vision* document made the rationales explicit for developing and expanding the military's roles and capabilities in cybersecurity. According to the *Command Vision*, a new strategy and doctrine was required because "in order to improve security and stability, we need a new approach" (CYBERCOM, 2018, p. 2), one which required that the government and military "expand the military options available to national leaders and operational commanders" (CYBERCOM, 2018, p. 2). The strategy was thus intended to expand the bounds of military responsibilities and demonstrate the credibility of its unique capabilities. The first form of the two rationales worth noting was articulated in terms that suggested adversaries are 'forcing' the government's reaction:

> Our adversaries maneuver deep into our networks, forcing the US government into a reactive mode after intrusions and attacks that cost us greatly and provide them high returns. This reactive posture introduces unacceptable risk to our systems, data, decision-making processes, and ultimately our mission success. (CYBERCOM, 2018, p. 5)

'Persistent engagement' was thus a strategy that was portrayed as having emerged in response to strategic competition in cyberspace, determining the government's responses. The strategy of persistent engagement was an effort to move beyond 'reactive' postures and expand the capacities available to the military's dedicated cyber command. Echoing the military cyber (in)security imaginary outlined earlier, the second form of rationale was that the nature and character of the environment posed unique challenges:

> Cyberspace is a fluid environment of constant contact and shifting terrain. New vulnerabilities and opportunities continually arise as new terrain emerges. No target remains static; no offensive or defensive capability remains indefinitely effective; and no advantage is permanent. Well-defended cyber terrain is attainable but continually at risk. (CYBERCOM, 2018, p. 5)

Such fluid 'terrain,' where no 'capability remains indefinitely effective,' implied the necessity for the military to keep "building the operational expertise and capacity" available to them (CYBERCOM, 2018, p. 5), where "…[p]olicies, doctrine, and processes should keep pace with the speed of events in cyberspace to maintain decisive advantage" (CYBERCOM, 2018, p. 2). When conceived of in this way, the military imaginary of cyberspace as a domain meant the operational concept to 'defend forward' naturalised as much as it shaped the desire of US cyber forces to "maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations" (Nakasone, 2019a, p. 13). This new concept emerged because when cyberspace was conceptualised in this way, the primary purpose of US military cyber forces thus became "to limit the terrain over which the enemy can gain influence or control." (Nakasone, 2019a, p. 13) This concept was meant to shift them from a reactive posture in which the adversary and the technology was shaping their responses, to one in which they were proactively dealing with threats: as Nakasone went on to explain, if they were "only defending in "blue space," we have failed." (Nakasone, 2019a, p. 13). By rationalising their role in terms of defending territory, the doctrine of persistent engagement and defending forward thus worked to literally extend the military roles and activities beyond military networks, where in 2010 they were proscribed from doing so because of political and normative restraints on military actions outside of peacetime. This framing was also indicative of the extent to which cyber 'space' was to be conceived of and institutionalized as a 'terrain' to be defended, again serving to make the context intelligible and actionable as a military matter.

However, as this chapter has demonstrated, a closer examination of the emergence of these military articulations the military cybersecurity imaginary shows how the development of distinctively 'military' cyberspace capabilities has not been the result of a 'natural trajectory' of cyberspace or technologies. The chapter has argued that long-held distinctions about peacetime and wartime have thus constituted the kinds of capabilities and technologies that the military have sought as much as any 'essential characteristics' of the operating environment. For example, while boundaries between intelligence and offensive capabilities had long been technically and organisationally downplayed through initiatives such as the co-location of NSA and military cyber units, this chapter has shown how military actors are now working hard to *reinscribe* boundaries between intelligence and military capabilities. In this regard, we have seen how organisational boundaries have shaped technological capabilities, expanding the range of permissible military activities at a tactical and technical level below the threshold of war. When the new Command was established, its mission focus was described as a consolidation of DoD efforts to defend its own networks (Lynn, 2010; Shanker, 2010). Congress changed the law in 2018, so that CYBERCOM was authorised to take actions inside a non-Defense Department network overseas as part of traditional defensive military activity (Nakashima, 2019), indicating the extent to which the bounds of permissible peacetime activities have expanded.

The initiatives discussed in this chapter suggests the extent to which boundary work around the distinctions between peacetime and wartime activities have enlarged the roles, responsibilities and capabilities of the military in 'cybersecurity.' Thus, the strategy of 'persistent engagement' emerged in response to, and as a condition of boundary work intended to extend the military roles and activities beyond military networks. An analysis of the different boundary work strategies (in turns collaborative, configurational and competitive) demonstrated how actors have struggled to articulate the distinctiveness of military cyber operations and to fit them into pre-existent notions of what military capabilities 'should' look like based on long held peacetime-wartime distinctions. This is still a matter of ongoing conceptual and institutional boundary work, highlighting that possessing superior material or organisational resources does not overdetermine the success of those different boundary work strategies. 'Persistent engagement' has thus simultaneously been the product of, and can be viewed as the performance of, boundary work.

3.4 Conclusion

This chapter has analysed in turns episodes of competitive and collaborative boundary work, where drawing boundaries between 'military' and 'intelligence' and 'peacetime' and 'wartime' have been used to demarcate the parameters of military actions in the name of 'cybersecurity.' The boundary work analysed in this chapter was thus animated by competing conceptualisations or visions of how far cybersecurity should *go*; whether it was to be a matter of peacetime operations or wartime activities, and about articulating imaginaries in ways that could subsequently direct policy and funding.

Contrary to a great deal of the mainstream policy discourse and imaginaries of insecurity then, it was not that a strategy of 'persistent engagement' - national or institutional - was chosen and then a military cyberspace command and technologies created to fulfil its requirements. The technological environment of cyberspace did not automatically necessitate the development of these distinctively military capabilities. Instead, the military cyberspace operations programme was embarked on for reasons not much more explicit than that "cyberwar was coming" (Arquilla and Ronfeldt, 1993) and that long-held American distinctions about peacetime-wartime activities prevented their intelligence agencies from undertaking more than espionage operations. Only as CYBERCOM has taken shape has the realization evolved that 'persistent engagement' is the strategy that best justifies or fits military cyberspace capabilities and helps military actors defend their organisational boundaries. To differing extents at different moments in time, capabilities have informed strategy and boundaries, while boundaries have informed capabilities and strategies.

However, as the next chapter will now begin to show, these military imaginaries of cyber (in)security and of cyberspace as a 'domain' have not been universally accepted or hegemonic across

the government. Though military framings have dominated cybersecurity politics in the US, they have also been shaped by competitive boundary work from other federal agencies, who have articulated competing imaginaries of security.

Chapter Four: 'Domesticating' Cybersecurity – 'Borderless' cyberspace and territorial agencies

4.0 Introduction

In the previous chapter, we saw how the military imaginary of cyberspace had worked to organisationally embed a conception of networked communication technologies in terms of borderless threats and constant contact, promoting an imaginary that reinforced a narrative about the 'structural and technological imperatives' of cyberspace's 'nature' as a domain. Meanwhile, in this chapter I will show how DHS have sought to re-territorialise imaginaries of cyberspace in distinction to the military's visions. The largely *competitive* boundary work analysed here is therefore concerned with establishing who 'cybersecurity' belongs to, and which state agencies should have what roles and responsibilities.

This chapter will argue that to contest the military's cybersecurity imaginary of cyberspace as a warfighting 'domain,' the DHS mobilised similarly spatialised distinctions of borders and 'homeland.' Despite commonplace narratives of cyberspace's 'borderless' nature, this chapter finds that boundary distinctions of 'internal' and 'external' have served as productive strategic resources for actors working to defend the legitimacy, credibility and authorities of the DHS. This chapter argues that DHS actors were able to 'domesticate' and 'reterritorialise' cybersecurity by shifting the focus onto managing the nation's 'internal' vulnerabilities through a risk-based framing, in distinction to the 'external' agency of threat actors that they allocated as a military concern.

To substantiate this argument, the chapter will begin with an analysis of the DHS' cybersecurity visions and imaginaries, to outline how they articulated cyberspace as an ecosystem and an environment instead of a 'domain.' This was a product of their organisational culture as much as a commitment to a particular vision of the future. Then, in Part Two, an analysis of the *competitive* boundary work in turf battles between DHS and DOD shows how the characteristics of those boundaries and categories have been negotiated through contestation. Actors emphasised different characteristics and attributes of 'cybersecurity' according to their strategic interests. Finally, Part Three will analyse the boundary work in initiatives that it argues show how risk-based approaches emerged and iterated over time to re-spatialise or domesticate a 'borderless' cyberspace. DHS' cybersecurity programs cannot be seen simply as a series of technical initiatives. Instead, they are simultaneously the instantiation of a social and political project to extend and constitute risk-based modes of governance into cybersecurity on the one hand, working *for* boundaries to defend DHS' credibility on the other.

4.1 Part One: imaginaries of reterritorializing cyberspace

In this section, we will see how the DHS sought to weave a story of a territorialised cyberspace, a 'homeland' in distinction to the military's cybersecurity imaginaries. This narrative would work to draw territorial boundaries in ways that would constitute a spatialised and 'scalar imaginary' of cybersecurity and cyberspace, working *for* boundaries that could demarcate an exclusive territory for the DHS. In short, the DHS was working to make sense of cyberspace in terms that could get this idea to fit into ideas of territorial scales and 'homeland security.' It used scalar terminology to do so, but it is more than rhetorical, as Part Three will show. The idea of 'the homeland' as a delimited, bounded, spatially coherent, exclusive and calculable space would be a formulation repeated throughout federal discourses and DHS imaginaries. In distinction to the military's imaginary of 'cyberspace' as *terrain*, the DHS's imaginary focused on demarcating the *territory* of a 'homeland.'

The story of the 'homeland' cybersecurity imaginary begins in 2002, when the DHS was established. The creation of DHS represented the biggest reorganisation of the national security apparatus since 1947's National Security Act. It brought together subdivisions that had each separate cyber responsibilities and expertise, from Department of Commerce, the FBI, the General Services Administration, the Treasury, the Secret Service and even the Department of Defense's National Communications System (Fitzgerald, 2003; Deppisch, 2019). It was the DHS that authored the nation's first cybersecurity strategy document in 2003, which tasked the nascent department with working with the private sector to protect the nation's "critical information infrastructures." These infrastructures were conceptualised as located within the geopolitical bounds of the US, so designating it a matter of homeland security mirrored a habitual territorial understanding in the US of the division of security activities. Between the reorganisation and the strategy document, cybersecurity thus became organisationally designated as a matter of 'homeland' security in 2002.

According to this emerging imaginary, the nation was facing a series of challenges which were distinctive for the ways that they crossed territorial borders, and cyberspace was included in this conceptualisation. When the DHS was established in 2002, claims about cyberspace's 'borderless' nature were widespread in American culture and political discourse (Ó Tuathail, 1999; Valovic, 1999; Agre, 2002). Furthermore, by amalgamating disparate federal agencies and subdivisions that had been working on matters of critical infrastructure protection and information security, DHS had inherited a particular organisational conceptualisation of cyberspace as "…a new geography, where borders are irrelevant and distances meaningless, where an enemy may be able to harm the vital systems we depend on without confronting our military power." (President's Commission on Critical Infrastructure Protection, 1998, p. ix). This 'borderless' conception of cyberspace had been a prominent feature of

cybersecurity politics in the US since President Clinton signed Executive Order 13010 "Critical Infrastructure Protection" in 1997. As part of that Executive Order, a President's Commission published a report that elevated the matter of the nation's "critical infrastructures" – its networks of communications, transport and utilities – to a matter of 'national security,' declaring that new security paradigms would be necessary when in "the cyber dimension there are no boundaries" (President's Commission on Critical Infrastructure Protection, 1998, p. vi). Throughout the report, cyber threats were described as distinctive for the ways that they transgressed historic and territorial boundaries and "perhaps most difficult of all, the defenses that served us so well in the past offer little protection from the cyber threat." (President's Commission on Critical Infrastructure Protection, 1998, p. vi). Where previously it could be assumed that "broad oceans, peaceable neighbors" and military power, were elements that had historically "provided all the infrastructure protection" America needed (President's Commission on Critical Infrastructure Protection, 1998, p. ix), cyber threats, as conceived of above, would necessitate "new thinking [that] must accommodate the cyber dimension." (ibid, p. vi).

This articulation of the problems posed by cyberspace foreshadowed how the DHS would describe the challenges of terrorism in its first homeland security strategy too (DHS, 2002). For those subdivisions tasked with managing national borders in terms of flows of goods and people, this meant that the DHS would use technological and organisational means of policing (and reaffirming) the nation's territorial boundaries (Amoore and de Goede, 2005; Amoore, 2006; Martin and Simon, 2008). For the subdivisions of the DHS charged with cybersecurity though, securing a (cyber) space that exceeded those territorially-based ideas about the Federal government's responsibilities required a "transition to a new national cooperative paradigm" (DHS, 2003, p. vii) where security would instead be a 'shared responsibility.'

To make the case for this transition to a new security paradigm, the DHS undertook boundary work strategies that drew an explicit categorical distinction between 'national security' and 'homeland security.' While they pointed out that "…traditionally, national security [had] been recognized largely as the responsibility of the federal government […] in the defense of [their] airspace and national borders," the security of critical infrastructures including cyberspace exceeded such a definition of federal responsibilities, when predicated on national borders in this way. This security imaginary was here alluding to the habitual necessity of being able to demarcate the bounds of the nation or territory to be defended: distinctions that had long played a constitutive role in shaping the organisation of the national security apparatus. In the DHS' first *National Strategy to Secure Cyberspace* (White House, 2003), the geographical basis for those distinctions was clear:

> In the last century, geographic isolation helped protect the United States from a direct physical invasion**.** In cyberspace national boundaries have little meaning. Information flows continuously and seamlessly across political, ethnic, and religious divides. Even the infrastructure that makes up cyberspace—software and hardware— is global in its design and development. Because of the global nature of cyberspace, the vulnerabilities that exist are open to the world and available to anyone, anywhere, with sufficient capability to exploit them. (White House, 2003)

As Megoran et al have argued in other contexts, "the border, whilst at the skin of the state literally, rhetorically is at its heart" (2005, pp. 734–5). In this imaginary then, what had formerly been a nation enclosed and physically bounded by geography and borders was now a subject with vulnerabilities that were 'open' to the world for exploitation, its borders no longer the skin they were once thought to be. Such a spatialised and embodied conception of vulnerability thus meant it was essential that solutions were found that could redraw those boundaries in new ways. Echoing those spatialised formulations, the DHS' report on securing critical infrastructure repeatedly emphasised that securing cyberspace and other critical infrastructures would require the federal government to "…draw upon the resources and capabilities of those who stand *on the new front lines*—our local communities and private sector entities that comprise our national critical infrastructure sectors." (DHS, 2003, p. 3, emphasis added). Securing cyberspace thus fell under the remit of the new categorical distinction that was 'homeland security' as something that "[could not] be accomplished by the federal government alone" (DHS, 2003, p. vii), but it would still be a spatialised endeavour.

Despite the early narratives about the global and open 'nature' of cyberspace then, the DHS increasingly worked to cast cybersecurity within a distinctly spatial lexicon. This work *for* boundaries took four main forms: through narratives of territoriality; imposing a scalar imaginary; a focus on physical infrastructures; and a shift to 'mapping' the nation in terms of risks.

Firstly, the DHS' early strategy and policy documents increasingly emphasised narratives of territoriality. This was not just about establishing how the nation's borders could be 'mapped' or redrawn in matters of cyberspace and infrastructure protection, it was also about defining and narrating the community (Sala, 2017). The DHS made appeals to community based on normative and symbolic values, not least of which was its own role as a security actor. Symbolically, this was a community in which critical infrastructure sectors provided "the foundation for our national security, governance, economic vitality, and way of life" and their continued reliability formed "an important part of our national identity and purpose" (DHS, 2003, p. viii). This was a task that represented more than just the protection of 'things' or infrastructures, it was the protection of assets that were "symbolically equated with traditional American values and institutions or U.S. political and economic

power." (DHS, 2003, p. viii). However, these assets were a "highly complex, heterogeneous, and interdependent mix of facilities, systems, and functions" dispersed amongst a broad range of non-governmental actors (DHS, 2002, p. 2). Such insecurity was represented in terms of cyberspace' dispersed and complex, widely distributed assets, so that a centralised federal government intervention was precluded on technical grounds as much as on normative grounds about the "traditions of federalism and limited government" (White House, 2003). According to this imaginary, the nation's normative and symbolic values were thus at stake in these appeals to community ideals, shifting the focus from the nation's external boundaries to its internal infrastructures.

Second, and as time went on, the DHS was increasingly imposing a scalar imaginary (Campbell, 2016) on their articulations and conceptions of 'cybersecurity.' What started as a matter in which 'national boundaries had little meaning,' scalar abstractions such as global, international, national, state, and local were cast like shadows from above to try and impose some order on how DHS imagined the 'homeland' in terms of cyberspace (Campbell, 2016). The primary goal of the 2003 *National Strategy to Secure Cyberspace* was not simply to secure computer systems and the networked infrastructures that relied upon them, but to enact a series of initiatives designed to secure 'cyberspace' as a whole. In doing so, it sought to translate the atomised practices of computer and network security – disparate practices undertaken amongst actors in "our communities and the individual institutions that make up our critical infrastructure sectors" (DHS, 2003, p. 3) – into a nationalised or territorialised conception of 'homeland' security. In effect, by speaking of computer or network security in terms of national, federal or even international scales with its implied judgements of magnitude and importance, the DHS was working to politically 'elevate' practices of securing computers and networks. This was no longer 'merely' a matter of localised (and private) computer and network security and therefore out of the reach of public government: describing it in such terms would make it a matter that a state could 'see' to govern (Scott, 1998).

The description of a decentralised, nodal and networked cyberspace that worked across territorial, sectoral and organisational boundaries meant that Cold War notions of isolating physical and information infrastructures "into 'stovepipes' to assure their protection" was "no longer adequate" (DHS, 2003, p. 8). Indeed, when the operating environment was conceived of in this way, the federal government could no longer keep 'defense' separate from 'offense' (DHS, 2008, p. i). As the previous chapter showed, drawing such distinctions operated as a political strategy for demarcating authority and political legitimacy, but for the DHS it would also suggest a specific set of organisational responses predicated on "mission bridging" through the Comprehensive National Cybersecurity Initiative (White House, 2009, p. 8). Though specific organisations were given (high-level, policy) responsibilities for cybersecurity early on, working out how to operationalise those responsibilities amongst federal departments and agencies would trigger a series of 'turf battles.'

Charged with expanding on "…the sharing of expertise, knowledge, and perspectives […] between network defenders" such as the DHS' departments, and their more 'offensively-minded' counterparts in the intelligence, military and law enforcement organisations (White House, 2009, p. 8), the DHS' efforts to establish its legitimacy and authority in matters of cybersecurity would be predicated on re-drawing such distinctions.

Unlike the "closed world" of the Cold War then (Edwards, 1996), mapping the lines of responsibility – and by extension, demarcating the DHS' role in cybersecurity – led them to advocate for being part of a distributed "homeland security enterprise" rather than a centralised or hierarchical state response (DHS, 2011, p. iii). This was not to be a matter that the national government claimed sole oversight for. The 'homeland security enterprise' was made up of "Federal, state, local, tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of America and the American population." (DHS, 2011, p. D-3). By demarcating cybersecurity along a scaled system, from federal, to state, to local, to individuals, their programs and imaginaries were a spatial practice built on a scalar imaginary of territory. This would gradually shape a shift from seeing the architecture of networked technologies as an existential threat, as was commonplace in the military cybersecurity imaginary discussed in the last chapter, to describing their approach as "levarag[ing] the distributed nature of cyberspace in its own protection" (DHS, 2011, p. 7). This framing by federal actors represented more than simply the exercise of commonly used and culturally embedded spatial expressions. As the later parts of the chapter will demonstrate, paying attention to how the imaginary is constructed and mobilised will show how it has had material consequences by shaping technical programs and initiatives.

Thirdly, a focus on the physical manifestations of this dispersed infrastructure would shape a gradual shift in the characteristics of cyberspace that DHS would emphasise. Having been tasked by the Homeland Security Act of 2002 with the protection of critical infrastructure, of which networked communications were just one of sixteen sectors, the DHS began to emphasise these networks' more 'physical' attributes. The seeds for this more 'grounded' conception of cyberspace's attributes were foreshadowed by the 2002 DHS Strategy when it described how infrastructures also included: "Our national icons, monuments, and historical attractions [and] preserve history, honor achievements, and represent the natural grandeur of our country." (DHS, 2002, p. vii). Drawing on an imaginary of monuments and 'natural grandeur' represented the physical instantiation of symbolic ideals and a national identity, but would also lead the DHS to shift its understanding of infrastructures in terms of a "[p]hysical protection dimension of homeland security." (DHS, 2002, p. vii). This was evidenced in cybersecurity strategy documents when the nation's dependence on "a network of networks" and "the information infrastructure" was described as controlling a range of physical objects, so that "the

reach of these computer networks exceeds the bounds of cyberspace." (White House, 2003). Contrary to DoD or other mainstream framings, cyberspace was not just the flow of virtual or digital information, or an informational 'domain,' it was increasingly described in terms of 'cyber-physical systems.'

Fourthly, such a shift of imaginary to 'mapping' cyberspace in terms of its physical systems, and mapping the nation as a field of vulnerabilities, was both a condition for, and a condition of, a particular organisational culture at the DHS (Collier and Lakoff, 2008). By describing cyberspace and its infrastructures in terms of its "highly complex, heterogeneous, and interdependent" characteristics, DHS was narrating how risk-based strategies would be the most feasible political response to protecting the "sheer numbers, pervasiveness, and interconnected nature" of these infrastructures. It was thus a "given [that] the immense size and scope of the potential target set" (DHS, 2003, p. 3) meant that by 2008 DHS were telling readers that "risk management" was to be "the primary basis for policy and resource allocation decision making" (DHS, 2008, p. i). In its desire to rationalise the department's allocation of scarce resources when addressing this conceptualisation of a complex and interconnected infrastructure, the DHS would match this problem framing with solutions for risk mapping and 'Modeling, Simulation, and Analysis Initiatives' (DHS, 2003). As later parts of this chapter will show, such risk-based thinking is notable for how it imagines networks as a two-dimensional surface in which a spatial approach of 'bounding' and perimeters can be applied, despite the increasingly complex topologies of user devices and 'cloud' computing.

By 2011, the DHS's cybersecurity strategies and documents would articulate a distinctive vision of a desirable future from those of their military and intelligence colleagues. A further corollary of their organisational penchant for risk-management approaches was that, combined with its scalar imaginaries and its growing emphasis on constituting 'the homeland' in terms of physical infrastructures, a spatial framing of cyberspace in terms of 'environments' and 'ecosystems' became a more intuitive concept than information 'domains.' In their *Blueprint for a Secure Cyber Future*, the DHS described a 'roadmap' that consisted of two areas of action: "Protecting our Critical Information Infrastructure Today" and "Building a Stronger Cyber Ecosystem for Tomorrow" (DHS, 2011, p. iii). Invoking an imaginary of stewardship, their vision of a 'secure cyber future' was predicated on *protecting* cyberspace rather than *defending* it, again drawing distinctions to the terms that the DoD had been advocating for (c.f. Lynn, 2010; DHS, 2011, p. vi). Rather than focusing on threats from outside the homeland, the DHS would increasingly shift its focus to the characteristics of an ecosystem of 'physical, cyber and human' components to shift the spatial imaginary away from 'domains.'

As we shall see in the next section though, different federal actors have emphasised different spatialising characteristics in different ways, according to their interests and organisational cultures.

These competing interests during this period contributed to DHS engaging in a 'turf battle.' As with the other chapters in this thesis, another animating factor in the turf battle was the competing, contested and ambiguous conceptualisations of the matter at hand. 'Cybersecurity' is contested bureaucratically, politically and technically and turf battles such as these are about who gets what and why. Spatial and scalar imaginaries have informed a significant amount of largely competetive boundary work in turf battles between DHS and DOD. As we saw in Chapter Three, this was a time during which the US had invested a great deal of resources and political effort in establishing a new combatant command dedicated to cyberspace, despite the economic crisis of 2008-2009 and ensuing sequestrations of budgets. This meant there were institutional and political interests within the DoD, Congress and the defence industry to see CYBERCOM (and by extension, the NSA) extend its capabilities. Meanwhile, advocates for DHS's role had their own institutional interests in defining its role in overseeing critical infrastructure protection and institutionalising its own capabilities. More than just bureaucratic and political contestation, by working *for* boundaries, boundary work here would define priorities, allocate resources for carrying out different tasks related to cybersecurity, and embed competing visions and goals into the boundary infrastructures discussed in Part Three. This turf battle therefore provides a useful starting point for analysing how security actors enact, control and contest consequential distinctions. In the next section, we will see how, despite early narratives about the 'borderless nature' of cyberspace, DHS have worked to translate and reaffirm territorial and spatialised distinctions in matters of cybersecurity.

4.2 Part Two: DHS' credibility on the line

Working out security roles and responsibilities for 'cybersecurity' has been a matter of political, technical, and organisational contention for more than two decades, but this was particularly evident in the period between 2002 and 2014. These were fundamentally opposing visions of who 'cybersecurity' should belong to, and which state agencies should have what roles and responsibilities. Boundaries would be worked out, or *worked for*, at two levels: the expansive policy level, and the granular technical levels. The granular level was concerned with technical programs and bureaucratic politics that produced and enacted cybersecurity in practical and organisational terms, where Part Three will turn its attention. The expansive (and the more nebulous) aspect of the pursuit of bounding 'cybersecurity' was where government actors sought to expand technical programs to the level of national security, and where they worked to extend cybersecurity to national policy level debates, defending, contesting and recreating boundaries in the process (Mueller and Kuehn, 2014). At the policy level, the period 2002-2014 was the time that saw the Department of Homeland Security consolidated as the focal point for the cybersecurity of the nation's critical infrastructure.

Although the 2003 cybersecurity strategy had designated the DHS as the lead agency for domestic cybersecurity, how its roles and missions fit within territorial distinctions were still the subject of contestation five years later. This was exemplified by a formative bipartisan report written by members of Congress and the Center for Strategic and International Studies think-tank in 2008. The Center for Strategic and International Studies' (CSIS) Commission on *Securing Cyberspace for the 44th Presidency* was established in August 2007 to examine the state of the art for policy and strategy ahead of the next administration. The Commission was co-chaired by House Representatives Jim Langevin and Michael McCaul and it was notable for how they contested DHS' suitability for overall responsibility for the cybersecurity mission based on a characterisation of 'the domestic mission.' Their objection was that "…[s]ecuring cyberspace is no longer an issue defined by homeland security or critical infrastructure protection. This is far too narrow a scope. Cybersecurity is no longer (if it ever was) a domestic issue." (Langevin *et al.*, 2008, p. 35). According to this logic, cyberspace exceeded distinctions between the domestic and the international in such a comprehensive way that the DHS was not the suitable agency for this task. Furthermore, this articulation of the problems posed by cyberspace was predicated on distinguishing between external (threat) actors who possessed their own agency in contrast to the United States' own agency as an actor. Approaching cybersecurity in terms of a specific characterisation of the 'foreign intelligence agencies and militaries' facing the United States meant that…

> …DHS is stronger in 2008, but even if DHS were strengthened further (and some in the Commission believe this could be done rapidly), the nature of our opponents, the attacks we face in cyberspace, and the growing risk to national and economic security mean that comprehensive cybersecurity falls outside the scope of DHS's competencies. DHS is not the agency to lead in a conflict with foreign intelligence agencies or militaries or even well-organized international cyber criminals. (Langevin *et al.*, 2008, p. 35)

By drawing attention to the external agency of threat actors, the Commission was challenging the DHS' competency in the matter of cybersecurity, because according to this logic, the same legal and normative distinctions that had informed the designation of the DHS as the lead agency also meant that they were ill-equipped to 'lead a conflict.' The implication here was that conflict was and should be a task assigned to the US' military and intelligence agencies. Langevin and McCaul likely had their own interests in articulating the problem in such terms: cybersecurity contractors General Dynamics, Raytheon, Deloitte and BAE were some of their biggest election contribution sources for the 2010 elections (Carney, 2011) and the report would have promoted a vision of cybersecurity that could generate lucrative government contracts for such companies (Brito and Watkins, 2014).

The Commission's recommendation was based on a specific reading of the problem, namely that cybersecurity should be thought of as a 'battle' or a 'conflict' between actors. Conceptualising the problem as one posed by motivated or agential threat actors suggested a specific approach to the problem and this would be an important motif in cybersecurity politics in the years to come. On the one hand, military and intelligence actors would focus on threats, and the external agency of threat actors, in distinction to the United States' own agency as an actor. Meanwhile, to consolidate their capabilities and credibility, DHS would end up shifting the focus to the internal vulnerabilities of the homeland to be secured. It was up to DHS and its supporters to draw distinctions so that other ways of approaching cybersecurity (distinct from that of the military) could be politically possible.

Such arguments in favour of the military's role in cybersecurity were based on pragmatic reasoning about the DoD's superior technical and organisational resources. This meant that the DHS had practical difficulties in drawing links between 'homeland security' and cybersecurity. When Jane Lute took office as Deputy Secretary of Homeland Security in 2009, as the lead agency for cybersecurity and critical infrastructure protection DHS was expected to execute that mission with just twenty-four computer scientists: the Department of Defense on the other hand employed more than seven thousand (Harris, 2014, p. 160)**.** This disparity in resources was one of the main factors that Rod Beckstrom, the head of DHS' critical infrastructure and cybersecurity subdivision the National Protection and Programs Directorate (NPPD), cited in his resignation letter that year. He had been tasked with heading the nascent National Cybersecurity Center (NCC) which was responsible for protecting the US Government's communications networks. In addition to the lack of resources, he also described the NSA's overpowering involvement in strong terms, complaining that "NSA effectively controls DHS cyber efforts through detailees, technology insertions and the proposed move of NPPD and the NCC to a Fort Meade NSA facility." (Beckstrom, 2009) He was concerned that "NSA dominates most national cyber efforts" and as a result these efforts were strangling the DHS' nascent initiatives before it could assert its own authoritative standing (Beckstrom, 2009). Despite initiatives intended to carve out DHS's role in cybersecurity, in practical terms the NSA still had control and oversight in some important ways. While DHS had officially assumed the mission of homeland cybersecurity on the basis of such historically resonant distinctions, they would therefore have to work hard to make sure that the DoD's organisational and technical impetus did not make this a permanent arrangement.

Pragmatic arguments about the DoD's organisational and technical advantages over the DHS would have potentially far-reaching consequences for the longstanding restrictions on military actions within domestic domains. These debates would shape the kind of cybersecurity programs and the kinds of organisational priorities that would get funded. While at the policy level the DHS was responsible for securing domestic cyberspace, at the programmatic and technical level some advocates for the DoD were working to expand the Pentagon's remits. By the time that General

Alexander assumed the controversial "dual-hatted" role (discussed in the previous chapter) as commander of CYBERCOM in addition to his role as director of NSA in 2010, the DHS had already had several Government Accountability Office (GAO) audits challenging their capabilities (e.g. Powner, 2009; Government Accountability Office, 2010), as well as the CSIS Commission Report described above. Alexander's confirmation hearings demonstrate some of the ways that those advocating for increased DoD's responsibilities for defence of the nation through cybersecurity would identify specific 'policy gaps':

> …policy gaps exist that prevent us from doing all that can be done to increase the cyber security of the Nation, especially our Nation's critical infrastructure. Foremost amongst these gaps are the potential impediments to the public-private cybersecurity information sharing partnership, which I believe is critical to more effectively attributing and countering this threat. (Alexander, in US Senate, 2010, p. 235)

In distinction to DHS' more competitive strategies, Alexander here was trying to downplay these historically resonant distinctions, working *at* the boundaries of the DoD's concept of cybersecurity to expand their remit. Implied in this discussion of 'policy gaps' was an expanded role that the DoD should play to fill those gaps. Here, Alexander was suggesting that those tasked with the security of 'our Nation's critical infrastructure' had not done 'all that can be done.' It was sentiments in testimony such as this that would shape the DoD's efforts at exploring and trialling different ways of extending their military resources into defense contractor networks, the DIB initiative discussed later in Section Two. As far as Alexander and some members of the Senate Armed Services Committee were concerned, the open and unbounded nature of attacks through cyberspace problematised existing authorities predicated on distinctions between 'internal' and 'external' security. Actors who were advocating most strongly for the DoD's leadership in matters of cybersecurity would be the ones to emphasise the ways that cyberspace challenged the traditional demarcation of labour between domestic and foreign agencies, seeking to renegotiate or downplay distinctions. As discussed in Chapter Three, by this point DoD had declared cyberspace as a domain of warfare and had clearly articulated their policies and strategies for supporting military operations abroad, but the question of who should defend against attacks on domestic networks was still open to contestation, or even how to draw the bounds of 'domestic networks' and 'portions' of cyberspace in distinction to 'international' cyberspace.

In order to bound 'domestic' networks in such a way as to stabilise their claims to jurisdiction, during DHS' formative years between 2002-2014 DHS advocates would begin to shift the emphasis away from cyberspace's claimed borderless qualities to a focus on the ways that distinctions between internal and external could be mapped into interpretations of cyberspace and cybersecurity, thereby

working to defend ad recreate boundaries in distinction to the DoD. Deputy Director Lute and counsel Bruce McConnell of the DHS took umbrage at Alexander's efforts in speeches and Congressional testimony to reconfigure the bounds of CYBERCOM's responsibilities, and wrote an op-ed piece in *WIRED* magazine to contest the military's role in defending cyberspace:

> These days, some observers [i.e. Keith Alexander and NSA] are pounding out a persistent and mounting drumbeat of war, calling for preparing the battlefield, even saying that the United States is already fully into a "cyberwar," that it is, in fact, losing. We disagree. Cyberspace is not a war zone. Conflict and exploitation are present there, to be sure … But the vast majority of cyberspace is civilian space. (Lute and McConnell, 2011 n.p.)

Lute and McConnell were implicitly invoking the long-standing divide between the domestic sphere governed by civilian agencies and the military's jurisdiction in matters of warfare. While Alexander had posed the diffuse nature of cyberthreats as the justification for extending military responsibilities in domestic cyberspace, Lute and McConnell contested this with a more moderated view of cyberspace's borderless qualities:

> Though it relies on machines – e.g., servers – that are each physically somewhere, connected by communications technology that spans the globe, *cyberspace is a place where geography matters differently, the reach of national law is incomplete, and the role of nation-states in its security is an open question...* No single actor has the capability to secure the largely privately owned virtual world that straddles national boundaries. (Lute and McConnell, 2011 emphasis added)

For representatives of the DHS, geography still mattered in cyberspace, even if it mattered 'differently'**:** such definitions would have important ramifications for asserting their jurisdiction over matters of cybersecurity in and beyond the homeland. Emphasising that national boundaries could be 'straddled' without being negated was an important distinction to make for the agency with responsibilities for domestic threats and vulnerabilities. Framed by the imaginary discussed above, they would work to translate and produce these distinctions through technical programs too.

Demarcating the bounds of 'domestic' networks was thus a matter of contention. Alexander was not apparently perturbed by Lute and McConnell's public rebuke. A few days later he presented very similar remarks at a conference in Washington D.C. about domestic security, suggesting early on that "…[t]here's a lot of folks that say we'd like the technical capabilities of NSA … but we don't want the NSA in there" (Alexander, 2011 n.p.). He went on to assure that audience that "…[w]e don't want to be in [the civilian networks]. We want to help protect it. We don't want to spy, we want to protect you" and joked that so many other hackers, governments, and malicious actors were already in civilian

networks that **"…**the only ones not in your networks today are us. There isn't enough room for us in there." (Alexander, 2011 n.p.) Talking about civilian networks in such spatialised terms, as a space that NSA could be *in*, suggested an effort at bounding the external perimeters of that network space so that intelligence or military agencies could patrol that perimeter. At the same time, patrolling that perimeter would require visibility into what was happening 'on the inside': in another speech about responding to attacks on critical infrastructure, he argued that "[i]n order to stop it, you have to see it in real time, and *you have to have those authorities*," (Alexander, cited in Nakashima, 2012c, emphasis added). His public efforts to problematise the DoD's traditional lack of remit over domestic infrastructures was thus couched in spatialised distinctions between a network interior and a hostile exterior, and he was advocating for further authorities in order to enact that approach to cybersecurity.

Bureaucratic wrangling and competitive turf battles over DHS' roles and jurisdictions would have technical and technological repercussions. So far, the chapter has analysed some key moments in these bureaucratic and political battles because it is necessary for understanding why the initiatives discussed in the next section took the shape they did. In Part Three, we will now see how these were more than just rhetorical efforts to build support for preferred courses of action, but were also a constitutive part of the policies and initiatives that followed. Much as Alexander described network 'interiors', we will see how military actors would try to produce a 'homeland' by enacting and managing the 'external' boundaries of that homeland as part of efforts to constitute cybersecurity in terms of external threats, downplaying boundaries that had traditionally constrained military remits for action. Meanwhile, civilian agencies and DHS actors would seek to produce a 'homeland' by enacting and managing 'internal' boundaries of that homeland, as part of their efforts to constitute cybersecurity in terms of internal vulnerabilities. Through an analysis of some key initiatives, the following section will argue that security actors are constituting 'cybersecurity', and also constituting a 'homeland,' by linking boundaries of the two together. By invoking or drawing on distinctions about 'the homeland,' 'internal,' and 'external,' actors are 'domesticating' cybersecurity, and this particular approach to cybersecurity is in turn constituting a 'homeland' to be secured.

4.3 Part Three: bounding 'Homeland' cybersecurity

While longstanding institutionalised distinctions between internal and external security had been formative in giving DHS the responsibility for homeland cybersecurity, defining (and defending) the parameters of that role was about more than just the rhetorical turf battles discussed in the previous section. The difficulties that DHS were having in bounding cybersecurity and 'domestic cyberspace' were working out in several key initiatives and programs. The first initiative that helps this

chapter demonstrate these efforts to translate such distinctions into 'cybersecurity' is the Comprehensive National Cybersecurity Initiative (CNCI), developed in 2008. Created towards the end of the Bush Administration, the CNCI was a program that involved a range of government agencies, with tasks assigned to DHS, the FBI, the NSA, and the OMB amongst others as a "mission bridging" exercise (White House, 2008). There were many different programs under the broader umbrella of the CNCI's funding, but three programs are salient for the purposes of this chapter: the 'National Cybersecurity Protection System' (including 'EINSTEIN,' and the Continuous Diagnostics and Mitigation (CDM) program); the 'Trusted Internet Connection' (TIC) program; and the NSA's 'Defense Industrial Base' pilot program[8]. As we shall see, through programs such as these the CNCI was intended to outline and enact the parameters of the federal government's responsibilities in distinction to those of private sector operators, building on the assumptions set out in the 2003 *National Strategy to Secure Cyberspace*. However, this would entail a series of technical and organisational challenges. Specifically, these were challenges related to defining and defending the 'federal domains' that the government and the DHS were claiming responsibility for. Bounding this remit would be an important part of bounding and producing the state's approach to cybersecurity.

4.3.1 'National Cybersecurity Protection System:' Bounding 'the homeland' at the technical level.

Efforts to bound 'federal domains' – plural, rather than the singular cyberspace-as-domain framing – were full of spatial connotations and were a prominent feature of the Obama administration's publication of the hitherto classified CNCI in 2010. This version of the initiative identified three major goals that were "designed to help secure the United States in cyberspace", the first of which was to "establish a front line of defense against today's immediate threats" (White House, 2010). Meanwhile, the second and third goals were to "defend against the full spectrum of threats" and to "strengthen the future cybersecurity environment" (White House, 2010). Each of these goals have a spatial element, whether it is to establish a defensive 'front line', act as a barrier to a spectrum (or field) of threats, or strengthen an 'environment.' Such language is indicative of a culturally specific way of approaching matters of security, where producing lines between a safe inside and a dangerous outside both shape and subsequently constitute the kinds of policy responses that emerge (Campbell, 1998; Weldes *et al.*, 1999). This can be demonstrated in each of the following programs. The CNCI played a constitutive part in building a distinctive role for the DHS in cybersecurity,

[8] The 'Defense Industrial Base' was designated as one of the sixteen critical infrastructure sectors identified in the 2003 Homeland Security Strategy for Critical Infrastructure. This was made up of the defence contractors and manufacturers that the DoD were reliant upon, and was the only counterintelligence sector the DoD were tasked with organisational responsibility for.

though mapping boundaries of 'internal' and 'external' security into technical programs was to be an acute challenge. As we shall see, despite the programs' technical failures and organisational shortcomings, DHS was still able to 'domesticate' or 're-territorialise' cybersecurity and thus constitute a distinctive role for itself based on boundary work that referenced 'internal' and 'external' security.

One of the technical programs that best illustrates the difficulties that DHS had in establishing 'a front line of defense' and in constituting an internal space to secure through the CNCI was the 'National Cybersecurity Protection System (NCPS).' The NCPS was operationally known as 'EINSTEIN', a program that evolved over three numbered iterations. It started as an intrusion detection system to monitor for known malicious software "threat signatures," like fingerprints for malware, in the internet traffic flowing through the network gateways of federal civilian executive branch agencies. The DHS' description of the program on their website is worth quoting at length for its spatial analogies, where they suggested thinking of EINSTEIN in terms of "physical protections at a government facility":

> The first phase of EINSTEIN, known as EINSTEIN 1, is similar to a camera at the entrance to the facility that records cars entering and leaving and identifies unusual changes in the number of cars. EINSTEIN 2 adds the ability to detect suspicious cars based upon a watch list. EINSTEIN 2 does not stop the cars, but it sets off an alarm. In sum, EINSTEIN 1 and 2 detect potential cyber attacks before they can enter the facility. The latest phase of the program, known as EINSTEIN 3A, is akin to a guard post at the highway that leads to multiple government facilities. EINSTEIN 3A uses classified information to look at the cars and compare them with a watch list. EINSTEIN 3A then actively blocks prohibited cars from entering the facility. Using classified information allows EINSTEIN 3A to detect and block many of the most significant cybersecurity threats. (CISA, 2020b)

In other words, the EINSTEIN program in its various iterations was intended to act as a "perimeter defense" (CISA, 2020b) at the boundaries of government networks. However, there would be many technological as well as organisational impediments to this approach.

Producing the 'front line of defense' for federal cybersecurity that the CNCI had envisioned was pursued in a remarkably literal sense at the technical level. Underpinning the deployment of EINSTEIN's scanning and inspection capabilities were efforts to aggregate network traffic through as few external connections as possible (CISA, 2020b). Known as the Trusted Internet Connections (TIC) program, this effort was initially intended to consolidate federal connections to the public Internet so that EINSTEIN capabilities could be deployed at each of those access points, so as to monitor traffic going into or exiting government networks. Before this program, federal agencies were autonomous

in their sourcing of internet service connections, with the result that the number of external connections was nearing 5,000. The TIC program intended to reduce this number to fifty approved external access points (Mueller and Kuehn, 2014). In this sense, programs such as the TIC and EINSTEIN were designed with the intention of physically managing the bounds of the federal government's attack surface, of producing bounded 'federal domains' that were defensible in a manner synonymous with a fortress or territorial space. This in turn was intended to help constitute the DHS' approach to cybersecurity, by constructing a physical incarnation of the federal cyberspace that it had been tasked with securing since the 2002 Homeland Security Act.

However, technologically bounding federal network connections in such a way proved to be unmanageable. The spatialised focus on perimeter security and the desire to consolidate federal civilian network connections had produced a technical program that was focused on threat indicators, by scanning network traffic flows for malicious activity and comparing it to known signatures. However, as the DHS' Assistant Secretary at the Office of Cybersecurity and Communications acknowledged in Senate testimony defending the program, the effectiveness of these perimeter defences was only as good as the information that was fed to them (Ozment, in US Senate, 2015b, p. 27). Senators had appreciated Ozment's explanation of the program in non-technical terms when he had likened the program to the physical protections surrounding a government facility, such as fences and guard posts looking for suspect car traffic. However, these defences were "a necessary but not sufficient technology" on their own (US Senate, 2015b, p. 27). This was a recognition of the technical shortcomings of a system that could only detect familiar threat signatures and that it had not been widely deployed, for it had not been consistently deployed across the federal networks and could not 'see into' all the traffic that it did monitor. Metaphorically speaking, for the 'perimeter fence' to be effective it needed to encompass the entire facility. DHS representatives would have been aware of its technical limitations in this regard, given that there had already been a series of public reports criticising the program. In 2014 the DHS' Inspector General described major flaws in how DHS was managing the program, including lack of performance measures and timelines, inadequate privacy protections, and minor vulnerabilities in Top Secret computer systems (DHS Inspector General, 2014). Later, in 2016, the program was again criticised by the General Accountability Office (GAO) for the focus on signature-based intrusion detection, revealing that in testing EINSTEIN the GAO auditors discovered that the program failed to detect 94% of the signatures tested (General Accountability Office, 2016; Smith, 2016).

Another problem the program faced in trying to bound and manage the federal networks like a single domain was that posed by cyberspace's architectures. Since sensors for EINSTEIN 1 had been deployed on network connections in 2005 as a perimeter defence, and EINSTEIN 2 in 2008, their effectiveness had been grounded on being able to demarcate the federal networks' parameters and

subject them to a kind of technical scanning that required insight into network flows. The scale of the government's connected and interconnected information systems, databases and agencies was one of the reasons that DHS struggled to produce credible boundaries between those networks and 'cyberspace' more broadly. Testimony by DHS Acting Deputy Under Secretary for Cybersecurity in 2017 explained that there had been delays to rolling the programs out because of the technical challenges of "accommodating a large and diverse customer set with unique network infrastructure and technical concerns, such as Internet Protocol version 6 and Domain Name System Security Extensions capabilities, lack of consolidated Domain Name System, and outdated infrastructure" (Manfra, in US House of Representatives, 2017b, p. 51). Translating distinctions between internal federal cyberspace and external non-federal cyberspace was apparently impeded by their "sprawling and disparate Federal networks" (Rep. Thompson, in US House of Representatives, 2015b, p. 7), and consolidating those connections and diverse technological protocols and systems was proving to be a technical feat too complex for EINSTEIN to achieve as a single program.

Furthermore, the deployment of different iterations of the EINSTEIN program had been stymied by procedural, bureaucratic and organisational difficulties. While DHS had been given the task of helping federal agencies defend their networks with programs like EINSTEIN, the DHS did not have any means of regulating or forcing its uptake. While they could issue 'binding operational directives', there were no consequences for agencies not adhering to the directives (US House of Representatives, 2015e, pp. 31–32) and uptake of the program was slow, indicative of the lack of credibility that DHS possessed at the time (Deppisch, 2019). For those agencies that did sign up, there were "tremendous procedural hurdles" that agencies would have to navigate to buy, secure and allow technologies to be integrated into federal networks (Ryan Gillis, former member of cybersecurity directorate at DHS, cited in Otto, 2015).

Describing the 'National Cybersecurity Protection System' (NCPS) in terms of distinctions between 'internal' and 'external' network space was therefore more than just rhetorical boundary work: EINSTEIN's technical design was predicated upon trying to reproduce spatialised boundary distinctions by constructing a perimeter and installing sensors on it to defend against 'external threats,' using technology that could inspect traffic coming in and out of the federal network. As well as indicating a degree of bureaucratic inertia, this also suggests how persuasive lawmakers and DHS officials have found the programs' promise to produce distinctions between internal network space and external threats, of keeping threats 'out', despite EINSTEIN's apparent technical limitations in constituting those distinctions. While Congressional leaders were pointing out that more than 10 years on, "only half of the Federal civilian agencies have deployed the latest version of EINSTEIN" (US House of Representatives, 2015b, p. 7), iterations of the program have continued to receive Congressional mandates to expand across Federal agencies.

Rather than abandon the project, the awareness of these technical limitations would lead DHS advocates to shift the focus. Instead of than relying on a technology to keep threats out, DHS started to advocate for programs that could deal with threats *inside* the network, both shaping and echoing the broader organisational imaginary discussed earlier in Part One. Even while defending the program to Senators in this Homeland Security Appropriations hearing to advocate for its sustained funding, Ozment continued with the spatial analogies to suggest that the technology still needed further refinement:

> The final aspect of it is that it's necessary to have a fence, and it is great that our fence uses classified information that makes it a cutting-edge fence*. It is still not sufficient*. […] there is no one tool, no one security measure that solves the security challenge. Just as in a physical building you have multiple layers of security—a fence, guards, cameras, locks on doors—you have to have the same in cybersecurity. (US Senate, 2015b, p. 27, emphasis added)

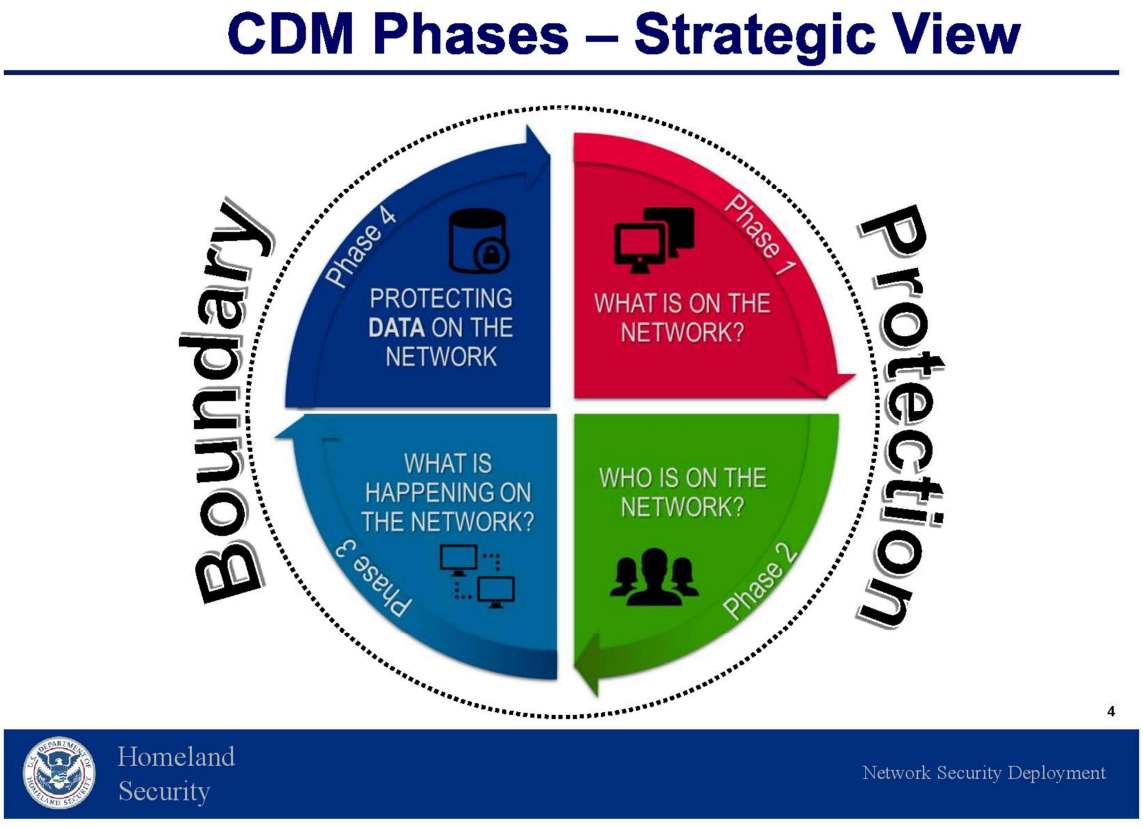
By 2015, DHS officials were recognising that 'securing the perimeter' with the 'fence' that was EINSTEIN on its own was no longer sufficient in their efforts to fulfil their responsibilities for federal cybersecurity. By describing cybersecurity in terms of 'multiple layers', DHS programs were thus shaping how actors understood and addressed the problem in spatialised terms. Ozment's testimony in 2015 was a reflection of broader DHS descriptions of EINSTEIN as "no silver bullet" on its own (CISA, 2020b), whilst simultaneously leaving room for further programs and iterations by alluding to DHS' need for more 'layers' of security programs.

Having recognised the difficulties that networked architectures posed to comprehensively aggregating federal networks to protect them from external threats, other programs were developed by DHS to 'fill in the gaps' left by EINSTEIN's program. Congress provided funding in the 2013 DHS Appropriations Act to implement another program, the Continuous Diagnostics and Mitigation (CDM) (Homeland Security Secretary Napolitano, in US Senate, 2013c, p. 96). If EINSTEIN had been technically inadequate for defending the network's perimeters on its own, the CDM was viewed as the "security on the inside" of the government's network (Ozment, in US Senate, 2015c, p. 27). DHS had a facilitating role in providing that extra tool, with Ozment going on to tell Senators that "[a]gencies have to do more of that internal security based upon their unique needs and missions, but Continuous Diagnostics and Mitigation is a program [that] we have to help agencies with that" (US Senate, 2015c, p. 27). According to the program's publicity documents by the DHS in 2013, the "CDM Program is a dynamic approach to *fortifying* the cybersecurity of computer networks and systems" (DHS, 2013, emphasis added), again invoking the spatialised language of bounding the federal networks to protect from external threats. By this point, iterations of the EINSTEIN program had been in development for

more than a decade and would have acted as a formative model and reference point for DHS's efforts to consolidate their cybersecurity roles.

The influence that the EINSTEIN program had on the design decisions of programs that DHS devised in response to EINSTEIN's limitations can be seen in the way that the CDM was described in a progress report in 2016. CDM involved agency-installed sensors being deployed on networks to perform ongoing autonomous searches for known cyber flaws, with data getting transmitted back to a central dashboard at that individual agency (DHS, 2020). The program had a four-phased development of requirements, and the intent for CDM to 'bound' federal networks was made explicit in a Powerpoint presentation that the DHS' Chief of Cybersecurity Assurance gave in 2016. The CDM capabilities were intended to initially describe 'what was on the network' by cataloguing the devices and endpoints, then phase two would add a capability to check 'who was on the network' by checking user credentials and privileges; phase three would monitor and scan for 'what is happening on the network' and phase 4's capability would be to 'protect the data on the network' (Stanley, 2016). The intended cumulative effect of these phases was that it "BOUND" (sic) and 'protect the boundaries' of the network (Stanley, 2016, p. 2). In this sense, CDM was further consolidating the work of EISTEIN in producing a technological boundary to protect from 'external' threats, but now it would also look for those threats inside the network. (see FIG 4.1)

FIG 4.1: 'Bound' the network'. Taken from Stanley, 2016 p.4



Distinguishing between 'inside' and 'outside' the network was to be an enduring gauge for the effectiveness of the DHS' programs throughout their lifetime. In Congressional testimony responding to criticisms of the EINSTEIN program in the GAO's 2016 report (General Accountability Office, 2016), as Acting Deputy Under Secretary for Cybersecurity Jeanette Manfra presented CDM as part of the DHS' solutions to the GAO's recommendations to improve their approach to federal cybersecurity. In written responses to questions from the Committee, Manfra described the CDM as…

> …focused on monitoring the internal assets of an agency's network and NCPS's EINSTEIN is positioned on the external network boundary, [so that] combining data from both programs will allow DHS to understand potentially malicious activity that cannot be understood by either program in isolation (US House of Representatives, 2017b, p. 57)

The combination of CDM and EINSTEIN were thus represented by DHS as how they envisioned achieving their cybersecurity mission to secure the dot.gov networks. A key part of this formulation that distinguished between 'inside' and 'outside' networks was that in tandem, these programs would enable DHS to cover more of the network with their sensors and thus get a clearer 'vision' of what was happening on those networks. As Ms Manfra described them, a key objective of these programs was to enable DHS to "address the evolving threat by extending external visibility into internal agency structures" (Manfra, in US House of Representatives, 2017b, p. 45). These programs were intended to play a key part of DHS constituting the 'space' to be secured, and their visibility into it. The importance of an ability to "see bad actors on the networks, once they're already through the perimeter" was something that Chris Cummiskey (who until 2014 was DHS's acting undersecretary for management) reflected upon when describing the benefits of CDM over EINSTEIN (cited in Lyngaas, 2015).

Similarly, in 2015 they were still defending the programs in spatial terms. Despite the technical shortcoming DHS had faced with using EINSTEIN as a tool to demarcate a network perimeter, the Secretary of Homeland Security defended the program by describing the visibility that the programs afforded, arguing that:

> The Einstein system is the only system that can give situational awareness across all of the federal government. One thing we don't want to do is have everyone go off on their own and have their own discreet view, *because we want to see the whole battle space*. (Johnson, cited by Otto, 2015, emphasis added)

As the comments from the Secretary indicate, for all its shortcomings the long-running program was still being defended by the DHS as the most effective means of gaining the situational awareness they viewed as a crucial component for distinguishing their mission from other state agencies. To defend

the federal network, they had to 'see the whole battle space' and the CDM was viewed as a necessary addition to the NCPS. A focus from early on in the DHS' life on the threats coming from outside the network had produced a particular set of programs in which DHS had now invested a significant amount of money and effort. This in turn meant that the programs had been shaping the way that DHS approached the 'threats' as external to the network.

DHS would thus have trouble 'domesticating' cybersecurity while they focused on 'threat' and 'battlespace' framings and technical boundaries that programs like NCPS sought to constitute. EINSTEIN and CDM were based on old technologies and approaches to information security, with one senior DHS official describing latest iteration of the program, EINSTEIN 3 as "really where we needed to be 15 years ago" (Greg Touhill, cited in Otto, 2015). In 2010, Suzanne Spaulding, who would become the Under Secretary of the NPPD in 2013, was already describing why thinking of cybersecurity in terms of building defensive boundaries was outdated, where the "promise of an impervious cybersecurity shield protecting vast amounts of information from a determined and sophisticated adversary is at best a distant dream, and at worst a dangerous myth." (Spaulding, 2010). The problems of approaching cybersecurity in terms of programs that tried to recreate distinctions between internal network security and threat actors that originated outside those networks led Senator Tom Coburn to highlight the problems with DHS' cybersecurity programs as part of a comprehensive review of all of the DHS' roles (Coburn, 2015). For DHS' cybersecurity role, the report drew attention to the problems of their threat-based approach as embodied by the NCPS, and recommended that "Congress and the Department should fundamentally rethink DHS's strategy for safeguarding and securing cyberspace" because of "the limits of vulnerability mitigation—and that the idea of a cyber shield securing our networks is a dangerous illusion" citing instead "the understood benefit of deterring adversaries" (Coburn, 2015, p. 97). 'Deterring adversaries' was something that the military agencies were making a strong case for (see Chapter Three), which meant that the DHS had to differentiate themselves if they were going to retain a grip on their share of cybersecurity policies and programs.

At the same time as the NCPS and TIC programs, the other issue that DHS were grappling with was their mission to protect critical infrastructure. Here, they were having to demarcate their mission from a DoD that was advocating for more authorities during this period. In addition to protecting U.S. federal civilian government agencies cyber networks, legislation had also tasked DHS with leading the protection of critical infrastructure and its connections to cyberspace (Napolitano, 2011). As the next section will illustrate, another program that fed data into EINSTEIN would also work *for* boundaries and help DHS constitute and consolidate its approach to cybersecurity.

4.3.2 Domesticating cybersecurity at the policy level

While EINSTEIN 1 and 2 were a key program in DHS' efforts to bound federal networks, they also had to consolidate their role as lead agency responsible for coordinating the cybersecurity of critical infrastructure. As the discussion in the first part of the chapter showed, the period between 2009 and 2014 was one of the most fraught for DHS' cybersecurity identity, in the context of the newly established CYBERCOM and General Alexander's efforts to expand the capabilities of the DoD in matters of cybersecurity. The Defence Industrial Base (DIB) 'pilot' scheme was to be a key program in shaping and constituting the DHS' approach to cybersecurity. In November 2011, the Washington Post reported on a pilot being run by the Pentagon since July in which the NSA possessed and distributed threat signatures, and acted as the primary interface with Internet Service Providers (ISPs) who would in turn use that information to monitor the internet traffic of twenty-five defence firms in the trial (Nakashima, 2011). The program was predicated on the same kind of technology as EINSTEIN 3: sensors would be installed on the external network connections of organisations, and the network traffic inspected by automated signature detection programs to compare it with known threat signatures. The NSA would provide the signatures, but the Internet Service Providers would operate the sensors.

The DIB pilot scheme was an effort to trial and extend the Pentagon's roles in cybersecurity. Deputy Defense Secretary William Lynn had advocated for an initiative such as this in 2010 when he argued that "…the Pentagon must leverage its ten years of concerted investment in cyberdefense to support broader efforts to protect critical infrastructure," even while recognising that the government would have to consider whether it was "necessary and appropriate" to do so (Lynn, 2010 n.p.). In other words, Lynn realised that the 'long normative and legal' restrictions (discussed earlier) on 'appropriate' military actions in domestic contexts were likely to be a source of contention as the Pentagon trialled its involvement in protecting the 'critical infrastructure' of the Defense Industrial Base. Although the DoD had been allocated in legislation as the lead agency for coordinating and managing the cybersecurity of the DIB, they had to work out what this would look like in practice, at the localised level.

If it was successful, the DIB Pilot scheme had the potential to shift the boundaries of the military's role in critical infrastructure protection within the homeland. As Lynn stated at a global security conference in 2011, "We hope the […] cyber pilot can be the beginning of something bigger. It could serve as a model that can be transported to other critical infrastructure sectors, under the leadership of the Department of Homeland Security." (cited in Banusiewicz, 2011). Though Lynn was careful to point out that there would still be a role for DHS, the scheme would still need to convince Congress, citizens and the owners of critical infrastructures that it was viable. For the commander of

NSA and CYBERCOM too, this scheme could provide the basis for 'proving' the NSA's capabilities in defending critical infrastructure beyond the DIB. General Alexander had suggested to reporters before a Congressional hearing in 2010 that he envisaged the creation of a "secure, protected zone" for certain critical infrastructure, akin to a 'dot-secure' space (McConnell, cited in Jensen, 2010, p. 1534; Reuters, 2010; Shanker, 2010). As we saw in the last chapter, the desire to demarcate 'portions' of cyberspace was a formative part of the military (cyber)security imaginary and was underwriting Alexander's articulation of the problem.

This approach to securing cyberspace was significant for the way it sought to transpose or translate longstanding notions of internal and external security responsibilities into cybersecurity. It would do this by technically bounding or fortifying a portion of 'domestic' cyberspace, to make it analogous to the territorial or geopolitical space that the military had traditionally been responsible for. Furthermore, advocates of the military's capabilities argued during this period for reclassifying and therefore redrawing the bounds around the kinds of critical infrastructure that military agencies could help secure. In remarks before an audience of servicemen and contractors at a Symposium in Colorado Springs, General Alexander suggested that as commander of CYBERCOM and director of NSA he did "…not have the authority to stop an attack against Wall Street or industry, *and that's a gap I need to fix*." (2011, cited in Harris, 2014, p. 162, emphasis added). This meant that in addition to the networks of defence contractors, Alexander was also beginning to advocate for DoD's role in defending civilian dot.com domains, which had been designated as DHS' area of responsibility. However, like Lynn in 2010, he was also apparently conscious of the way that distinctions between domestic and foreign activities would have to be carefully made for such programs to be successful. Alexander at the time suggested that "…doing it, technically, is fairly straight forward. The hard part is now working to and ensuring everybody's satisfied with what we're (proposing) to do." (cited in Reuters, 2010). It was not technology that would obstruct such efforts, but wider normative and legal constraints. He would have to convince 'everybody' that this would not be an infringement of civil liberties or an overextension of the military's powers into matters traditionally thought out of bounds.

The NSA's case for extending their cybersecurity role was not as technically 'straight forward' as Alexander had suggested, however. In November 2011, a Carnegie Mellon report commissioned by the Pentagon had validated the concept behind the programme to match NSA threat signatures against the network traffic of defence contractors, but had not determined how effective the concept was (Harris, 2014). Echoing the problems that the EINSTEIN program had encountered with trying to approach network security in terms of perimeter defences, Rep. James Langevin said that the Carnegie Mellon report was further evidence that "signature-based defenses alone will never be enough to secure our critical infrastructure" (cited in Nakashima, 2012a). More significantly, the NSA had trouble demonstrating the distinctiveness and unique effectiveness of their threat signatures. The Carnegie

Mellon study found that of fifty two incidents of malicious activity detected during the pilot, only two were the result of NSA-generated threat signatures that the companies did not already have prior knowledge of and the report concluded that "the added value of the classified signatures relative to already available signatures was not conclusively demonstrated during the pilot" (cited in Nakashima, 2012a). The day-to-day practicalities of transferring the classified threat signatures to the ISPs were also technically constrained. According to one industry official cited in the Washington Post, the classified data had to be hand-delivered on paper to the operators every few days, and then hand-typed into the detection systems (Nakashima, 2012a). While the NSA had substantially more technical and organisational resources than the DHS at this point, on this occasion it did not help them establish their credibility with the private sector operators.

In addition to the technical issues with the pilot, longstanding distinctions between civil and military roles were the reason that it was not kept with the Pentagon. When DoD representatives presented the findings of the Carnegie Mellon report to the White House, the administration declined to roll out the programme in its original format. According to later reports, it was around this time that the Obama Administration put pressure on the Senate Intelligence Committee to block legislation that would have extended the NSA's role in monitoring the private network communications of these companies (Nakashima, 2012b). Implicit in these objections were concerns about how the program would fit into (or challenge) longstanding normative and legal distinctions circumscribing civilian and military activities. As then retired vice chairman of the Joint Chiefs of Staff Gen. James Cartwright recalled, Alexander and the NSA "were asking for way too much authority and they were contravening the Constitution with what they were asking for — to take unilateral action outside of their area of responsibility" (cited in Nakashima, 2012b). Eric Rosenbach, the deputy assistant secretary of Defense for Cyber Policy in the Department of Defense also invoked historic restrictions on domestic action in this regard:

> Obviously, there are amazing resources at NSA, a lot of magic that goes on there. But it's almost certainly not the right approach for the United States of America to have a foreign intelligence focus on domestic networks, doing something that throughout history has been a domestic function. (Rosenbach, cited in Zetter, 2012)

Thus, while NSA had 'amazing' organisational and technical resources that could have made them more adept than DHS at cybersecurity programs such as this, this program had failed to convince the Administration that it fit within with historically resonant 'Constitutional' distinctions. This would work to DHS' advantage in terms of consolidating the department's distinctive role. As a result, in January 2012 Defense Secretary William Lynn gave DHS an expanded role in the DIB Cyber Pilot: the DHS would

take the place of NSA in acting as the interface with the private sector ISPs (Corrin, 2012). This was the first of the gradual increases in DHS' oversight of the scheme over the proceeding months and years.

The debates that prominent actors were wrestling with through the DIB Pilot were thus symbolic of the tensions that security actors faced in trying to articulate the boundaries between the DoD's traditional remit over foreign threats and the DHS' domestic mission. The DIB Pilot became a symbol in some ways of DHS's struggle to assert its authority over the security of federal and domestic networks. By hailing links between boundaries signifying internal and external, and boundaries signifying cybersecurity, they had in effect translated or reconstituted longstanding distinctions into the context of cybersecurity.

With DHS and not the DoD officially designated as the central intermediary between the private sector and other federal agencies for cyber threat sharing, it had thus apparently been successful in asserting the domestic orientation to cybersecurity. Janet Napolitano, as Secretary of Homeland Security, reflected on such distinctions to articulate why such a program should be "more appropriately located with the DHS", telling Senators in 2012 that…

> …the DIB pilot really gets to the division of responsibility between military and civilian, and what we are talking about here are private companies that do important defense contracting work, but they are in essence private companies. And so the authorities and the laws that we use are better situated in DHS, which deals in this context as opposed to DOD. (Napolitano, in US Senate, 2012b, p. 18)

Managing distinctions between NSA technologies and private sector operators would thus prove to be decisive. By cementing their role as the central hub for threat information sharing the DHS had thus managed to frame the problem of cyberspace in terms of domestic-level responses rather than foreign sources of threats. In February 2013, the administration solidified the DHS' role as the central interface between the NSA's classified threat intelligence and the private sector defence contractors in the scheme through Executive Order 13636 (White House, 2013). This was confirmed by Congress in 2015 who passed legislation in the form of the Cybersecurity Information Sharing Act, which formally tasked the DHS to be the primary interface between foreign threat information and domestic infrastructures and organisations. With DHS successfully cementing their central role as the hub or intermediary for information sharing between federal and private entities, this worked to focus the federal analysis efforts at the domestic level. Even if the threats were coming from overseas, this sidestepped the problems of attribution in a way, by making the information about domestic companies and entities. It refocused the efforts away from foreign sources to a focus on the 'homeland' instead.

4.3.3 Cybersecurity constitutes risk, risk constitutes homeland cybersecurity

DHS had encountered organisational and technical difficulties in rolling out the EINSTEIN program across the federal networks. These difficulties had shaped a change in the DHS' approach to cybersecurity over the subsequent ten years, which is why they added programs such as CDM to the NCPS. They also had to keep up with changes to the morphology of the network and new technologies: by 2015, cloud computing and remote access habits were making it even harder to apply the "protect everything" approach that had sought to centralise and bound federal networks. The DHS' approach gradually shifted to an "assume breach" mentality, moving the technical programs' focus on perimeter defenses to a layered approach that evaluated the inner workings of the network, such as with CDM. Bound up in these shifts, these programs were also a contributory factor to shifts in DHS' approach away from the source of the threats, to a focus on the risks to the targets that they were tasked with securing.

By the time that the Obama administration released their version of the CNCI in 2010, this shift to managing risks and vulnerabilities (a 'resilience' framing, rather than stopping threats in their tracks) was beginning to shape the technical programs that the DHS would develop. Initiative number eleven of the CNCI described the importance of managing the risks "stemming from both the domestic and globalized supply chain" with strategic and comprehensive programs (White House, 2010, p. 5). This would require technical programs that could provide a "greater awareness of the threats, vulnerabilities and consequences" (ibid) of what was happening on the network because of the blurred boundaries between 'domestic and globalised' supply chains.

In other words, transposing distinctions between domestic and foreign technologies, and the vulnerabilities that stemmed from their use, was cited as a specific challenge, one that shaped the programs that emerged. The CDM was developed as one of the DHS' technical solutions to this charge. DHS' advocates recognised that EINSTEIN on its own was not sufficient, and CDM was a necessary extra layer:

> As we accelerate EINSTEIN deployment, we also recognize that security cannot be achieved through only one type of tool. That is why we need defense in-depth. EINSTEIN is not a silver bullet and will never be able to block every threat. For example, it must be complemented with tools that monitor the inside of agency networks. Our CDM program helps address this challenge. (Ozment, in US Senate, 2015c, p. 10)

Understanding vulnerabilities first required a catalogue of the network's features. CDM would do this by cataloguing the system's features, then comparing it to a list of known technologies, behaviours and security flaws so that network administrators could then address the most urgent issues. As Jeh Johnson, the Secretary of Homeland Security, described the CDM to Congress,

> Once fully deployed, CDM will monitor agency networks internally for vulnerabilities that could be exploited by bad actors that have breached the perimeter. CDM will allow agencies to identify, prioritize, and fix the most significant problems first. It will also provide DHS with situational awareness about Government-wide risk for the broader cybersecurity mission (Johnson, in US House of Representatives, 2015e, p. 15)

CDM was thus an important constituent in the shift from 'threats' to 'risks': it was designed to identify and manage risks on a continuous basis, whilst helping DHS to consolidate and centralise its broader cybersecurity mission. Even while admitting to Congress that the NCPS was no technological 'silver bullet', the risk management approach was a key element for shifting the focus from threats to risks and therefore distinguishing their mission expertise from that of the DoD's. CDM was also a technique for mapping network spaces as fields of vulnerabilities, one which grafted a spatial understanding from the structure of territorial administration – that the DHS was representative of – into its approach to cybersecurity, based again on 'perimeters' and territory (Lakoff and Collier, 2008).

While some technical programs such as the NCPS had struggled to reconstitute bounds between internal and external security at a technical and organisational level, boundary work that reproduced these bounds at a policy level were a foundational reference point in DHS' efforts to clarify their approach to cybersecurity. Over the course of the period discussed in this chapter, a key theme that emerged across the DHS' discourses was that of 'risk management' as a strategic response to the problem framing. Here, boundary distinctions were reinscribed and reproduced, rather than reconstituted.

In their efforts to domesticate cybersecurity and distinguish their approach to cybersecurity from that of the DoD, the risk-based approach to cybersecurity gradually emerged as a productive strategy for DHS advocates. This both shaped, and was shaped by, initiatives such as NCPS and the TIC. The DHS were already familiar with 'all-hazards' and risk management approaches. In other contexts, such as disaster management and counter-terrorism, measures the DHS had inherited and translated the techniques and organisational framework dating from the Cold War of 'distributed preparedness': a set of norms, techniques and practices concerned with risk management based on the mapping of national space as a field of vulnerabilities (Collier and Lakoff, 2008; Lakoff and Collier, 2008). This was evident in the National Preparedness Guidance and more recently the National Preparedness Goal issued by DHS for example (Department of Homeland Security, 2007, 2015). However, how cybersecurity would fit within the bounds of this approach had gradually iterated over time. As two key members of the DHS' cyber mission Suzanne Spaulding and Phyllis Schneck told Congress in 2015:

> While securing cyberspace has been identified as a core DHS mission since the 2010 Quadrennial Homeland Security Review, the Department's view of cybersecurity has evolved to include a more holistic emphasis on critical infrastructure which takes into account the convergence of cyber and physical risk (in US House of Representatives, 2015d, p. 12)

As we saw above in the discussion of DHS' spatial and scalar imaginaries, that DHS's 'view of cybersecurity' was something that had evolved indicated how their efforts had been shaped by the various programs that they had been engaged in, including the NCPS. The evolution of this view was also a product of broader political struggles to consolidate their institutional space and domesticate cybersecurity. Their approach to critical infrastructure was a constitutive part of this evolution because it would help shift technical and political focus away from the foreign or external *sources* of threats to their *target*, with important ramifications for the kind of national identity that was being secured.

Rather than solely focusing on agential external actors (that had long been the remit of military and intelligence agencies based on historically resonant notions of the borders between 'domestic' and 'foreign'), DHS advocates were portraying a much wider array of actors and motivations. By pointing to the breadth and complexity of the threat actors, this framing was intended to highlight the difficulties of addressing the *sources* and motives of the threats and would instead suggest a focus on the location of the *targets* (within the homeland). Representatives of the DHS' main cybersecurity department of the National Protection and Programs Directorate (NPPD) described DHS' overall strategy in terms of risk management, detailing the ways that risk assessments judge the unique interrelation of threat, vulnerability and consequence in their estimations of risks (US House of Representatives, 2016b, p. 19). However, they went on to underscore in this hearing and many others that "…DHS recognizes that risk cannot be eliminated and therefore must be managed through proven practices including timely information sharing." (Ozment and Durkovich, in US House of Representatives, 2016b). Such an approach was arguing for agencies and targets to therefore "identify and resolve cybersecurity vulnerabilities in a prioritized and risk-based manner" (Wilhusen, GAO, in US House of Representatives, 2017b, p. 18). Another way that actors justified this framing was with reference to limited workforce and financial means:

> Each incarnation of the cyber threat has unique traits, and mitigation requires agility and layered security. Cybersecurity is a process of risk management in a time of constrained resources, and we must ensure that our efforts achieve maximized security as efficiently as possible..." (Ozment, in US House of Representatives, 2015c, p. 14)

A risk management approach thus shifts the focus from dealing with the unique and varied traits of threats, to instead conduct risk assessments which aim to only deal with those threats that pose the

most likelihood of doing greatest harm, on a case-by-case basis. Instead of the traits and agency of the threats, in working to enact the DHS' scalar imaginary it was the traits of the target that should be the focus of DHS efforts, with the added intention of empowering individual information system administrators and managers tasked with 'local' network security.

As in the earlier debates surrounding the EINSTEIN 3 program, placing the emphasis on risk mitigation meant that DHS was developing the thread of the discourse that sidestepped the problems of attribution, instead locating the *domestic* targets at the centre of the problem framing. The 'foreignness' of the cyber threats thus assumed different importance, depending on the organisational affiliation of security actors: for DHS advocates, this was the least emphasised aspect of their threat framings. By 2018, this made their approach to cybersecurity distinctive: as one Congressional Research Service report neatly summarised:

> Much of the U.S. government's cybersecurity apparatus focuses on the adversary—the person or organization that seeks to or has already carried out an attack against information technology (IT) systems. The U.S. Department of Homeland Security (*DHS) is unique in the government's structure because its work to ensure national cybersecurity is largely agnostic to any individual threat actor, but informed by the risks that the actor presents*. (Jaikaran, 2018, p. 1, emphasis added)

The risk-based approach to cybersecurity was thus a key part to the DHS constituting the 'homeland' to be secured in cybersecurity, thereby both drawing upon and transcribing longstanding normative and legal distinctions into this context.

A focus on risk management and vulnerability mapping was also a constitutive element of a broader shift in how boundaries distinguishing 'the homeland' were made to matter in cybersecurity. This can be seen in the way that testimony from DHS representatives centred around the 'interconnected' qualities of cyberspace and the associated physical infrastructures, rather than their putatively borderless or virtual qualities. DHS actors would instead point to the ways that cyber and physical target systems were so interconnected as to be indistinguishable. In advocating to Congress for a re-alignment and consolidation of DHS' cybersecurity operations into a new 'Cybersecurity and Infrastructure Security Agency' (CISA), two Undersecretaries from DHS' NPPD jointly expressed this framing most explicitly:

> The risks that our stakeholders face are cyber and physical, natural and man-made. Some risks blur the distinction between cyber and physical… while others combine aspects of cyber and physical risk: Cyber-attacks causing physical impacts, natural disasters impacting communication networks, or man-made attacks on lifeline critical infrastructure. The

> proposed realignment, which was included in NPPD's draft reorganization proposal, will further the ability of our cybersecurity experts and physical security experts to work side-by-side, ensuring that risks to critical infrastructure are fully assessed and effectively mitigated and directly supporting our ability to address an emerging risk environment in which *cyber and physical boundaries are increasingly meaningless*. (Ozment and Durkovich, in US House of Representatives, 2016b, p. 19, emphasis added)

The "inextricable link between the physical and cyber domains, and the diversity of cyber actors" (Ozment, in US House of Representatives, 2015c, p. 13) were thus two of the foremost framings that featured in the DHS' efforts to draw attention to the ways that boundaries translated into cyberspace. By defining the target infrastructure in such a way, these NPPD representatives were advocating for a specific orientation to the problem. Specifically, these framings were symptomatic of DHS' efforts to demarcate how the threats would fit into established notions of their domestic responsibilities. The physical infrastructures of critical domestic sectors are the embodiment of the 'homeland' to be secured. Unlike the earlier discourses that emphasised the 'borderless' qualities of the threats, now it was the targets that were so deeply physically interconnected as to require the DHS' expertise for their protection.

In November of 2018, the Cybersecurity and Infrastructure Security Agency (CISA) Act was finally signed into law in the United States. While the legislation had not had an easy passage into law, it did further consolidate DHS as the lead agency responsible for domestic cybersecurity matters. In itself it was not a controversial proposal: the CISA Act was designed to streamline and rebrand the clumsily named 'National Protection and Programs Directorate' (NPPD), the hub given responsibility for both the cyber and physical security of the nation's sixteen critical infrastructure sectors. The now newly named Cybersecurity and Infrastructure Security Agency would continue to be the lead agency designated with the responsibility for sharing threat information with the private sector as well as taking the lead in national incident response management. This legislation was part of an overall expansion of DHS's cybersecurity authorities, reinforcing the department's profile as one of the government's key cybersecurity agencies. By 2018, DHS had managed to distinguish their mission from that of the DoD successfully enough that Pentagon officials would tell Congress how the latest strategy document and a newly signed 'Memorandum of Agreement' reflected and solidified distinctions between domestic and foreign activities. As the DoD's Assistant Secretary of Defense for Homeland Defense and Global Security, Kenneth Rapuano, explained it:

> DoD's focus on cyberspace, like in other domains, is to prevent or mitigate threats before they reach American soil. This focus complements the DHS cybersecurity strategy's emphasis on

> domestic preparedness and risk management. Together, the DoD and DHS strategies form a natural mutually supporting approach to defense in depth (Rapuano, cited in Serbu, 2018 n.p.)

As far as Pentagon and DHS security actors were concerned, how these distinctions applied to cyberspace and cybersecurity had thus largely been settled. In the end, distinctions between internal and external, and domestic and foreign, had provided productive resources as well as political constraints on how cybersecurity would be addressed. Despite the early narratives of 'borderless cyberspace', competitive boundary work embedded in federal cybersecurity initiatives had utilised but also reproduced distinctions between internal and external. Embedding such spatial and scalar imaginaries in technical as well as policy initiatives suggests that some boundaries may possess a historical resonance that are hard to completely reconstitute, despite the essentialised narratives of cyberspace's characteristics.

4.4 Conclusion

Between 2002 and 2014, the DHS' authority on matters of cybersecurity had consistently been contested in several respects, including whether they were functionally capable and possessed the right resources and expertise, or whether the 'nature' of the threats and the 'nature' of cyberspace made the DoD the more appropriate agency. In many ways, EINSTEIN and the NCPS programs can be understood as a symbol for DHS' struggle to assert its authority over the security of federal networks. Despite the technical and organisational shortcomings, this chapter has argued that these programs were productive in its efforts to domesticate cybersecurity according to longstanding and historically resonant distinctions.

The competitive boundary work analysed in this chapter was concerned with who 'cybersecurity' belongs to, and which state agencies should have what roles and responsibilities. Here, boundary work sought to embed competing visions and goals into technical and organisational infrastructures and has also helped define priorities and allocate resources for carrying out different tasks related to cybersecurity. In this sense, while military actors had tried to produce a vision of the homeland by enacting and managing the 'external' boundaries of that homeland, and so constitute a cybersecurity oriented around external threats by undertaking collaborative boundary work *at* boundaries, in the end the DHS' competitive boundary work was more successful in embedding and enacting links between the 'homeland' and 'cybersecurity.' Despite the DoD possessing more material and organisational heft, the DHS's boundary work strategies were able to mobilise and concretise a more resilient (and for policymakers, more culturally and politically palatable) set of distinctions. The discussion of the emergent relationships between the DHS' technical programs and its risk-based approaches in Part Three found that this boundary work took an iterative and co-constitutive path.

Programs and organisations were designed to enact boundaries; those programs subsequently informed organisational and conceptual boundaries and imaginaries. Here, the NCPS was shaped by boundaries to begin with, designed as a program that was trying to 'bound' and consolidate networks. Then, the difficulties of enacting those boundaries shaped (and was shaped by) risk-based approaches and spatialising imaginaries. DHS actors were thus able to 'domesticate' cybersecurity by shifting the focus onto managing the nation's internal vulnerabilities through a risk-based framing.

While this chapter has drawn out how the DHS were articulating a security imaginary in distinction to the military's cyberspace narrative, the DHS's own imaginary was also in turn being contested by those outside the government. At the same time that DHS was defending its credibility and authority in matters of cybersecurity amongst its Federal peers, we will see in the next chapter how DHS was simultaneously articulating a cybersecurity imaginary through configurational boundary work that sought to enrol and orchestrate the support of those outside of the Federal government, to varying degrees of success.

Chapter Five: Orchestrating and (re)configuring 'public' and 'private' roles in 'cybersecurity'

5.0 Introduction

In this chapter I will show the ways that making distinctions between 'public' and 'private' has set expectations about what the US government should, can – and cannot – do in cybersecurity. In other chapters, the project looks at federal initiatives that have followed from official strategies and visions of insecurity. In contrast, this chapter will show how government and private actors are using distinctions and categories of 'public' and 'private' to actualise but also modify those federal visions of 'cybersecurity'. In the boundary work analysed in this chapter we will see how at least two different visions of cybersecurity – and who it is *for* – emerge from the ways that different actors invoke and mobilise those categorical distinctions.

This chapter argues that 'cybersecurity' has emerged through boundary work that has sought to realign and redraw how those distinctions between categories of 'public' and 'private' have been mobilised to constitute boundaries of a thing called 'cybersecurity.' To substantiate this argument, each of the three parts to this chapter analyses boundary work that invokes categories of public and private, though to varying ends. The first part of the chapter will show how government actors have mobilised distinctions of public and private to make the case for 'extending' cybersecurity through 'public-private partnerships,' to devolve political authority for security away from the state. An analysis of federal strategy and vision documents finds *configurational* boundary work to orchestrate and produce collective action in the name of 'cybersecurity.' Part One sets out the parameters of what follows in Parts Two and Three, drawing out what those distinctions have been mobilised to mean in the context of US cybersecurity politics.

Two case studies will then show how those federal imaginaries are alternately supported, amended, or contested by those that the government are working to variously enrol, enlist, or compel in the vision of cybersecurity. In Part Two, controversies involving two companies, Mandiant and Apple, will serve as case studies to show differences in how willing they each were to mirror and actualise those official narratives. State-sponsored theft of intellectual property on the one hand, and encryption technologies on the other, would each trigger episodes of boundary work that made categorical distinctions between 'public' and 'private' explicit in articulating competing imaginaries of insecurity. For the most part, through *collaborative* boundary work, Mandiant would reproduce and echo government boundary work strategies *at* public and private boundaries, to the company's benefit. Meanwhile, Apple would undertake *competitive* boundary work *for* boundaries that resisted

those Federal framings of public and private distinctions, to offer an alternative imaginary they rooted in a civil society vision of 'security,' in which the government was the source of insecurity. This section will show how these are more than just rhetorical efforts to build support for preferred courses of action. As Part Three will bear out, these efforts also form a constitutive part of the initiatives and policies that follow. To show how the boundary work around these controversies was concerned with deciding both who would *produce* and who would *benefit* from 'cybersecurity,' Part Three will critically analyse the processes by which futures of cybersecurity were imagined and differently performed and contested by Mandiant, Apple and federal actors.

While other chapters examine how federal actors undertake boundary work in defence of their authority, legitimacy or autonomy, this chapter examines a form of 'socio-political boundary work' concerned with delegation and displacement of political authority: the division of labour and tasks, and the re-distribution of 'lines of accountability' for roles and responsibilities in 'cybersecurity.' Thus, by variously invoking and mobilising cybersecurity's 'public' or 'private' traits at different times, over time industry visions and corporate interests have shaped a vision of 'cybersecurity' which prioritises the protection of intellectual capital and corporate values. First though, the chapter will critically analyse how the federal government's imaginary of insecurity was articulated so that 'public-private partnerships' became the 'natural' political and practical solution.

5.1 Part One: (Circumscribing) 'The Government Role in Securing Cyberspace'

In setting out their vision for a *National Strategy to Secure Cyberspace* in 2003, DHS and the Bush administration were articulating more than just a policy statement, they were detailing the features of a secure future they hoped to see built, but not by themselves alone. In this federal strategy document and others, boundaries of 'public' and 'private' were drawn upon and problematised as a way for government actors to articulate their vision of insecurity in cyberspace. Such strategy documents exemplified a wider set of conceptions about the allocation of political authority thought to stem from distinctions between categories of 'public' and 'private.' In the American political imaginary, referencing distinctions of 'public' and 'private' draw upon and reference "normative infrastructures" of constitutional principles (Jasanoff and Kim, 2015, p. 22) where there were expectations placed upon government actors by 'the American people.' As the 2009 *Cyberspace Policy Review* made explicit, the Federal government could not "entirely delegate or abrogate its role in securing the Nation from a cyber incident or accident" as they had "the responsibility to protect and defend the country, and all levels of government have the responsibility to ensure the safety and well-being of citizens." (White House, 2009, p. vi). Making those distinctions

was therefore an important set of cultural and political reference points for government actors building a case that they were not to be the only producers of such security.

According to this vision of insecurity, distinctions between public and private were invoked to show how the government was incapable of securing cyberspace on their own. While the federal imaginary was making explicit their rationale for the state's involvement by defining the security of cyberspace and 'critical infrastructures' as a matter of national security (as Chapter Four showed), by simultaneously describing the security of cyberspace as a "unique problem" requiring "a unique process," they were also beginning to articulate the limits of the government's involvement and responsibilities (President's Commission on Critical Infrastructure Protection, 1998, p. vii; White House, 2003, p. 2). This was because most "critical infrastructures, and the cyberspace on which they rely" were "privately owned and operated," and America's "traditions of federalism and limited government require that organizations outside the federal government take the lead in many of these efforts" to secure cyberspace (White House, 2003, p. xiii).

By invoking those 'traditions' of limited government, federal actors were thus making the case that that "government alone cannot sufficiently secure cyberspace" on both political grounds and practical grounds. According to this logic, culturally significant traditions curtailed the political legitimacy of certain federal (public) actions, while practically, the government lacked the insight into privately owned and operated networks deemed necessary to address technical problems. The purpose of the 2003 strategy document was therefore described as 'engaging and empowering' "…Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact" (White House, 2003, p. 1). In other words, this vision of insecurity intended to delegate political authority, to empower (private) companies and citizens to take some degree of responsibility for their own security in cyberspace.

In the federal vision, the structure of cyberspace determined that insecurity resided in the 'private sector.' Even while narrating the ways that cyberspace provided the basis for the nation's prosperity and national interests, cybersecurity risks were described as "some of the most serious economic and national security challenges of the 21st Century" because the "digital infrastructure's architecture was driven more by considerations of interoperability and efficiency than of security" (White House, 2009, p. iii). Most frequently articulated in optic terms, concerns about a lack of federal insight *into* these networks has thus been a recurring theme in cybersecurity politics. As a case in point, the 2003 strategy described the challenges of cyberspace that came from there being "…no synoptic or holistic view of cyberspace […] there is no panoramic vantage point from which we can see attacks coming or spreading" (White House, 2003, p. 19)**.** Again invoking notions of the state's 'traditional' role as security provider, this vision of insecurity likened the threats from 'cyber attacks'

to the threats posed by missiles and rockets in the 1950s and 1960s to describe their use of radar. This was an expression of an anxiety, namely that because the "…vulnerabilities that most threaten cyberspace occur *in the information assets of critical infrastructure enterprises themselves*" (White House, 2003, p. xi, emphasis added). Federal actors would therefore advocate a role for the private sector to share information that could help them 'visualise' what was happening *inside* cyberspace. More than just a metaphoric habit, this anxiety about visualising data and vulnerabilities would shape governmental policy interventions and boundary work for both case studies later in the chapter.

While "public-private engagement" was to be "a key component" of their strategy to "secure cyberspace," there were some things that the federal government and its agencies *did* claim responsibility for by invoking such distinctions (White House, 2003, p. ix). The political authority and legitimacy that stemmed from such distinctions in US politics were implicit in statements that referred to instances where federal government responses were "most appropriate and justified." (White House, 2003, p. ix). As well as directing funding and research priorities, federal duties included "…forensics and attack attribution, […] and protection against organized attacks capable of inflicting debilitating damage to the economy" (White House, 2003, p. ix). Furthermore, the 2003 strategy was particularly concerned with setting the parameters for what would trigger federal action, stating that they would intervene for "…threats that cause significant damage to our economy or security," and that "…law enforcement and the national security community play a critical role in preventing attacks in cyberspace." (White House, 2003, p. 28). The federal government were thus described as possessing distinctive resources they were uniquely equipped with to fulfil their normative duties: their "…full authority, capabilities, and resources must be available to support critical infrastructure protection efforts. These include, as appropriate, crisis management, law enforcement, regulation, foreign intelligence, and defense preparedness." (White House, 2003, p. 17). However, in the years that followed, such 'unique' capabilities would become the locus of counter-narratives and controversy for those outside the government challenging official narratives. As we shall see later in the chapter, defining what would count as a 'large incident,' whose security would be deemed the most important, and who should assume responsibility for attributing such incidents would later trigger dissenting boundary work.

According to the federal imaginary, public-private partnerships stimulated cybersecurity by supplementing the federal government's 'distinctive' capabilities. As part of their efforts to describe (or circumscribe) '[t]he Government Role in Securing Cyberspace,' federal actors thus used distinctions between public and private to articulate how for the most part, the private sector was "best equipped and structured to respond to an evolving cyber threat" (White House, 2003, p. ix) because of normative concerns about federal over-reach as much as putative characteristics of such networked communication technologies and its operators. This was another facet underpinning the widespread

official articulations of cybersecurity as a matter of 'public-private partnerships' in the US: these distinctions were typically invoked to signal how government actors were politically constrained from encroaching upon 'private' self-determination and free-market logics (Carr, 2016). As we shall see throughout this chapter, shifts in how these distinctions are mobilised or referenced thus carry a lot of cultural significance in the US, given the ways that they are rhetorically and symbolically bound up with notions of American identity, Constitutional histories, and conceptions of national vulnerability.

So far, the chapter has shown how as an analytical concept, the 'federal cybersecurity imaginary' allocated a primary role to the private sector in producing 'cybersecurity,' to lend this imaginary an appeal across as many communities as possible. To enlist the support of the target constituents of these 'public-private partnerships,' the federal cybersecurity imaginary therefore claimed to reconcile economic and political concerns. Describing this in terms of the "dual challenge of maintaining an environment that promotes efficiency, innovation, economic prosperity, and free trade while also promoting safety, security, civil liberties, and privacy rights" (White House, 2009, p. iii), the federal imaginary attributed the environment of cyberspace, and by extension 'the private sector' with innate capabilities for innovation, efficiency and flexibility. In US political imaginaries, cyberspace was widely conceived of as the engine of a prosperous economy, and federal regulation viewed as a burden on such economic processes, so that public-private partnerships were offered as the solution for managing those apparently conflicting 'public' and 'private' attributes. This conception of cybersecurity assumed that it was manageable through some (federally encouraged) technological innovation and innate characteristics thought to inhere in the 'private sector,' without fundamentally compromising national values (civil liberties, free trade, privacy) or economic growth. However, actors in the private sector would later invoke those same attributes in different ways to contest this distribution of responsibilities for producing cybersecurity, using them to bound 'cybersecurity' in different ways. Government efforts to align corporate interests and commercial logics with those of the 'national interest' shows how these are not mutually exclusive rationalities in the US – the two are often mutually informed in official discourses.

As *configurational* boundary work, official imaginaries of insecurity have therefore sought to facilitate government efforts to act as 'orchestrators' rather than simply 'providers' of security in cyberspace (Abbott *et al.*, 2016). In the rest of the chapter, we will see how this federal orchestration takes the form of instrumental boundary work and a degree of moral suasion, whereby federal actors set out their intention to "…lead by example, giving cybersecurity appropriate attention and care, and encouraging others to do so." (White House, 2003, p. 43). Articulating these distinctions would form the basis for enacting (as well as resisting) the practical and political initiatives that federal actors were proposing. However, cybersecurity would be described as a public good in ways that would mean its benefits would not be equally distributed (McCarthy, 2018). At least two different visions of

'cybersecurity' – and who it is for – would thus emerge from the different ways that actors emphasised the 'public' or 'private' characteristics of 'cybersecurity.' As we shall see in the rest of the chapter, producing cybersecurity for the networked nation has not been the product of formal contracts and legal agreements that officially delegates political authority or responsibilities (Eichensehr, 2017). Instead, the chapter argues that cybersecurity has emerged through boundary work that has sought to realign and redraw how those distinctions between categories of 'public' and 'private' could and would be mobilised to constitute boundaries of this thing called 'cybersecurity.' In other words, what cybersecurity *is* depends on how its boundaries are drawn and by whom.

5.2 Part Two: Contesting categories/proposing solutions

By articulating cybersecurity as a problem that 'blurs' "traditional notions of public and private spheres" (Rockefeller, in US Senate, 2013c, p. 2), co-ordinating and orchestrating the roles and responsibilities thought to stem from such distinctions would therefore be the focus of much of the ensuing cybersecurity politics. As we shall see in the case of two demonstrative controversies in this section, while state actors had started to build a political case for cybersecurity as a 'shared responsibility,' actualising those configurational boundary work strategies and bounding the procedural and symbolic parameters of such 'public private partnerships' was to be a fraught endeavour.

5.2.1 State-sponsored corporate espionage triggers collaborative boundary work

The federal cybersecurity imaginary had sought to build the case for distributing 'traditional' security responsibilities amongst 'public-private partnerships' for cybersecurity, but during the controversy that emerged in response to state-sponsored corporate espionage by China between 2010 and 2014, the way they had mobilised distinctions between public and private would be called into question.

Over the course of hearings during the Obama Administration, Congress would hear testimony from representatives of companies, government agencies and policy advisers to the effect that nation-state hackers were conducting espionage and theft through cyberspace on an unprecedented scale. In a report entitled *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace*, the Office of the National Counterintelligence Executive (ONCE) made a report to Congress in 2011 that described "foreign economic collection and industrial espionage" as "significant and growing threats to the nation's prosperity and security." Furthermore, cyberspace was 'amplifying' these threats because malicious actors could "…quickly steal and transfer massive quantities of data while remaining

anonymous and hard to detect." (Office of the National Counterintelligence Executive, 2011, p. i). Then, by 2012, a report published by the U.S. China Economic and Security Review Commission went as far as to suggest that "Chinese state-sponsored actors continued to exploit U.S. government, military, industrial, and nongovernmental computer systems" (USCC, 2012, pp. 7, 9).

While the 2003 strategy document had made clear that attribution was one of the duties the federal agencies were responsible for, the traits of cyberspace that enabled actors to move quickly and anonymously would here be cited as technical constraints on federal attribution efforts. Furthermore, federal actors also expressed political and diplomatic reservations about making public attributions about the state-sponsorship of the groups extracting intellectual property via cyber espionage. The ONCE's report to Congress stated that "US private sector firms and cybersecurity specialists have reported an onslaught of computer network intrusions that have originated in China," and that the intelligence community "cannot confirm who was responsible" even while arguing that Chinese actors were "the world's most active and persistent perpetrators of economic espionage." (Office of the National Counterintelligence Executive, 2011, p. i). Yet despite this report, and despite their raising "…concerns at the highest levels about cybertheft with senior Chinese officials" (Vietor, cited in Sanger, Barboza and Perlroth, 2013 n.p), White House officials had said that a combination of diplomatic concerns and a desire to track the unit's activities had kept the government from publicly accusing the Chinese state (Sanger, Barboza and Perlroth, 2013). The ONCE and USCC reports did not rise to the level of official accusations. Public attributions by the government carried with it the expectation of diplomatic and foreign policy actions to enforce their findings (Pozen, 2013), something that the government were reluctant to pursue until 2013. For those (or their representatives) on the receiving end of industrial-scale espionage campaigns, this would prompt them to contest the government's categorisation of duties and responsibilities predicated on public and private distinctions.

Despite federal efforts at configurational work *through* boundaries detailed in Part One, corporate efforts to challenge the government's response therefore focused on drawing distinctions between 'public' and 'private' in dissenting ways to those mobilised in official government narratives. They argued that the federal responses to date were inadequate. As a case in point, a former FBI agent and Chief Risk Officer of security firm CrowdStrike offered testimony in congress that was illustrative of other evidence given by representatives of 'corporate America.' He criticised the government's approach by describing the shortcomings of the government's cybersecurity strategy, which risked:

> …morphing into a game of hot potato where, instead of the government fulfilling its traditional role of stopping the threat actor, our agencies now quickly pass information along to the targeted victims and wipe their hands of it. Remarkably, the government appears to

> expect that corporate America will stop well-resourced, determined, sophisticated actors using a defensive paradigm that is exorbitantly expensive, has proven ineffective over time, and has no precedent of success against persistent threats. (Chabinsky, in US Senate, 2014a, p. 7)

Invoking the 'traditional role' of government in this way was intended to challenge the government into taking more proactive measures than their 'defensive paradigm' had thus far produced. Chabinsky was working to re-establish the government's normative responsibilities by advocating how these 'sophisticated' and 'persistent' threats were beyond the capabilities of corporate America to deal with. This was about setting thresholds for what constituted a 'significant incident' discussed earlier: if Chabinsky and others could make the case that these thefts constituted an attack of sufficient magnitude, then the government – by its own admission – had a responsibility to act. Chabinsky went on to tell congress that:

> To date, the inescapable truth is that the risks associated with attacking and exploiting U.S. networks have been negligible, and the private sector has been left largely on its own – under the threat of government regulation and class action lawsuits no less – to defend itself against all enemies. (Chabinsky, 2014, p. 8)

Corporate espionage thus triggered boundary work that invoked categorical distinctions between public and private as a proxy for efforts to organise social order and political authority. Chabinsky was evocatively describing the private sector as being 'left on its own' to defend itself both from enemies as much as from government regulation and lawsuits, instrumentally casting the private sector in a different light to the federal narratives of efficient and innovative agency. While the President's 2011 *International Strategy for Cyberspace* had declared that the United States would "…ensure that the risks associated with attacking or exploiting our networks vastly outweigh the potential benefits" (White House, 2011, p. 13), Federal government agencies were thus having trouble putting that ambition into practice, or of convincing those in the private sector that they were capable of actualising their strategy and vision for cybersecurity.

At the same time however, the corporate imaginary of insecurity shared a lot of characteristics with the prevailing federal narratives about cyber(in)security, with important shaping effects upon what would be deemed most important to protect. This was an imaginary in which the things that America valued most were envisaged to be at stake: intellectual property, ingenuity and prosperity – characteristics that were intrinsic to what were thought to make America distinctive. In 2013, the White House released their *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* (Executive Office of the President of the United States, 2013). The theft of intellectual property was

here described as a threat to the values and characteristics of the nation, which would necessitate a robust response:

> We are going to aggressively protect our intellectual property. Our single greatest asset is the innovation and the ingenuity and creativity of the American people. It is essential to our prosperity and it will only become more so in this century. (Obama, cited in Executive Office of the President of the United States, 2013, p. 1)

In one of the most oft-cited quotations from these Congressional debates, General Keith Alexander of the NSA had described the threats posed by cyber espionage and crime were responsible for "the greatest unwilling transfer of wealth in history" (US Senate, 2012a; US House of Representatives, 2013c, p. 66). While actors such as Alexander would have different motivations for articulating the kinds of threats the US were thought to face in cyberspace (as we saw in Chapters Three and Four), in the wake of the financial crisis of 2008-9 and ensuing sequestration, this was an attention-grabbing articulation of a problem. In the opening statement explaining the rationale for a Congressional hearing entitled 'The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting Our National and Economic Security,' one Senator remarked:

> No one can deny the serious threat that we're confronting in cyberspace. Almost daily, we learn of new cyber threats and attacks targeting our government agencies and companies that drive our economy. In these perilous economic times, it's especially troubling that the intellectual capital that fuels our prosperity is being siphoned off by cyber criminals and even nation-states. (Thune, in US Senate, 2013c, p. 8)

At the strategic level, business interests and national interests would thus be conflated. That this hearing was concerned with establishing 'partnerships' for addressing cybersecurity threats was indicative of the extent to which these categories and roles were bound up with ideas of what was deemed most valuable and in need of protecting. As three former members of the National Security Council wrote in a newspaper op-ed, strategically "…the interests of U.S. businesses are essential to protecting U.S. national security interests. After all, political power and military power are derived from economic strength." (McConnell, Chertoff and Lynn, 2015 n.p) This meant that "…protecting business interests from massive economic espionage is essential" and nowhere had this imperative become clearer than in cyberspace (McConnell, Chertoff and Lynn, 2015 n.p). Such a framing of the cyber insecurities at hand was likely informed by their each having played active parts in working for, or establishing various defence contractors,[9] thus describing cybersecurity in terms that suggested the

[9] "Mike McConnell is a former director of the National Security Agency and director of national intelligence. Michael Chertoff is a former homeland security secretary and is executive chairman of the Chertoff Group, a security and risk management advisory firm with clients in the technology sector. William Lynn is a former

need for further investment and commercial involvement, but these framings also illustrated the kinds of culturally familiar reference points that would be invoked to make their political case. National values and shared conceptions of desirable futures were thus bound up in the debates about how 'public' and 'private' roles and responsibilities would be distributed in the matter of cybersecurity.

At both the practical and the ideational levels then, the large-scale theft of intellectual property had triggered competitive and collaborative boundary work that would contest the government's framing of distributed cybersecurity responsibilities, depending on which strategies would serve instrumental purposes at the time. However, as we shall see now, another set of incidents would make other actors contest these boundaries differently again. Here, insecurity was conceptualised as lying not with external threats, but in the actions of federal agencies.

5.2.3 Encryption, counter narratives and the 'limits' of federal reach

Whilst state-sponsored theft of intellectual property had triggered largely collaborative boundary work that sought to bound cybersecurity in terms of securing corporate actors and their intellectual property, another controversy would prompt government and private sector spokespersons to articulate distinctions between 'public' and 'private' in different, more competitive ways. Following a mass shooting in San Bernardino in December 2015, the FBI filed a request that a federal magistrate in California order the technology company Apple to help the FBI unlock an iPhone that had belonged to one of the perpetrators. The iPhone at the heart of this controversy would be articulated as the intersection of various tensions about access to data, about the relationships between law-enforcement and technologists, and contestation over the uses of encryption technologies. This was a resurrection of a debate over encryption technologies that state actors had lost in the 1990's, in what was referred to as the 'Crypto Wars' (Saco, 1999; Finklea, 2016; Schulze, 2017). Having failed to instigate encryption backdoors the first time around, this was an opportune moment for the DoJ and specifically the FBI to reawaken the debate of the so-called Crypto Wars, an opportunity that an email from an FBI official had suggested they had been waiting for since 2002 when they wrote at the time that the "current terrorism prevention context may present the best opportunity to bring up the encryption issue" again (anonymous, 2002, cited in Apuzzo, 2016 n.p.). After all, the San Bernadino case was described as a terrorist incident. The federal boundary work analysed in what follows was strategic practical action oriented towards once again trying to force technology companies like Apple to build 'backdoors' into their encryption technologies.

deputy defense secretary and is chief executive of Finmeccanica North America and DRS Technologies." (McConnell, Chertoff and Lynn, 2015 n.p)

In this context, encryption technologies became the locus for state actors to once again work *for* boundaries demarcate a putative separation between "fundamental" 'public' and 'private' roles as well as between "fundamental" rights to privacy and rights to security (US House of Representatives, 2016a e.g. p. 83). Here, the director of the FBI described his view of the problem at hand in Congressional testimony that suggested this was "the hardest issue I've confronted in government", namely, "…how to balance the privacy we so treasure, that comes to us through the technology that we love, and also achieve public safety, which we also all very much treasure" (Comey, in US House of Representatives, 2016a, p. 6). In other words, linking boundaries between 'public' and 'private' would be an instrumental part of legitimating federal visions of 'cybersecurity.' As one Congressman described it…

> …this is really about *fundamental issues of importance as it relates to who we are as a country*, the Fourth Amendment of the United States Constitution, the reasonableness of government intrusion, the rule of law, the legitimate centuries-old concern as it relates to government overreach and the damage that that can do. (Jeffries, in US House of Representatives, 2016a, p. 83, emphasis added)

This was to be a debate about more than encryption: encryption was standing in for debates about the existential values of the nation and normative limits on government action. Meanwhile, to differentiate themselves and their position, Apple's representative hailed a vision rooted in civil society conception of 'security' when they described how "the civil liberties that are at the foundation of our country" were at stake (US House of Representatives, 2016a, p. 98).

Like the debates about Chinese hacking, this was a controversy that sought to draw boundaries between 'public' and 'private' in particular ways in order to settle what 'cybersecurity' was and who it was for. However, in this instance, rather than an imaginary of 'cybersecurity' that construed it in terms that invoked intellectual capital and corporate value as in the last section, this imaginary would invoke individual rights and public safety. In this controversy, Apple would claim to act as spokespersons for their customers and defenders of individual civil liberties. Here, they would articulate boundaries between 'public' and 'private,' or 'security' and 'privacy' in competitive terms that implied that they (and their encryption technologies) were all that stood between an improper extension of government powers. Apple portrayed encryption technologies as a way to constrain government over-reach.

Unlike the controversy surrounding state-level hacking, in which lawmakers and the private sector were advocating for the protection of 'the private sector,' the debates surrounding encryption were explicitly described in terms of an antagonistic distinction between the government on the one hand and technology companies on the other. Apple were portrayed as providing a technology that

was the conduit for a move to "…a world we've never lived in before in the United States", one where law enforcement could not guarantee public safety because of "warrant-proof spaces" (Comey, in US House of Representatives, 2016a, pp. 6; 62). The FBI described two parts to the "[p]roblems highlighted by the Going Dark initiative", the first of which was law enforcement's "difficulty in receiving information from some technology companies" (FBI, 2011, p. 1). The second was articulated by District Attorney Cyrus Vance when he described the distinction not as "a matter of good or bad corporate citizenship" but "a matter of national public safety" (Vance, 2014 n.p.). Technology companies were thus being said to threaten public safety with default smartphone encryption, described by government representatives as standing at odds with the interests of the government and US citizens. Encryption was thus described in terms of an obstruction to law enforcement conducting their roles, with Apple being accused of facilitating its use in a way that exceeded their remit as a private firm (US Senate, 2016a, p. 17). Not only were Apple said to be overstepping the bounds of their role as a private company by making those spaces, they were also described as illegitimately placed to articulate their concerns with public safety. These distinctions would thus be mobilised by government actors to undermine Apple's claims to authority and legitimacy. Distinctions between public and private were described by Congressional leaders in terms of a "perpetual struggle" between 'security and privacy,' (Coburn, 2015, p. 2), but as we shall see now in Part Three, competing articulations of 'security' itself would also form the basis for claims to legitimacy and authority in the programs and debates that follow.

5.3 Part Three: Actualising imaginaries of insecurity, putting them to work

In the first section of Part Three that examines the case of Chinese attribution, we will see that collaborative boundary work by government and ex-government actors to downplay categorical distinctions has worked to make political space for 'private sector' actors to perform 'public attribution.' In a sense, such boundary work has enabled these actors to 'co-produce' roles and responsibilities for cybersecurity. However, the second section will analyse how a mix of configurational and collaborative boundary work strategies by government actors as efforts to orchestrate security at the interface of distinctions between 'public' and 'private' in the case of encryption demonstrate that government actors are not always able to stabilise or institutionalise their boundary work in the face of external competitive boundary work strategies, showing that the resources held by state and congressional actors does not automatically ensure success or resilience for their boundary work in this context. Each boundary work analysed in each section had important implications for shaping conceptions of who would produce and who would benefit from 'cybersecurity' whilst also being animated by a struggle of 'security vs security.'

5.3.1 (Re)configuring boundaries and roles with attribution reports

Economic espionage by nation states was to be a key point of contention in US cybersecurity politics because of the ways that it was raised to challenge the legitimacy of the state's official vision for cybersecurity. The publication of a controversial report by a US-based security company called Mandiant in February 2013 would trigger collaborative boundary work by representatives of the company and Congress, to instrumental ends. The report was controversial because this was the first time that a non-government agency would make a formal and detailed attribution of state-based hacking. The report by the computer security company presented detailed technical evidence of a singular group undertaking cyber espionage, a group who had targeted and stolen data from at least one hundred and forty-one organisations around the world (Mandiant, 2013). According to their report, the data which Mandiant had been collecting since 2004 was sufficient to convince them "…that the groups conducting these activities are based primarily in China and that the Chinese government is aware of them" (Mandiant, 2013, p. 2). The group they positively identified in their report — entitled 'APT1: Exposing One of China's Cyber Espionage Units' — was the People's Liberation Army 'Unit 61398.' In this instance, this was a level of detail about a specific division of the Chinese army that the United States government had not felt prepared to acknowledge publicly.

Drawing upon distinctions between 'public' and 'private' would be a strategy that Mandiant used as part of their efforts to legitimise their own standing as well as challenge the credibility of the government's response to the theft of intellectual property. As an example of a collaborative boundary work strategy, the report was framed by the company as claiming to speak on behalf of the private sector, whilst also referencing these distinctions to make a practical space for their services. When Mandiant's executives Kevin Mandia and Richard Bejtlich were invited to give testimony in front of the Senate Committee on Armed Services shortly after the publication of their report, they emphasised that they wanted to draw attention to the scale of the theft but also to channel the industry's frustration with the government response into some action. Mandiant "…wanted to do our part to arm and prepare security professionals to combat the threat" (Bejtlich, in US House of Representatives, 2013a, p. 35), but they had also described themselves as being "…on the front lines of the cyber battle, responding to active computer intrusions into dozens of American companies" (Mandia, in US House of Representatives, 2011, p. 36). One of the statements made by a representative of Mandiant was indicative of the ways they wanted to downplay and reconfigure the differences between government agencies and private actors:

> I would encourage anyone who believes that they are on the shopping list for an advanced threat, such as China or Russia, to have a relationship with your local FBI office… However,

> cyber still remains the one area where if there is a dead body on the ground, there is no police you call who will run to you and do the forensics and all that. For the most part, it is still a private-sector response. This is changing a little bit [for example with the United States Computer Emergency Readiness Team (US-CERT)]… But my company was created 9 years ago because there was no one to call. So we are the ones that go out, and we answer the call on these intrusions (Bejtlich, in US House of Representatives, 2013b, pp. 41–42)

Statements such as these revealed the extent to which Mandiant envisioned themselves as supporting and even standing in for state actors in cybersecurity, evocatively likening themselves to the police or FBI first responders dealing with 'a dead body on the ground.' Mandiant's testimony was thus a product of, as much as it reflected and reinforced the official discourses (discussed in Part One) about cybersecurity necessitating a blending of public and private responses to cybersecurity, even while this testimony was constituted by their own experiences as government- or military-trained specialists.

Another collaborative strategy was evident in how Mandiant would work to legitimise their work by situating their report in reference to broader governmental cybersecurity policies and discourses. In media interviews, Mandiant's Chief Security Officer Richard Bejtlich had explained that this was "…a time when there is a real push for security. The president just signed an Executive Order [13636], … and there are bills coming [in Congress on cybersecurity]" (in Armerding, 2013 n.p). In light of the complaints about government inaction discussed in Part One, 'critical' timing was thus cited as a significant rationale in Mandiant's decision to publish their research. This was also intended to lend more weight to their efforts. Before February 2013, Mandiant was little-known outside of the computer security community, but the report's publication gained mainstream news broadcast coverage and was featured across a range of technology journals, blogs and National Public Radio (Armerding, 2013). As one reporter for the Associated Press described the report, it put "…Mandiant front-and-center at a critical time on a national debate about cybersecurity [as its] founder [Kevin Mandia] testified earlier this month to the House Intelligence Committee on hacking threats" and intelligence sharing (Flaherty, 2013 n.p). Unlike the kinds of 'malware reports' typical of specialist computer security companies, which had historically tended to describe the results of reverse-engineered binaries (Bouwman *et al.*, 2020), this report was described by Mandiant as 'threat intelligence' and was one of the first of its kind, particularly in the amount of attention it received.

While in some respects Mandiant would argue that the company could stand in for state actors, they would also cite their unique technical capabilities to demonstrate how they could also supplement the government's role. By 2015, Mandiant were claiming they had a presence on one-third of Fortune 500 corporations (Bejtlich, 2015). Claims such as this implicitly signalled who and what

were deemed to be of most value in this vision of cybersecurity: companies with a high turnover were the ones deemed most in need of protecting, or perhaps were the most able to pay for Mandiant's expensive services (Finkle, 2020). The insights afforded by their presence on such networks was described as adding value to government efforts:

> Mandiant, when we obtain intelligence, we do it what I call laterally. We have to go from company to company to company to company. I think that the government is uniquely positioned at the top of the pyramid where they can get information from the bottom, which means they will have a top-down view that should be and is more comprehensive in scope than what Mandiant can provide going laterally. (Mandia, in US Senate, 2013b, p. 13)

While the government possessed this unique and comprehensive 'top-down view,' Mandiant thus articulated their distinctive contributions in terms of their insight into networks. The Mandiant APT1 Report built its claims for attribution based on visibility into the networks of 141 organisations, observing 1,905 instances of attackers connecting to command and control infrastructure for their attacks (Mandiant, 2013). This insight was something government actors had long been lamenting as a missing component in their own defensive policies and efforts (as we saw in Part One).

This was collaborative boundary work intended to make space for private sector involvement by firms such as Mandiant, without supplanting the 'unique' contributions hailed in the work of government agencies. The government's role was still thought to be an important source of authority. In other testimony Mandiant would draw these distinctions again to reference how the company could supplement the government's role:

> …our sense was that the government wanted to talk about this and we had the evidence to talk about it. And the report is completely based on our work, completely unclassified, not corroborated with government information. (Bejtlich, in US House of Representatives, 2013a, p. 27)

Emphasising how their work was entirely their own and not supplemented by government information was a way of giving lawmakers the political space to utilise the report without facing diplomatic repercussions. While government actors had been politically and technically constrained from making such public accusations, attribution reports like Mandiant had the potential to attenuate government responsibility for the technical judgements, which could have diplomatic benefits (Lin, 2016). This meant that Mandiant were also working to demarcate their independence from the government. As their blogpost accompanying the report explained:

> Without establishing a solid connection to China, there will always be room for observers to dismiss APT [advanced persistent threat] actions as uncoordinated, solely criminal in nature, or peripheral to larger national security and global economic concerns. (McWhorter, 2013 n.p)

In this way, Mandiant were providing a service that fed into wider narratives about the links between cybersecurity and national security, whilst also working to reconstitute conceptions of the political and technical acceptability of private attribution reports.

5.3.2 Government efforts to legitimise and orchestrate.

While Mandiant had done something unusual by publicly attributing a state actor, it was the work of state-representatives in Congress who would ultimately legitimise this report, as part of their efforts to orchestrate the cooperation of non-state actors through a mix of configurational and collaborative boundary work. Congressional lawmakers were therefore quick to take up the report in support of their political goals. Notably, Mandiant's testimony was used in appropriations hearings for the DoD budget for 2014 (US Senate, 2013b), indicating the ways that Mandiant's account of threats from China were used by legislators as part of the justifications for defence spending in addition to the cybersecurity legislation they were working to pass. In one of these Senate hearings, the Chairman of the Armed Services Committee described their report as…

> …a unique achievement in the depth of the research and the scope of its documentation. The report is impressive too for its professionalism and lack of sensationalism, and it lets the facts speak for themselves. (Hagan, in US Senate, 2013b, p. 2)

Claims about the ability of facts to 'speak for themselves' were an important part of efforts to depoliticise the report and its methodologies. Describing the report in this way was a strategy designed to invoke the credibility thought to derive from 'fact-based' policy making, and in turn legitimise its use in the discussions (Jasanoff, 1987). At the same time, by describing their report as providing "an important service for our public" (Hagan, in US Senate, 2013a, p. 2) policymakers were also granting Mandiant ideational support by attributing their efforts as a service to a greater good than policymaking alone, but also for the 'national good' of cybersecurity.

Describing the report in terms of intelligence community grades of quality was invoked as another marker of credibility. Here, lawmakers would draw upon the credentials of Mandiant's employees to highlight their (insider) qualifications for the job at hand when they described the quality of the report:

> The Mandiant Corporation has produced an Intelligence Community quality report without the benefit of the tools and authorities of our government and without the accompanying classification restrictions." (Hagan, in US Senate, 2013b, p. 2)

Here, government actors were signalling what was possible without the 'restrictions' typical of government work in this context, signifying where they thought such companies could fit into broader cybersecurity efforts. These credentials were something that Mandiant were careful to underscore too. Mandiant's report was unusual because unlike the malware reports other computer and network security companies had generally produced until then, such 'threat reports' would instead focus on the tools, techniques and goals – the modus operandi – of specific groups of hackers. In this way, the company was making a product that simulated the kinds of reports generated in the intelligence community, using similar vernacular and argumentation, even if it was in a far glossier promotional presentation. The company was composed of former members of the armed forces and intelligence community: its founder Kevin Mandia was a former U.S. Air Force cyber-forensics investigator, its General Counsel Steven Chabinsky was formerly a Deputy Assistant Director of the Cyber Division for the FBI's cyber intelligence program, and its Chief Security Officer Richard Bejtlich was a former Air Force intelligence officer with their computer incident response and cyber warfare divisions (Reese, 2011; Chabinsky, 2014; Finkle, 2020). As "a dedicated group of […] former military, former law enforcement, former Intelligence Community, and then just very motivated, highly skilled computer security people," (Bejtlich, in US House of Representatives, 2013a, pp. 27–28), statements such as these were illustrative of their efforts before Congress to position themselves as distinctively qualified to make these attribution reports. It also illustrated the extent to which ideas of 'cybersecurity' would be shaped by a revolving door between government employment and corporate testimony (Leander, 2014). Such distinctions would serve as instrumental strategies as much as they were a set of 'common-sense' cultural reference points for actors used to operating in government agencies.

'Extending' cybersecurity in the ways envisaged in official statements (from Part One) would require new non-federal actors to be legitimised to help them actualise federal visions for cybersecurity. By legitimising Mandiant's efforts, lawmakers were working to draw upon and mobilise the capabilities of non-governmental actors in support of their overall goals of drawing the parameters of cybersecurity's roles and responsibilities. Ranking committee member Congressman Patrick Meehan would praise the report in the highest terms:

> Members are also lucky to have a representative from Mandiant Corp. here today to testify on the cyber threat posed by China. […] a great deal of credit goes to Mandiant for its long-term work identifying the specific Chinese military unit responsible for looting our intellectual property and technological innovations and publicly naming its actual geographic location.

> That report is a service to all policymakers striving to combat the Chinese cyber threat. (Meehan, in US House of Representatives, 2013b, p. 4).

That this report was described as servicing policymakers' goals in this way was thus an explicit rationalisation of some of the government's strategic and political goals to orchestrate these efforts. He went on to further validate and lend credence to the report by citing "…perhaps the premier American intelligence official, former CIA and NSA director […] General Michael Hayden, who simply stated: 'It was a wonderful report.'" (Meehan, in US House of Representatives, 2013b, p. 7). Such an instrumental use of Mandiant's report and testimony would serve strategic and political goals. Policymakers were here making the case for the importance of private involvement in and shared responsibility for cybersecurity, granting the private sector legitimacy in their actions. In this instance, it was not just that Mandiant or other firms were being tasked with roles traditionally the remit of government actors, or that they were officially sanctioned in doing so, but that the parameters of these respective roles were each evolving and iterating over time so that attribution was no longer the sole remit of government actors.

5.3.3 Actualising a vision of cybersecurity for corporations and government

This collaborative boundary work by Mandiant and lawmakers would have productive effects. The prevalence of their testimony shows that Mandiant's efforts fed directly into the legislative process of the US and were also in turn used instrumentally by elite security actors to highlight the 'necessity' for private collaboration and the redistribution of responsibilities. Evidence such as Mandiant's was enabling lawmakers more broadly to develop specific policy responses and also helped to promote massive investment in new technologies. In the years prior to Mandiant's report, articulations of the threat to US national security posed by Chinese hacking had been mentioned in only two or three hearings a year, despite evidence of Chinese presence on DoD networks since the 'Titan Rain' campaign of 2001 (Kaplan, 2016; Harris, 2014). This level of concern escalated following Mandiant's report and Executive Order 13636, with thirteen hearings over the course of 2013 alone mentioning the threat to national security posed by Chinese hacking and espionage. Despite eighty-six bills related to cybersecurity introduced in the course of President Obama's administration, only three of those bills were passed into law and Mandiant's report fed directly into these legislative efforts. All three laws were informed by congressional hearings that either cited the Mandiant report directly or included testimony from the company. By 2015, Mandiant's congressional evidence had contributed its part in helping governmental actors produce the bounds of commercial and federal involvement in 'cybersecurity' by granting them legitimacy in naming nation-state actors.

The collaborative boundary work of Mandiant and lawmakers to reconfigure distinctions between federal and commercial roles in cybersecurity would have also a constitutive effect in producing a lucrative market for these products. By January of 2014, Mandiant had been acquired by FireEye, a cybersecurity firm, for approximately a billion dollars (Finkle, 2014), with some suggestions that the release of the report was a strategic manoeuvre to generate press and value (Finkle, 2013). Furthermore, following the publication of (and publicity surrounding) Mandiant's report, a new "cyber threat intelligence" industry gained traction (Oosthoek and Doerr, 2020). Mandiant's report was the most high-profile example at that time of the work of a 'threat intelligence' company and had a formative role in kickstarting a now multibillion-dollar market. The commercial market was valued recently at over $5 billion globally and is predicted to triple within the next five years (Bouwman *et al.*, 2020), with the products of these companies driving value within a wider global information security market (Work, 2020).

Despite policymakers hailing the company's technical expertise and 'objective' methods, making an attribution claim was not a neutral or apolitical process. Other companies conducting research on the activities of 'advanced persistent threat' hacker groups have deferred from making attribution claims, arguing that "[p]erforming attribution in a serious, scientific manner is a hard problem that is out of scope of [our company's] mission" (ESET, 2016, p. 11). These visions of cyber (in)security also favour a particular subset of interests and values. While the company claimed that they were "releasing more than 3,000 indicators to bolster defenses against APT1 operations" (Mandiant, 2013, p. 5), these indicators would benefit only a very few American companies who were likely to be on the receiving end of state-actor levels of persistent hacking activity. Petty criminal cyber activities are more commonly experienced by companies than 'APT,' but reporting on big nation-state actors produces good marketing (Oosthoek and Doerr, 2020). The data that Mandiant and other companies 'translate' into the policy process were also less complete than they imply. In a recent study of the 'intelligence feeds' of the two biggest cyber threat intelligence firms (including Mandiant's parent company FireEye), researchers discovered that of the twenty-two threat actors for which both vendors have indicators (such as the APT1 group named by Mandiant) there was an overlap of no more that 2.5 to 4% per group between feeds (Bouwman *et al.*, 2020). Given that vendors claim to be researching and providing threat intelligence on the same threat groups who use the same tools and techniques, such a small overlap in technical indicators of compromise challenges the possibility that these vendors can ever provide sufficient coverage (Bouwman *et al.*, 2020; Oosthoek and Doerr, 2020). The point here is that reporting on such incidents is therefore not simply a neutral or technical analysis, but requires all kinds of context and sense-making, and lawmakers' understandings of these incidents are shaped by the cultural and political prisms of the people carrying out the analyses (Egloff, 2020; Shires, 2020; Stevens, 2020).

This section has demonstrated that through configurational and collaborative boundary work, government actors have orchestrated the efforts of intermediaries – in this case, Mandiant – in pursuit of shared political and material interests. Boundary work by government actors gave Mandiant material and ideational support that gradually supported and produced an alignment in visions of 'cybersecurity.' State actors are thus acting as orchestrators by setting the boundaries of legitimate public and private involvement in a strategic way to achieve their ends, but with the result that norms of public and private practice in security are gradually being extended in the case of attribution. These are not practices that state actors are formally privatising. Instead, both 'public' and 'private' actors are involved in co-constituting these practices and the associated norms for operations in cyberspace, demonstrating the ways that modern security practices are rarely a neat divide between two opposing or distinct logics. It is not just a 'rise of the private' security actor or commercial logics, but a continual re-articulation of the relationships between imaginaries of 'public' and 'private' roles and responsibilities. Cybersecurity debates in this context thus become about fixing the bounds of cybersecurity so that they conform to (but also at times challenge or reconfigure) ideas about the state as security provider, and the state's relationship with cyberspace.

However, as I will now demonstrate through an analysis of controversies surrounding Apple's encryption technologies, governmental efforts at orchestrating cybersecurity by drawing distinctions between 'public' and 'private' have not been so successful in other this context. While government actors and threat intelligence firms co-produced a vision of cybersecurity in favour of protecting intellectual property and 'corporate America' using collaborative strategies *at* boundaries, technology companies such as Apple would claim fundamentally different definitions of 'security' to government actors through competitive boundary work *for* boundaries. Theirs was a view of cybersecurity claimed in terms of individual security, in distinction to governmental conceptions, and to Apple's own instrumental ends and benefits. As a result, they would be less willing to actualise governmental visions of insecurity on their behalf and would instead invoke and mobilise those category distinctions to different political ends, thus producing different visions of 'cybersecurity.'

5.3.4 Encryption as a challenge to federal imaginaries

In the controversy between Apple and the FBI, the qualities and benefits of encryptions technologies would be hotly contested. As in the previous case, boundary work would centre on distinctions between 'public' and 'private' and the roles that such symbolic and categorical boundary work sought to legitimise. In the case that follows though, rather than downplaying boundary distinctions to facilitate a re-distribution of authority through configurational and collaborative boundary work, state actors would seek to establish the legitimacy of their actions by *policing* such

boundaries in competitive strategies, in what was described as "the perennial struggle" between privacy and enabling public safety. Here, specific technical features of encryption were drawn out to invoke boundary configurations, rhetorically and functionally, depending on the interests of the actors. Law enforcement would pose encryption as a barrier to being able to undertake their customary roles and responsibilities and would seek to shift the (technological) boundary by using a court order to implement their objectives, strategically seeking to reawaken the debate they had failed to win from the 'Crypto Wars.' Meanwhile, Congress' would try policing these boundaries through stalled legislation and rejected commissions, signifying the limits of their desire to downplay and orchestrate distinctions of public and private for organising cybersecurity. The analysis will argue that while these efforts were intended to orchestrate the enrolment of Apple as an intermediary for the government's conception of 'cybersecurity,' these initiatives are examples of unsuccessful efforts by political leaders at stabilising their boundary work, indicating some of the limits of the authority and legitimacy that state-based actors were able to mobilise with their boundary work strategies.

5.3.5 Court orders and dissenting imaginaries

In February of 2016 the FBI filed a request that a federal magistrate in California order Apple to help the FBI unlock a single iPhone: the phone that had belonged to one of the perpetrators of a mass shooting in San Bernardino in December 2015. The court order was an attempt by law enforcement to use legal precedent to legitimise their preferred course of action and to institutionalise new (legal) parameters for acceptable practices in the future. The court order application was built on the premise that encryption technologies presented a barrier to the FBI undertaking their 'traditional' responsibilities, echoing the debates of the 'Crypto Wars' (Hellegren, 2017; Schulze, 2017; Jarvis, 2020). Apple would resist those framings and offer an alternative imaginary rooted in civil society, questioning federal interventions in matters of digital security. Between the court order application and Apple's public responses, the attributes of the specific iPhone formed the basis of much of the ensuing controversy and served as a means for actors to articulate the limits of their respective roles.

In the court order, the FBI sought to distinguish theirs and Apple's respective roles and responsibilities by portraying the features of encryption in a way that implied a neat separation between government remits and the company's capabilities. In describing features of the phone in terms of problematic "non-encryption barriers" (United States of America v Apple Inc, 2016), the court order application sought to differentiate between the algorithms and encryption keys that encrypt or scramble the phone's data ("encryption") and the features that serve as an interface with the encryption processes ("non-encryption"). The court order thus requested Apple's assistance in

overcoming the 'non-encryption' barriers by building a new version of the phone's operating system that would circumvent "several important security features" on the phone (Apple, 2016). The court order application described the technical features in such a way that suggested security was made up of features that were isolatable: firstly, that isolating one phone's security features would not affect other phones' security features, and secondly, that each piece of security software could be 'switched off' and isolated from the others with a technical solution from Apple. Though the government lawyers sought to demarcate the legitimacy of the prospective FBI actions arising from the court order by restricting it to the single phone, Apple would instead argue that this was no simple technical fix and that the features of the iPhone's security that the FBI's application was trying to isolate were in fact only effective as part of a whole.

By discussing the security features of the phone in essentialised terms, the court order tried to neatly delineate 'digital security' from 'national security and public safety.' Instead, Apple invoked the security features of the phone to argue that such a neat demarcation of was impossible because of the broader security repercussions such a move would have. As Apple described it, the problem with this approach was that "[i]n today's digital world, the "key" to an encrypted system is a piece of information that unlocks the data, and *it is only as secure as the protections around it*" (Apple, 2016 n.p.). Apple's objection was thus based on the ways that "encryption" was not simply a discrete technology but only effectively functional as part of a whole system of features. In fact, Apple argued that contrary to the FBI's claims in the court order application, by building this new operating system the whole security system of all Apple phones would be compromised, stemming from the ways that security features work as part of an interlocking ecosystem, not as isolatable switches. They argued that if they built this new iOS, they would effectively be building a "backdoor," one which ran the risk of revealing how to circumvent the passcode interfaces and thus undermine encryption's efficacy.

For the FBI, encryption technologies were an obstruction to be overcome as much as an opportunity to retry the terms of the encryption debate. The court order application thus imputed Apple with 'coding' the technical features of the phone to carry out Apple's intentions to obstruct law enforcement. In one indicative passage, the court order application described the problem whereby

> …the FBI has been unable to make attempts to determine the passcode because Apple has written, or "coded," its operating systems with a user-enabled "auto-erase function" (United States of America v Apple Inc, 2016)

In other words, the FBI implied it could not do its job because Apple had intentionally coded its operating systems in a particular way. By framing the matter as public safety versus privacy, those in favour of getting access to these "encryption-proof spaces" would talk of technological affordances in essentialised terms as a way to separate the effects that access to a single phone would have to

broader matters of national or cyber- security. According to this narrative, if law enforcement were to be able to maintain their customary responsibilities, then "the Going Dark problem is, at base, one of technological choices and capability" preventing law enforcement from obtaining "evidence pursuant to the legal authority that Congress has provided to keep America safe." (Comey, US House of Representatives, 2016a, p. 12). The implication was that this was a technical choice, that it should be a neutral or a-political matter. The court order application and congressional testimony therefore tried to make the case that Apple's involvement was primarily a question of technical capability, that Apple's rightful role in the matter was to provide a technical tool, rather than obstructing law enforcement from fulfilling its responsibilities as it was.

However, Apple would narrate a competing imaginary of what was at stake. According to Apple's Lawyer and representative, "we have told them and as we have told the American public, building that software tool would not affect just one iPhone. It would weaken the security for all of them." (Sewell, in US House of Representatives, 2016a, p. 99). Although Apple acknowledged in hearings that the 'technical fix' that the FBI have asked for in the court order was technically possible to build, they argued that it was not technically *feasible*. By asking Apple to 'weaken the security' of their products, Apple's representative suggested that their compliance with the FBI's request for technical assistance could be used by "hackers and cybercriminals… to wreak havoc on our privacy and personal safety" (ibid). As the computer security expert called on to testify suggested, the "FBI has pitched this battle as one of security versus privacy, but as a number of the Members have already observed, it's really about security versus security" (Landau, in US House of Representatives, 2016a, p. 104). 'Security' was invoked to mean different – and incommensurate – things in this debate. She was here suggesting that at the heart of this debate there were differing notions of security at work amongst the different stakeholders, and that by framing of the matter in terms of public safety and privacy the FBI was treating encryption as a separable feature rather than a foundational requirement for cybersecurity. For Apple, 'security' was drawing on a conception from the technical community that was oriented around the engineering parameters of encryption (Nissenbaum, 2005), while for the FBI, theirs was a broader conception of security that was thought to be synonymous with 'public safety.'

These were fundamentally opposing visions of what 'cybersecurity' was about, and whom it served. By emphasising the complex ecosystem of encryption's features and capabilities, the pro-encryption advocates envisaged encryption as a key constituent of both national security and privacy and argued that the two should not be mutually exclusive. Accordingly, by asking Apple to circumvent the "non-encryption" features of the iPhone, the FBI was described by its critics in the information security and privacy advocacy communities as putting the whole country's security at risk:

> …if you think more broadly about the risks that our nation faces … you've been hearing it from … all the people who have been involved on the DHS and NSA side. The only thing that can secure [national security] is security everywhere, and the move that Apple makes to secure the phones is one of the many steps we need in that direction. (Landau, in US House of Representatives, 2016a, p. 170)

Thus, encryption was synonymous with cybersecurity and could provide a technical 'fix' for national security; while for the Department of Justice, encryption was equated to an obstacle to national security.

As Apple's objection to the Court Order above had argued, their vision of cybersecurity was that it should protect the privacy and security of individuals. When asked in the Congressional hearing why "we are moving to end-to-end encryption on many devices and apps, not just Apple iPhones", Apple's representative suggested that it was "a combination of things", but that from Apple's perspective, it was…

> …because we see ourselves as being in an arms race, in an arms race with criminals, cyberterrorists, hackers. We're trying to provide a safe and secure place for the users of our devices to be assured that their information cannot be accessed, cannot be hacked or stolen. (Sewell, in US House of Representatives, 2016a, p. 146)

Theirs was described as more than just a response to market pressures, but a series of design choices and features emerging in response to an 'arms race' of actors, capabilities and technologies. Apple gave more detail in their letter to their customers following the Court Order, suggesting that they had…

> …built progressively stronger protections into our products with each new software release … because cyberattacks have only become more frequent and more sophisticated… Hackers and cybercriminals are always looking for new ways to defeat our security, which is why we keep making it stronger (Apple, 2016 n.p.)

According to this narrative, Apple objected that their technical assistance was not such a simple or neutral matter. More than a designer and purveyor of technology, Apple framed the matter in terms of their security responsibilities to their customers. Apple maintained that if they complied, the government "…would have the power to *reach into* anyone's device to capture their data." (Cook, 2016 n.p., emphasis added). The company argued that "…the order would set a legal precedent that would *expand the powers of the government* and we simply don't know where that would lead us" (Cook, 2016 n.p., emphasis added). Implicit here was a normatively laden notion of how the

boundaries around and between government action and private companies *should* operate. Apple acknowledged in their public statements that technology firms can and should cooperate with law enforcement when warrants and subpoenas compelled access to private data, but that this specific effort to compel Apple's assistance would transgress the boundaries of established behaviour for government actors. Apple was thus narrating a vision in which they were curtailing a perceived expansion of government powers.

Apple also disputed law enforcement's efforts to distinguish between 'cybersecurity' and 'national security' and sought alternative ways to enlist a broader consensus. In their legal response to the court order, Apple described encryption as something that it used to "…protect its customers from cyber-attack… It is these protections that the government now seeks to roll back by judicial decree" (Boutous Jr et al, 2016, p. 2). For Apple, losing control of data was synonymous with putting "privacy and our safety at risk" (Apple, 2016 n.p.), implying that the government was thus undermining security standards it was traditionally tasked with protecting. The technology firm's attorneys argued the government was using the court order to seek…

> …a dangerous power that Congress and the American people have withheld: the ability to force companies like Apple to undermine the basic security and privacy interests of hundreds of millions of individuals around the globe. (Boutrous Jr, Hanna and Vandevelde, 2016, p. 1)

In this case, Apple argued that they were standing in for more than just their American customers, but for hundreds of millions of individuals worldwide. Moreover, they argued, the court order was trying to expand the government's remit in a way that Congress had more legitimacy to decide than the courts:

> …rather than pursue new legislation, the government backed away from Congress and turned to the courts, a forum ill-suited to address the myriad competing interests, potential ramifications, and unintended consequences presented by the government's unprecedented demand. (Boutrous Jr et al 2016, p. 1)

Of the options open to law enforcement, Apple here argued that boundaries between digital security and national security, and the boundaries circumscribing legitimate government jurisdiction should be established through legislation rather than legal precedence.

The FBI were thus unable to force Apple's cooperation, despite their competitive boundary work and strategic practical efforts to build support for their vision of cybersecurity though the court order and congressional hearings. While representatives of the FBI, Apple and security experts were called to testify before Congress on the first of March that year with a view to informing legislative

action, as the next section of the chapter will draw out, Congress would have little success in adjudicating the 'myriad competing interests' Apple had cited in their application.

5.3.2 Failed congressional efforts at orchestration

While the court order and the application narrated encryption as a 'barrier' to government actors doing their rightful jobs, the hearings and Congressional initiatives that followed were instead concerned with establishing how encryption technologies could be 'balanced' with the customary roles and responsibilities of government actors and technology companies. Here, lawmakers would seek to orchestrate the cooperation of companies and corporate actors in actualising the federal vision of cybersecurity through configurational boundary work. As far as these lawmakers were concerned, it was the task of government actors to adjudicate and settle the ambiguities of encryption technology. Two illustrative actions taken by Congress demonstrate the work that lawmakers put into building a case for how the government should resolve the boundaries being contested in the controversy. One was a proposal to instigate a Commission to build consensus on how to regulate the use of encryption, while the other was a piece of legislation designed solely by lawmakers, to regulate and restrict the uses of encryption. As this next section will now demonstrate, both initiatives were efforts to rhetorically and legally establish how past experiences or current roles fitted into a 'new' technological context. However, unlike in other chapters in the thesis, an examination of these cases shows how both initiatives are examples of unsuccessful boundary work, in that they were unable to make the case for extending the boundaries of permissible government action into the regulation and uses of encryption.

Invoking ideas of national identity was one of the strategies that lawmakers used to stake out the legitimacy of particular actions or claims to legitimacy. One committee's chairman suggested that encryption was a topic with wider implications than being "arcane, or only the province of techies", recognising that it was "…a subject whose solutions will have far-reaching and lasting consequences", arguing for Congress' central role in adjudicating "the perennial struggle between protecting Americans' privacy and enabling robust public safety." (Goodlatte, in US House of Representatives, 2016a, p. 2). Goodlatte went on to make the rationale for the title of the hearing explicit, suggesting that "…society has been walking a tightrope for generations in attempting to balance the security and privacy of Americans' communications with the needs of our law enforcement and intelligence agencies." Boundary work would thus centre around strategic efforts to configure, negotiate or 'balance' encryption with these ideas of national identity and 'foundational' rights, roles and responsibilities as part of their efforts to "rearrange the sets of boundaries influencing others' behaviours" (Langley et al., 2019: 8).

The first Congressional initiative that sought to help lawmakers build a case for how past experiences or current roles fit into a changing technological setting. Here, lawmakers recognised that they were unable to deal with this matter single-handedly "…while all sides continue to talk past each other" (Warner, 2016 n.p.) and that they would need establish a "dialogue that takes fuller account of technological limitations, investigative tools and legal needs" than "politicians debating one another" would normally permit (McCaul and Warner, 2015 n.p.). It sought to build a consensus of technical experts and governmental actors in order to "…strike a balance between protecting our privacy and strengthening our national security" (Warner, 2016 n.p.). In the intervening period between the Court Order filing and the Congressional hearing, a bipartisan group of senators and representatives introduced legislation that would convene a multi-stakeholder 'National Commission on Security and Technology Challenges' that would be "…charged with developing recommendations for maintaining privacy and digital security" at "…the intersection of digital technology and national security" (Warner, 2016 n.p.).

In other words, the Commission would be charged with determining how encryption would work or moderate the boundaries of that intersection. By bringing together "leading experts and practitioners from the technology sector, cryptography, law enforcement, intelligence, the privacy and civil liberties community, global commerce and economics, and the national security community", it was hoped that the Commission could "break the deadlock" in the fundamentally different interpretations of the technology and its implications for security (ibid). The Commission was thus intended to provide a crucial starting point for future legislative action, one of the main responsibilities Congress has traditionally been tasked with and one of the courses of action thus open to them.

However, the bill did not progress beyond its introduction. Although the Commission was intended to open up the debate to multiple stakeholders, it was still intended to lead to legislation concerning the use of encryption, or in other words, to somehow regulate who could use encryption technologies and in what circumstances. According to the Center for Democracy and Technology, a think-tank funded by technology companies such as Apple and Google (Influence Watch, 2019), "…it is hard to envision what a new Commission focused on old, well-settled issues can hope to accomplish" other than legislation that would try to regulate or restrict the use of the technology as the Clipper Chip debates had tried (CDT, 2016 n.p.): rather than finding alternative solutions or avenues open to Congress, a Commission would just lead to another failed set of legislative measures. The role that Congress could play in setting the parameters for encryption's uses (beyond acting as a forum for these claims to be aired) suggested that it was out of the bounds of their available interventions in this instance.

Another initiative developed by Congress to orchestrate and more formally delegate the responsibilities for actualising the federal vision of cybersecurity was a more direct attempt to legislate the use of encryption, but without the input of so many stakeholders. In April, two senators circulated a discussion draft of the 'Compliance with Court Orders Act of 2016', a bill that was intended to reinforce how technology companies should comply with pre-existing legal procedures. In this first draft, the senators tried to demonstrate how current authorities determining technology companies' compliance with warrants should be extended to encrypted communications, arguing that "no entity or individual is above the law " (Feinstein, 2016 n.p.). Although they did not mandate a specific technical solution nor require any specific design limitations on products, they stated instead that technology firms must provide unencrypted data to law enforcement or the means for law enforcement to obtain that data themselves (Burr and Feinstein, 2016 n.p.). The bill was intended to give federal judges broad authority to order technology companies to help the government. To remain legally compliant when issued with warrants, the legislation intended that companies would have to retain some means of decrypting data, a facility that would have to be designed into their products. This was designed to set a performance standard rather than mandate a specific technical solution, but it implied that some sort of technical solution would need to be devised by the companies.

However, this configurational boundary work to make the technological affordances of encryption fit within extant legal bounds was unsuccessful. The proposal faced heavy criticism from the technology and legislative communities, with the White House declining to support the legislation (Hosenball and Volz, 2016) and one senator stating that they would object strongly, even filibuster the bill, citing that it would "…undermine the foundations of cybersecurity for millions of Americans" (Wyden, cited in Conger, 2016). Boundary work is more than rhetorical: new legal precedent and legislation are each examples of efforts to reconfigure boundaries over time, of attempts to stabilise boundaries and practices. However, neither bill progressed beyond their introduction, indicating that this boundary work failed to stabilise boundaries in a lasting way.

Like the court order, boundary work here was about building a case for how past experiences or current roles fit into a new context, of rhetorically demonstrating how current authorities should be extended, as efforts to stabilise some (reworked) conceptions of boundaries. Encryption was implicitly taken to challenge the symbolic boundaries that defined legitimate state action in the federal imaginary of insecurity, in this instance by preventing state actors from undertaking their responsibilities for national security. However, congress was unsuccessful in building the normative case for their imaginary in the face of Apple's own boundary work and legal resources. Unlike the case of Mandiant, there were incommensurate conceptions of 'security' at work here which meant that the government was unable to convince nor compel Apple to act as their intermediary in matters of

cybersecurity. Apple had set a resilient symbolic boundary; one which law enforcement were unwilling or unable to challenge in public.

Encryption was thus posed as both a *key constituent of* and a *threat to* cybersecurity and national security, depending upon the context and interests of the speaker. That a technology such as this could lead to such incommensurate attempts at policy responses and system updates suggest how iterative and mutable these categories are. Whether or not it is the explicit intention of designers or users, the implementation of the technology here sets subsequent 'reasonable expectations of privacy' and forms the technical starting point of subsequent social practices and disputes.

5.4 Conclusion

Part One showed how DHS and other federal discourses articulated configurational boundary work strategies through a vision of 'extending' cybersecurity roles and responsibilities beyond the state. As part of this imaginary of insecurity, boundary distinctions were invoked and mobilised by government actors to set up the conditions for a reconstitution and shift of roles and responsibilities over time. We saw that as part of efforts to expand or enlarge the kind of tasks involved in producing their vision of cybersecurity and to make space for private sector involvement, state actors articulated an imaginary of insecurity in which their lack of insight into networks posed an existential threat to national values, social orders, and technological futures, with the intention of instigating particular kinds of collective action in the name of 'cybersecurity.'

In Parts Two and Three, the case studies worked as examples of how federal actors have sought to orchestrate and mobilise intermediaries in pursuit of their stated goals of public-private partnerships for cybersecurity outside of formal contract-based arrangements: in the case the Chinese hacking controversy, this saw actors undertaking collaborative and configurational boundary work to build the case for non-state assistance instead of, and in addition to, governmental attribution work. Meanwhile, in the 'going dark' encryption controversy, government actors were trying to compel technical assistance with encryption through competitive strategies *for* boundaries. The main difference lay in how willing the non-state actors were to engage with the government: in the case of attribution, elements of the private sector were actively endorsing a role for themselves where both state and non-state actors carefully downplayed boundary distinctions through collaborative strategies. The second case of encryption meanwhile was demonstrative of the technology companies pushing back and of technology resisting the efforts of law enforcement to work *for* drawing boundaries in new ways with competitive strategies. Here, Apple were working to produce distinct and clear boundaries between groups. The failed boundary work of congressional lawmakers in this chapter again reflects the overall argument in this thesis that cybersecurity practices are not as

structurally and technologically driven as federal discourses suggest: competing visions of cybersecurity have emerged through boundary work, not all of it federal, and not all (competitive, collaborative, configurational) strategies are equal. Moreover, federal actors may not be able to mobilise the resources in support of boundary work in the ways that some private sector actors may be able. The perceived legitimacy of boundary work, it widespread acceptance and subsequent concretisation in sociotechnical arrangements, does not automatically stem from the resources or political prominence of the actors involved, as in the case of failed governmental efforts who failed to mobilise the likes of Apple into their initial vision of cybersecurity and boundary work *at* distinctions of 'public' and 'private.' But it also underscores the social nature of boundary work as much as its ability to be materialised and concretised: its 'success' is contingent upon an audience (with legitimacy and authority of their own) hailing that boundary work.

We also saw how at least two different visions of cybersecurity – and who it is *for* – emerge from the ways that different actors invoke and mobilise those categorical distinctions. Both Mandiant and federal actors were able to mobilise those distinctions for instrumental ends, empowering Mandiant and other threat intelligence companies to conduct public attribution reports, whilst focusing on measures that favour the protection of intellectual property and those corporate business interests. Meanwhile, Apple were able to mobilise their resources, lawyers and public relations to contest the governments efforts to compel their compliance, focusing on a conception of security putatively in the name of citizens' rights and individual liberties. That said, their corporate interests were also served by their boundary work and the resources that they were able to mobilise to protect those interests.

The case studies in this chapter demonstrated how category distinctions of public and private are culturally specific, mutable, contingent, and context-dependent. The analysis in this chapter supports the thesis' premise that these are not essential categories that form the subject of boundary work in cybersecurity politics. In both of these cases, we can see how these boundaries are simultaneously the source and the result of contestation: like 'cybersecurity,' boundaries are emergent and contingent phenomena. Nevertheless, we have seen how such boundaries make a difference: in this chapter, distinctions of public and private act as a basis for claims to political legitimacy and authority, setting bounds upon 'cybersecurity' in specific ways. The findings of this chapter do not suggest a zero-sum shift of political authority from 'public' to 'private', but a fragmentation and reconfiguration of political authority that favours the interests of those who can mobilise and embed those distinctions with their resources. Boundary work is strategic practical action, it is about interests and power, and this chapter has shown the interests at work in invoking particular configurations of distinctions between public and private, and invoking cybersecurity's public or private characteristics. Just like science is not a singular thing but has different characteristics

depending on who is speaking (Gieryn, 1989), cybersecurity is attributed different public or private characteristics depending on who is speaking. We will see this too in the next chapter, but unlike this chapter's efforts to enrol and orchestrate those outside the government, we will now turn to an account of competitive boundary work by federal actors. Rather than trying to enlist the involvement of the private sector, the next chapter shows how official efforts to defend the legitimacy of official visions of 'cybersecurity' will be in distinction to those security imaginaries of the private sector and civil society groups.

Chapter Six: Making vulnerabilities and cybersecurity intelligible through 'disclosure' and the VEP.

6.0 Introduction

From 2013 onwards, a series of cyber breaches and international cybersecurity incidents prompted criticisms from diverse commentators outside of the US government. They challenged the rationales and legitimacy of the government's use of software and hardware vulnerabilities in the course of intelligence and law enforcement missions. In response to accusations that "the NSA – despite what it and other representatives of the US government say – [is] prioritizing its ability to conduct surveillance over our security" (Schneier, 2016 n.p), government representatives and White House administration officials over the course of two administrations would gradually release details of an interagency deliberation process called the Vulnerabilities Equities Process (VEP). While the VEP started life as an initiative that was wholly classified, the VEP and 'disclosure' would gradually become the locus and shorthand for broader debates about the parameters of the Federal government's role in 'cybersecurity.' As we shall see, the *competitive* boundary work analysed in this chapter is about two conceptualisations or visions of what cybersecurity *means*, what it *is* – to patch, or to spy; a technical conception of cybersecurity to secure cyberspace by fixing vulnerabilities, or a political conception of cybersecurity to secure cyberspace by utilising vulnerabilities for wider strategic ends. Those outside of government meanwhile would articulate alternative imaginaries of insecurity to administration officials.

Like other chapters that have shown how different characteristics are ascribed to cybersecurity at different times, depending on the interests and background of the speaker, this chapter finds that 'disclosure' has been used to demarcate political and operational bounds of 'cybersecurity.' This chapter will argue that the VEP has worked as strategic practical action intended to legitimate a federal vision of cybersecurity biased towards the interests of intelligence and law enforcement, a vision in which the use of vulnerabilities for law enforcement and intelligence can be rationalised. Here, 'national security' has been invoked to signal the limits of 'cybersecurity.' This is a conceptualisation in which the use of vulnerabilities is claimed to not undermine broader 'cybersecurity,' and the VEP is an example of an initiative that has emerged in response, but also in turn shaped, that security imaginary.

While the chapter argues that the VEP has set procedural and practical parameters on disclosure in order to protect the autonomy of government agencies to use vulnerabilities, it will also show first how official discourses have adapted to dissenting narratives in order to defend the political

legitimacy of the government's conceptualisation of cybersecurity in Parts One and Two. Part One will demonstrate how disclosure was used as the basis for claims to legitimacy by different communities. In the case of Federal actors, 'disclosure' was used as competitive work *for* boundaries between lawful and illegal uses of vulnerabilities, and to draw boundaries between 'national security' and 'cybersecurity.' This boundary work had the aim of reasserting the legitimacy of Federal agencies in the face of external criticisms and to redraw the political stakes of 'disclosure.' Meanwhile, Part Two will show how critics of the government's claims would articulate different roles for 'disclosure' to contest the government's vision. Here, they would undertake competitive boundary work strategies to challenge the government's claims, methods and rationales for weighing whether to retain or disclose vulnerabilities. Part Three will then show how federal actors have worked to constitute 'disclosure' in particular ways.

This chapter will show how vulnerabilities are not simply technical or external structural imperatives, but are a product of an interplay of technical, social and political efforts, and are made intelligible through strategic practical action. Put another way, I argue that boundary work and the VEP play an important part in making vulnerabilities intelligible, and work to constitute vulnerabilities in particular ways. Specifically, this chapter argues that in response to those external criticisms, the VEP is strategic practical action to 'translate' vulnerabilities into quantifiable entities that can be deliberated, rationalised and putatively unbiased. This is important because by circumscribing vulnerabilities in this way and by gradually constituting 'disclosure' as a spectrum rather than a binary choice for 'cybersecurity,' this chapter finds that the VEP has re-constituted boundaries of disclosure to accommodate their vision of cyber (in)security. The political and procedural parameters of disclosure have thus been drawn differently and reconstituted over time through these debates to 'do' or facilitate different things. First though, the chapter will show how a series of controversies would trigger boundary work by government representatives that used 'disclosure' to draw boundaries between legitimate and illegitimate uses of vulnerabilities.

6.1 Part One: Using disclosure to draw boundaries

In April 2014, security researchers discovered a critical flaw in the way that many websites send information, a flaw they named 'Heartbleed.' This 'vulnerability' in Open SSL, a protocol by which many websites handle the encrypted connection to a computer, meant that attackers could in theory trick vulnerable websites into leaking small packets of data that were residing on the internet server at the time, including usernames, passwords, credit card details or whatever was in the memory at the time. 'Vulnerabilities' in this context refer to undiscovered flaws in the software and hardware that make up cyberspace. Such flaws can be present in the systems from the day of their launch:

discovering all the potential bugs in the millions of lines of code in a piece of equipment or software is time-consuming and not always economically induced for the vendors. Vulnerabilities arise and embody what Chun (2008, p. 300) has called the "vicissitudes of execution" which emerge as code, interfaces, and users interact and behave unexpectedly and unpredictably, resulting in bugs or 'vulnerabilities'[10]. When 'vulnerabilities' are unknown to the vendor or manufacturer, they are often referred to as 'zero-day vulnerabilities,' or '0-days,' because developers have had zero days to address and patch the vulnerability. Such bugs in coding and technical configurations can sometimes be intentionally exploited through research and the development of specifically tailored code ('exploits'). Heartbleed was a major concern for security researchers because there was the possibility that this flaw could be used to steal the encryption keys that websites use to encrypt traffic, so that attackers could potentially decrypt this data or impersonate legitimate websites as a way to trick users into inputting their login details (Zetter, 2014b). One cryptographer and computer security professor at the University of Pennsylvania described it as "the worst and most widespread vulnerability in SSL [cryptographic technology] that has come out," (Blaze, cited in Zetter, 2014a n.p)

By 2014, wider concerns that the NSA were actively trying to 'break widely used internet encryption' informed criticism of the US government from diverse commentators, who cast doubts on how federal and state agencies professed to use and weigh the risk posed by such capabilities. When Bloomberg News published a now-disputed story later that month alleging that the NSA had known about and exploited this vulnerability in widely used website encryption technologies, such suspicions about the NSA were informed by documents dating from 2010 and released in 2013 by Edward Snowden, the former NSA contractor, that described a program called 'Bullrun.' One GCHQ document related to this program suggested that for "…the past decade, NSA has lead [sic] an aggressive, multi-pronged effort to break widely used internet encryption technologies" and that as a result, "…[v]ast amounts of encrypted internet data which have up till now been discarded are now exploitable." (cited in Ball, Borger and Greenwald, 2013 n.p.). The National Security Council issued a statement that such claims were outright "wrong" and that "the federal government was not aware" of the vulnerability until it was publicised in the news (Caitlin Hayden, cited in Sanger and Perlroth, 2014 n.p). However, as the Electronic Frontier Foundation argued, the issue was that "…[s]ince these vulnerabilities potentially affect the security of users all over the world, the public has a strong interest in knowing how these agencies are weighing the risks and benefits of using zero days instead of disclosing them to vendors," (Crocker and Galperin, 2014 n.p). Heartbleed would thus prompt commentators from the

[10] "A bug is when a system isn't behaving as it's designed to behave. A vulnerability is a way of abusing the system (most commonly in a security-related way) - whether that's due to a design fault or an implementation fault. In other words, something can have a vulnerability due to a defective design, even if the implementation of that design is perfect" https://stackoverflow.com/questions/402936/bugs-versus-vulnerabilities

media, security community, policy experts and civil rights activists to challenge how the government regulated its hacking capabilities.

The government wanted to preserve their ability to use vulnerabilities, despite allegations that government agencies were undermining their own "commitment to an open and interoperable, secure and reliable Internet" (Daniel, 2014 n.p.) by withholding information about vulnerabilities rather than disclosing them. From 2014 onwards, government representatives would release details of an internal interagency deliberation procedure called the Vulnerabilities Equities Process, or 'VEP' (discussed in more detail in Part Three of this chapter). Details of the existence and parameters of the procedure's justifications were articulated in terms of 'transparency' and 'accountability:' Michael Daniel reflected these motives in his explanation for the need to disclose details of the interagency process: "…[t]oo little transparency and citizens can lose faith in their government and institutions, while exposing too much can make it impossible to collect the intelligence we need to protect the nation." (Daniel, 2014).

For government actors, the purpose of working *for*, or of drawing boundaries between intelligence, national security and cybersecurity was to protect the autonomy of federal government agencies. Edward Snowden's revelations had "opened up a big can of worms about what the government's role is," and this role was "already a big open question in cyberspace," (Bruce McConnell, Department of Homeland Security's Acting Deputy Undersecretary for Cybersecurity, cited in Selyukh, 2013). Such questions would again be raised by critics of the government's institutionalised use of vulnerabilities following the events of May 2017, when a piece of ransomware called WannaCry gained access and spread through systems across the world using a variant of an 'exploit' called EternalBlue. This exploit was designed by the NSA to take advantage of a vulnerability they had discovered in Windows-powered computer systems (Monte, 2015, p. 171). However, the exploit's subsequent repurposing and use as a part of WannaCry was the result of a leak of that classified tool, a leak that facilitated an "unprecedented" global cyber incident (EUROPOL, 2017). These events triggered a vociferous public debate that centred around whether the government retained or disclosed vulnerabilities.

As the next section will show, Heartbleed and subsequent debates about the VEP would therefore become a shorthand, a locus, for wider debates about the government's vision of insecurity and how that demarcated their role in cybersecurity, and this would trigger government actors to use competitive strategies where 'disclosure' was invoked to work *for* boundaries between legitimate and illegitimate uses of vulnerabilities.

6.1.2 Federal imaginaries of cyber (in)security

In response to Heartbleed and WannaCry, government representatives over the course of two administrations would use 'disclosure' to articulate a vision of insecurity in which the use of vulnerabilities was in the name of 'national security' and would not undermine broader conceptualisations of 'cybersecurity.' In 2014, the White House Cybersecurity Co-ordinator Michael Daniel took the unusual step of publishing a blog post to address the allegations. He set out the stakes of government involvement in exploiting vulnerabilities by articulating a boundary between the government's institutionalised use of such vulnerabilities and their use by adversaries. On the one hand, he argued that such vulnerabilities could be used as tools "…to collect crucial intelligence that could thwart a terrorist attack, stop the theft of our nation's intellectual property, or even discover more dangerous vulnerabilities that are being used by hackers or other adversaries to exploit our networks" (Daniel, 2014 n.p.). Vulnerabilities in the hands of 'hackers or other adversaries' were thus 'more dangerous vulnerabilities' than the ones being used by the government. On the other hand, he recognised that retaining "a huge stockpile of undisclosed vulnerabilities" would leave the "Internet vulnerable and the American people unprotected" (Daniel, 2014 n.p.). This was one of the most explicit acknowledgements that the government had made to date of its institutionalised uses of vulnerabilities during its lawful intelligence and law enforcement activities. While hyperbolic, by describing the whole internet as being vulnerable, and making references to 'stockpiles,' Daniel was working to invoke historically resonant conceptions of the state's role as security provider. According to this logic, the government was historically responsible for protecting the American people, and managing vulnerabilities was to be an important component in that role. By articulating their 'traditional' roles in this way, the administration was working *for* boundaries to make political space for their preferred courses of action and direct resources to those ends – as we will see in Part Three.

Government actors would also use disclosure to draw boundaries between national security and cybersecurity in other ways too. Although "responsibly disclosing a newly discovered vulnerability is clearly in the national interest", Daniel highlighted how instrumental "this tool [was] as a way to conduct intelligence collection, and better protect our country in the long-run" (Daniel, 2014 n.p.). By invoking national security prerogatives, the implication here was that though 'some' might disagree, the government were working to demarcate the legitimacy of using such vulnerabilities during their intelligence and law enforcement activities. Hailing the use of vulnerabilities by Federal agencies as like "so many national security issues," Daniel was conveying how they thought that this was a matter that the government had unique normative authority to act as an adjudicator for, suggesting that while "the answer may seem clear to some", the "reality is much more complicated" (Daniel, 2014 n.p.).

The administration thus drew a boundary between two positions: on the one hand was the government's commitment to the security of cyberspace more broadly – cybersecurity – and on the other were their national security prerogatives. Here, there was to be a "trade-off" (Daniel, 2014 n.p.) between 'disclosure' of vulnerabilities and 'national security' missions. Echoing Michael Daniel's depiction of the 'trade-off' between cybersecurity and national security, Daniel's successor in the role of White House Cybersecurity Coordinator, Rob Joyce, published a 2017 blog post that made the government's rationales for *limiting* disclosure explicit:

> Our adversaries, both criminal and nation state, are unencumbered by concerns about transparency and responsible disclosure and will certainly not end their own programs to discover and exploit vulnerabilities. Although I don't believe withholding all vulnerabilities for operations is a responsible position, we see many nations choose it. I also know of no nation that has chosen to disclose every vulnerability it discovers. (Joyce, 2017)

Despite the government's commitment "to promote resilience in the digital systems architecture" (Joyce, 2017 n.p), immediate or total disclosure was thus argued to be at the expense of pursuing adversaries who were unencumbered by such limitations. Joyce, like Daniel in the Administration before him, was here setting the parameters of disclosure in normatively laden and historically resonant terms of 'transparency' and 'responsibility,' so that 'national security' was hailed as setting limits on requirements for limited and 'responsible disclosure,' even if it was in the name of cybersecurity.

For government actors involved in defending the use of vulnerabilities, claims to 'national security' such as those above were often a productive rhetorical strategy to underline the legitimacy both of their actions and themselves. Like claims to being 'scientific' are part of efforts to defend epistemic authority and legitimacy (Gieryn, 1999), claims to security are invoked to confer political and normative authority. However, as we shall see in the next section, in the case of cybersecurity the sources and criteria for this authority were contested, and 'disclosure' operated as a site to contest these criteria.

6.2 Part Two: Dissenting imaginaries of cybersecurity and disclosure

For commentators challenging the government's use of vulnerabilities and the security imaginary that rationalised their use, disclosure was used as a symbolic resource to contest boundaries that the government had drawn to legitimate their use. These were fundamentally opposing visions of what 'cybersecurity' *meant*, what it *is* – whether it meant to patch, or to spy, based on either a technical conception of cybersecurity to secure cyberspace by fixing vulnerabilities, or on a political

conception of cybersecurity to secure cyberspace by utilising vulnerabilities for wider strategic ends (Nissenbaum, 2005). Here, disclosure was used to differentiate and work *for* boundaries between technical and political conceptions of cybersecurity.

6.2.1 'Technical' imaginaries of cybersecurity

For those self-described in the technical community concerned about the government's exploitation of vulnerabilities in widely used systems, disclosure for patching was meant to be a constitutive part of 'cybersecurity.' Through competitive boundary work strategies, they would mobilise these boundaries to proffer a different solution to that of the government. In a report that was intended to offer policy recommendations to help the US government weigh "the security value of disclosure versus the benefit of stockpiling and using vulnerabilities," one Washington think tank report by *New America* described how,

> *[m]uch* of *cybersecurity can be reduced to* a constant race between the software developers and security experts trying to discover and patch vulnerabilities, and the attackers seeking to uncover and exploit those vulnerabilities. (Wilson *et al.*, 2016, p. 2, emphasis added)

That cybersecurity could be characterised as such a patch-or-exploit dynamic is indicative of the way that many software developers and security experts viewed the role of disclosure in facilitating security. The centrality of patching for cybersecurity articulated here was echoing a perspective found across the privacy and information security community. As one prominent security expert in this debate, Bruce Schneier, had described the role of disclosure in 2012, "regardless of the motivations," the role of disclosure was to facilitate patching (Schneier, 2012, n.p). This was because it was an important constituent to security more broadly: "…a disclosed vulnerability is one that -- at least in most cases -- is patched. And a patched vulnerability makes us all more secure." (Schneier, 2012, n.p). It was therefore on the grounds of disclosure's role that in 2012 the civil liberties non-profit group the Electronic Frontier Foundation (EFF) questioned the government's commitment to cybersecurity more broadly, stating that,

> If the U.S. government is serious about securing the Internet, any bill, directive, or policy related to cybersecurity should work toward ensuring that vulnerabilities are fixed, and explicitly disallow any clandestine operations within the government that do not further this goal. (Hofmann and Timm, 2012 n.p)

In other words, the EFF was arguing that fixing vulnerabilities would be a key indicator of the government's commitment to cybersecurity. As Bruce Schneier later summarised, "[p]retty much uniformly, security experts believe we ought to disclose and fix vulnerabilities." (Schneier, 2016 n.p). By invoking a consensus of 'we' amongst this technical community, and citing the expertise of this

community of security professionals, Schneier was constructing boundaries around disclosure on the basis of the credentials of the 'experts' on the one hand, disputing the government's credentials on the other. As far as this security, privacy and policy advice community were concerned, they were arguing that the use of vulnerabilities for clandestine operations by government agencies would undermine the credibility and capability of the government's broader cybersecurity efforts, because 'disclosure' was synonymous with 'security.'

The administration had used disclosure in a different way to draw boundaries around the use of vulnerabilities. As illustrated in the earlier discussion, Daniel and Joyce had each acknowledged the importance of disclosure for ensuring cybersecurity of the nation whilst simultaneously arguing that such disclosures had *limits*. Here, immediate disclosure was equivalent to disarmament:

> The Federal Government […] has an important responsibility to closely guard and protect vulnerabilities as carefully as our military services protect the traditional weapons retained to fight our nation's wars. Some argue that every vulnerability should be immediately disclosed to the vendor and patched. In my view, this is tantamount to unilateral disarmament. (Joyce, 2017 n.p)

This language sought to make an equivalence clear between 'traditional weapons' and vulnerabilities and served to invoke long-standing ideas of what counts as a matter of national security (weapons and capabilities) and who was responsible for keeping those secrets (Federal agencies). According to this logic, disclosing vulnerabilities immediately would put the United States at a disadvantage akin to forgoing conventional weaponry, a disadvantage that "adversaries […] are unencumbered" by (Joyce, 2017 n.p). Here, Joyce was hailing the arguments from "some" in the community of security experts and policy advisers that had questioned the government's articulation of the role that disclosure played in matters of national security. By drawing links with conventional weaponry as Joyce did, he sought to make the implication that those outside government were not qualified to make such judgements, thereby outlining a form of 'limited disclosure' instead of 'full disclosure.'

Technology companies also used this analogy to conventional weapons, but to articulate an opposing position. Technologist Bruce Schneier had argued that "[f]ixing vulnerabilities isn't disarmament; it's making our own countries much safer." (Schneier, 2014 n.p). Likewise, in the wake of WannaCry, Microsoft President Brad Smith wrote a post on the company's website that highlighted what he saw as the dangers for cybersecurity that governments keeping secrets posed:

> The governments of the world […] need to take a different approach and adhere in cyberspace to the same rules applied to weapons in the physical world. We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these

> exploits. This is one reason we called in February for a new "Digital Geneva Convention" to govern these issues, including a new requirement for governments to report vulnerabilities to vendors, rather than stockpile, sell, or exploit them. (Smith, 2017 n.p).

In seeking to apportion blame elsewhere for the attacks that targeted their software after WannaCry, in this post the head of Microsoft wanted to contest the government's rationales for limited disclosure. In both cases here, cybersecurity was instead premised on a more 'technical' and practitioner-based conceptualisation of cybersecurity predicated on ensuring the confidentiality, integrity and accessibility of data. According to this 'technical' conceptualisation of cybersecurity, government operations that utilised vulnerabilities fundamentally undermined the security of cyberspace. In this dissenting security imaginary then, government agencies were the source of insecurity, not the vulnerabilities themselves, so that advocates of this alternative imaginary would challenge the sources and the criteria of the authority conferred by the administration's claims to 'national security,' as the next section will now show.

6.2.2 Disclosure to contest boundaries of national security

For those challenging the government's articulation of the boundaries between national security and cybersecurity, disclosure played a different role. In 2013, a report generated by the President's Review Group on Intelligence and Communications Technologies, convened post-Snowden and before the fallout from Heartbleed, questioned the government's approach to withholding information on zero-day vulnerabilities. Their reading of the matter was that "…NSA, DHS, and other agencies should identify vulnerabilities in software widely employed in critical infrastructure and then work to eliminate those vulnerabilities *as quickly as possible*." (Clarke *et al.*, 2013, p. 219, emphasis added). Withholding vulnerabilities, even for a short time, therefore risked undermining "that duty to defend", and that it was "…in almost all instances […] in the national interest to eliminate software vulnerabilities rather than use them for US intelligence collection." (Clarke *et al.*, 2013, p. 220). More than playing a small role, disclosure was thus described as a constitutive part of the government's defensive *duty* to ensure cybersecurity, here broadly conceived as the security of cyberspace. Patching had a key role in this conceptualisation of security: "…[e]liminating the vulnerabilities—"patching" them— strengthens the security of US Government, critical infrastructure, and other computer systems." In other words, contrary to how Daniel and Joyce would later articulate its limits, the role of disclosure was to facilitate patching that would contribute to the security of whole systems.

For security and privacy advocates, boundaries could not be drawn so clearly between 'cybersecurity' and broader 'national security' as the government was signifying. For them, Heartbleed

and WannaCry had highlighted how governmental discovery and use of vulnerabilities in widely used technologies was a distinctive challenge compared to conventional weaponry. Here, segregating and compartmentalising the use of vulnerabilities separately from the broader internet ecosystem was not such a clear equivalence. According to Bruce Schneier,

> There is no way to simultaneously defend US networks while leaving foreign networks open to attack. Everyone uses the same software, so fixing us means fixing them, and leaving them vulnerable means leaving us vulnerable. (Schneier, 2014 n.p.)

Like Schneier, and in an echo of boundary work in Chapters Three and Four at distinctions between 'offense' and 'defense' in cyberspace, Harvard Law Professor Jack Goldsmith also reflected on the difficulty of segregating and compartmentalising the use of vulnerabilities when he observed that "every offensive weapon is a (potential) chink in our defense - and vice versa." Similarly, in response to WannaCry and Joyce's blog posts, a former principal technologist at the American Civil Liberties Union was reported as highlighting the risks that all users endure from unpatched vulnerabilities given that, "…[w]e all use the same technology. We all use the same laptops, we all use the same web browsers, we all use the same word processing programs." (Soghoian, cited in Hopper and Waldman, 2017 n.p). These observations were not restricted to those outside of government: as the ranking Democrat on the House Intelligence Committee pointed out in the context of the NSA's use of vulnerabilities, cybersecurity was particularly challenging because "…[w]hen it comes to cyber in particular, the line between collection capabilities and our own vulnerabilities … is virtually non-existent" (Schiff, cited in Nakashima, 2016 n.p.). The challenge posed by government computer network operations was that they take advantage of software and hardware vulnerabilities that domestic civilians and organisations may also use: Schiff's (and Microsoft's earlier) argument was that government actors cannot so easily segregate or compartmentalise their actions as they might in other classified contexts. Statements such as these were each challenging the sources and criteria of the authority conferred by the Administration's claims to 'national security'. They challenged the argument Federal government agencies were uniquely qualified to manage the knowledge of these vulnerabilities as though they had direct equivalence with conventional weaponry and 'other matters of national security.' In this reading, government agency uses of zero-day vulnerabilities were not so easy to segregate from the security interests of wider technology users, and as the next section will show, this also led critics to undertake boundary work that challenged the government's political and epistemic authority.

6.2.3 Disclosure to contest categories and classification

As well as contesting the government's rationales for disclosure, commentators would also invoke boundaries of disclosure to challenge the credibility and competency of government agencies. For advocates outside of the government who were contesting official rationales for limited disclosure, the government's desire to control and categorise vulnerabilities and exploits as controllable information was not something that could be guaranteed, citing the distinctive characteristics of the operating environment. For the director of New America's Open Technology Institute, WannaCry had demonstrated:

> …the key risk of the U.S. government stockpiling computer vulnerabilities for its own use: Someone else might get a hold of them and use them against us. This is exactly why it should be U.S. government policy to disclose to software vendors the vulnerabilities it buys or discovers as soon as possible, so we can all better protect our own cybersecurity. (Bankston, cited in Nakashima and Peterson, 2016 n.p.)

By questioning the ability of government agencies to control classified information, members of the computer security community were thus questioning the government's credibility more broadly for ensuring 'our' cybersecurity. A representative of the Electronic Frontier Foundation also expressed concerns about the unique risks that limited disclosure in this context posed, suggesting that:

> …[w]hen governments acquire [vulnerabilities] they take a gamble that no one else is going to find out about them or that they won't be stolen or leaked. Now I'm not saying that they should never retain vulnerabilities in the first place, but that that's a risk that has to be understood. (Crocker, cited in Sternstein, 2017 n.p.)

Even when acknowledging that vulnerabilities may be retained according to the government's rationales, WannaCry and a series of other breaches and leaks of classified information meant that government agencies' ability to control and compartmentalise vulnerabilities had become a matter of contention in defending the credibility of their imaginaries for cybersecurity. For technology companies such as Microsoft, this was "an emerging pattern in 2017", where repeatedly, "…exploits in the hands of governments have leaked into the public domain and caused widespread damage" (Smith, 2017). Even the former senior director for cybersecurity at the National Security Council admitted that:

> …[i]n the current environment, government-held vulnerabilities are going to leak. Governments should not expect that they can hold on to vulnerabilities as long as they used to and we have to come up with coping mechanisms for it. (Schwartz, cited in Carberry, 2017)

At the heart of many similar such articulations of 'the current environment' was an essentialised view of vulnerabilities' characteristics, that they were something that could be 'held on to' and that the government could have a unique (if temporary) hold of. As Part Three will shortly demonstrate though, conceptualising vulnerabilities in such terms would shape the imaginary that directed the development of the VEP in important ways.

Those in the 'technical community' would contest the government's account as a way to challenge the credibility of their claims that the federal agencies could manage such information, arguing that such an approach belied a technically illiterate understanding of vulnerabilities as something that could 'held on to.' As one former NSA hacker described the matter,

> …it is obvious to the technical community (although not to lawyers and policy makers) that 0days are not a simple commodity like grain or oil, but often are highly correlated, composed of smaller parts and techniques, and *uniquely non-fungible***.** (Aitel, 2016 n.p., emphasis added)

In distinction to those outside this self-described community, such as lawyers and policy makers, to this 'technical community' in the know, such non-fungible and hard-to-categorise matters meant that the VEP could only bound vulnerabilities and 'disclosure' in limited ways. Claims to expertise in the operational complexities of vulnerabilities would thus be used to challenge both how government actors such as Daniel and Joyce categorised vulnerabilities as well and government efforts to quantify the risks posed by them. As the rest of the chapter will set out, vulnerabilities are not simply technical or external structural imperatives, but are a product of an interplay of technical, social and political efforts, made intelligible through strategic practical action such as the VEP.

6.3 Part Three: Constituting disclosure and actualising imaginaries of cybersecurity

The VEP was a procedural effort on the part of the US government to formalise the parameters within which government agencies could utilise vulnerabilities for offensive purposes. Although its development was classified, the initial establishment of the VEP-as-procedure began in 2008. Details of this policy have since been released in redacted form and show that the government was concerned about managing communication across so many different state agencies, each with different and sometimes competing mission interests, or equities, in the discovery and use of vulnerabilities. According to the working group tasked with developing the procedure between 2008-9, "proper coordination" was a distinctive challenge for "cybersecurity activities" because these could "…take many forms: defense (CND), offense (CNA), investigation (CNI), as well as counterintelligence (CI)." (Office of the Director of National Intelligence, 2014, p. 12). There was therefore a perceived need for a new procedure to address these distinctive challenges: in such an expansive reading of

"cybersecurity activities" where such diverse offense, defense and intelligence "activities are all linked," there was an imperative to make so many cybersecurity equities more easily amenable to categorisation and coordination. According to the document intended to formalise this new interagency process in 2010, the discovery of vulnerabilities "…may present competing equities for [government] offensive and defensive mission interests" and went on to recommend that "…actions taken in response to knowledge of a specific vulnerability must be coordinated to ensure the needs of each of these 'equities' are addressed" (VEP, 2010, p. 1). A process was therefore needed to 'balance' the competing interests of federal agencies in cybersecurity.

As each section of the reminder of the chapter will now lay out in turn, by making claims to being rational, unbiased and deliberative, the VEP worked to set the procedural and political parameters of disclosure, with the goal of protecting the autonomy of government agencies to use vulnerabilities. The VEP can thus be understood as procedural and practical work that has constituted more expansive, but also more flexible, bounds of disclosure as a spectrum, rather than a binary state. It has been an embodiment, a concretisation, of competitive boundary work for boundaries as a mechanism for state agencies to preserve their operational autonomy. But like the other chapters so far, this shows another instance in which official imaginaries of cybersecurity have been iterative and processual rather than overdetermined by structural or strategic 'imperatives.'

6.3.1 Disclosure as deliberative

The VEP was designed as an interagency process to weigh up the risks against the benefits associated with government agencies discovering vulnerabilities in widely-used technologies and the decision to keep them secret or to disclose them to manufactures to be fixed. The VEP thus set the parameters for the debate amongst multiple government departments internally and externally negotiating their competing mission interests, or 'equities'. Facilitating the process, the 'National Security Agency/Information Assurance Directorate' would serve as the Executive Secretariat, and they would document, host, and maintain the regular meetings. The 'Equities Review Board' was made up of representatives from several agencies who had submitted a vulnerability to the process or might have an interest in the vulnerability. The 'Points of Contact' were tasked with "ensuring the applicable … equities of their organization" were "appropriately represented in the process", which included cybersecurity, intelligence, counterintelligence and law enforcement equities amongst other listed mission interests (VEP, 2010, p. 5). Several agencies would have been involved in the process beyond the NSA, but aside from a redacted section describing the agencies involved, the unredacted agencies were described in more tentative terms in the 2010 policy document with the phrase "other participants may include" Departments of State, Justice, Homeland Security, Treasury, Commerce and

Energy. This procedure was designed to be "…a comprehensive common policy and systematic process for handling the problem across the USG." (VEP, 2010, p. 2). By hosting regular meetings, turning the complexity and organisational breadth of these competing interests into a formalised procedure was therefore meant to impose some boundaries on the problem of vulnerability use and set procedural parameters on who would be involved and when.

The procedure also set boundaries on disclosure by seeking to draw a symbolic as well as procedural line between dissemination and retention so that consensus was a simplified matter. To begin with, the purpose of the procedure was to build consensus amongst the range of government agencies. At this stage, the procedure was primarily concerned with setting parameters upon internal interagency deliberations, but a by-product of these negotiations was what they called the decision "…to disseminate information pertaining to the vulnerability" (VEP, 2010, p. 8). At this stage in the procedure's existence, disclosure was not its main focus. The procedure was instead more concerned with institutionalising a forum that would broaden deliberations to involve government agencies involved in vulnerability questions beyond the NSA. It was also to act as a formalised mechanism that would set the terms of those deliberations, and the 2010 VEP policy document spent the most time outlining those terms. The focus in the VEP policy was on procedural matters – who should attend, what kinds of clearances they must have, what the hierarchy of decisions were, the step-by-step process for electing vulnerabilities to the process, and the process for contesting decisions. In other words, deliberations were concerned first and foremost with assessing the internal equities of the different agencies and providing a platform for them to communicate information about vulnerabilities amongst themselves. With a procedural focus on classified and uniquely governmental knowledge of vulnerabilities, this procedure was oriented around when to communicate *within* the Federal government. As time passed though, and in response to the allegations (discussed in Parts One and Two) that the government's actions were making cyberspace less secure, the procedure would become more concerned with questions of when and why agencies should disseminate information to those *outside* the government.

As a result of the focus on setting the procedural and interagency bounds of vulnerability equity decisions, to begin with, the procedure established parameters of dissemination in binary terms. According to the official guidelines in the 2010 policy, the Equities Review Board would reach a decision to disseminate, or to not disseminate. To the extent that the policy document stipulated what the ERB should consider as dissemination, the document contained an appendix of terms, where 'external dissemination' (as opposed to dissemination amongst government agencies) was described as the "sharing or release of vulnerability information to entities external to the USG." (VEP, 2010, p. 12). Unlike later incarnations of the VEP, at this stage, there was no indication of temporary restrictions, or of a range of possible measures in between 'disclosure' or retention. Depending upon

the vulnerability in question, information about it would be disseminated to relevant 'cyber centres' tasked with incident response or defensive network security, according to the sector in question. Even the terms used – dissemination, rather than disclosure as would be used later[11] – suggested a cybernetic model of information transfer, of senders actively distributing information rather than passively uncovering it or it being in need of interpretation (Fenster, 2015; Stampnitzky, 2020). The redacted information in the policy document may have indicated a more detailed range of vulnerability dissemination options to those "external to the USG" (VEP, 2010, p. 2), but given that the sections that remained redacted after review by the Office of the Director of National Intelligence in 2015 and 2016 were based on the government's desire to withhold information about offensive capabilities rather than defensive equities and the procedural parameters of dissemination (Hudson, 2015, 2016; Electronic Frontier Foundation, 2016), a more nuanced account of dissemination options is unlikely to have been in the redactions of this document.

By the time that Daniel made the blogpost in 2014, the language he used indicated a shift in how the procedure was constituting disclosure. There was now a more nuanced expression of the bounds of 'disclosure.' In referencing this "…debate about whether the federal government should ever withhold knowledge of a computer vulnerability from the public" Daniel made reference to the *timing* of disclosure (Daniel, 2014 n.p) as a way of moderating the either-or position instituted in the early VEP-as-procedure. Describing the procedure itself as "…a disciplined, rigorous and high-level decision-making process for vulnerability disclosure", this interagency forum was concerned about when to "…*temporarily* withhold[..] knowledge of a vulnerability" and suggesting that there were "no hard and fast rules" for making these judgements (Daniel, 2014 n.d., emphasis added). While the *organisation* of the Equities Review Board was instituted and disciplined in a rigorous way, the vulnerabilities themselves were more loosely bound in this procedure. Disclosure could be temporarily delayed, and categorising the vulnerabilities was more done more flexibly than being subject to 'hard and fast rules.' Unlike the 2010 policy document, Daniel's 2014 blogpost also outlined the range of considerations that the review board subjected vulnerabilities to, including asking the question of whether they "… could … utilize the vulnerability for a short period of time before" it was disclosed (Daniel, 2014 n.p) – it could be temporarily exploited, and nor did disclosure prevent it from being exploited while patches were developed or as long as patches remained uninstalled on targeted

[11] According to Collins American English dictionary, "to disseminate information or knowledge means to distribute it so that it reaches many people or organizations"; to disclose means "to bring into view; uncover"; in insurance, "if you disclose information to an insurer, you provide information about a risk that may be relevant" – an interesting analogy given the VEP's later focus on categorising and quantifying risks posed by government discovery and uses of vulnerabilities.

systems (Hennessey, 2016). The procedure's rationale was now beginning to reflect a more expansive range of what constituted 'disclosure.'

By emphasising its deliberative attributes, Daniel accordingly described how the procedure functioned as a way of "instill[ing] some confidence" that the government was "acting responsibly" (Daniel, 2014 n.p). Though a lot of details remained out of bounds to the public, including the names of Federal agencies specifically involved, Daniel described how "the agencies that you would expect" used a "multi-factor test" to quantify the risks posed by vulnerabilities that government agencies had submitted to the VEP (Daniel, cited in Zetter, 2014c n.p). This was now to be "…a deliberate process that [was] biased toward responsibly disclosing the vulnerability," (Daniel, 2014 n.p). The bias towards disclosure was now built in, even if there were to be exceptions to this disclosure.

With each iteration of the VEP, 'disclosure' would become more wide-ranging in scope, with actors increasingly emphasising the fuzzy edges of what constituted 'disclosure.' By the time of Rob Joyce's blogposts in 2017 in response to the Shadow Brokers and WannaCry incidents, the VEP was enacting 'disclosure' as a *spectrum* of possible outcomes. Building on the VEP's broadening of 'disclosure' highlighted by Daniel in 2014, the spectrum that disclosure operated along was made explicit by the 2017 procedure, and it is worth quoting the 2017 Policy Charter at length:

> The U.S. Government's determination as to whether to disseminate or restrict a vulnerability *is only one element* of the vulnerability equities evaluation process and is *not always a binary determination***.** Other options that can be considered include disseminating mitigation information to certain entities without disclosing the particular vulnerability, limiting use of the vulnerability by the USG in some way, informing U.S. and allied government entities of the vulnerability at a classified level, and using indirect means to inform the vendor of the vulnerability. All of these determinations must be informed by the understanding of risks of dissemination, the potential benefits of government use of the vulnerabilities, and the risks and benefits of *all options in between***.** (VEP Charter, 2017, p. 1, emphasis added)

Pointing to a more complex range of disclosure 'options' in this way was working to 'fuzz' or downplay its boundaries. The publication of this unclassified VEP Charter was the most detailed account of the VEP's functioning to date, indicating that the public controversy discussed in Part One had not been settled by official statements during the Obama Administration and was further aggravated by high profile incidents like WannaCry. Here, the VEP Charter was releasing more details of the procedure's range of considerations, and underscoring 'disclosure' as a spectrum meant that reaching unconditional limits or thresholds was not the goal. As a former deputy director of the National Security Agency Rick Ledgett wrote in a personal op-ed following WannaCry, disclosure and patching were not a panacea:

> …WannaCry […] exploited flaws in software that had either been corrected or superseded, on networks that had not been patched or updated, by actors operating illegally. The idea that these problems would be solved by the U.S. government disclosing any vulnerabilities in its possession is at best naive and at worst dangerous. (Ledgett, 2017 n.p)

While this was a confrontational articulation of the possible bounds of disclosure and its role in cybersecurity, instituting a spectrum of disclosure was in support of this general sense that it was not a binary state or an unmediated good. This meant that government actors would be less likely to 'fail' in reaching publicly acceptable thresholds for disclosure, that they would be less likely to face criticism, if the VEP had already established that those thresholds were contingent or mutable. Whilst the VEP had set parameters on disclosure by drawing different agencies together and making it a deliberative procedure rather than a distributed and 'messy' problem, it had also expanded disclosure's possible permutations.

6.3.2 Disclosure as rational

In contrast to the 2010 procedure, the way that 'disclosure' was constituted by the VEP following Heartbleed in 2014 was beginning to shift. Rather than a procedural focus on when to disseminate knowledge of vulnerabilities amongst government agencies, the shift in approach was now specifically orienting the VEP around 'disclosure.' The whole of Daniel's 2014 blogpost was describing the VEP in terms of its focus on when to disclose vulnerabilities to those outside the government. Repeatedly, government officials would emphasise that the VEP was weighted towards disclosure, on disclosure as the norm rather than the exception. As the head of NSA had described the process within the VEP, "…by orders of magnitude, the greatest numbers of vulnerabilities we find, we share." (Rogers, 2014 n.p). This phrasing was echoed by Daniel in an interview, who stated that the procedure was working on the assumption that "…the overwhelming majority of those that we find we do disclose. The idea that we have these vast stockpiles of vulnerabilities stored up—you know, Raiders of the Lost Ark style—is just not accurate." (Daniel, cited in Zetter, 2014c n.p). The implication here was that the VEP was not designed to withhold information on vulnerabilities (or metaphorically store vulnerabilities like stacks of mysterious crates) but was an institutionalised and 'rigorous' manifestation of 'disclosure' in action.

Despite the VEP working to concretise disclosure practices as a spectrum, rather than an either-or, and thus broadening the boundaries of 'disclosure' in political terms, in other ways it was institutionalising a set of categorical parameters. Specifically, it did this by demarcating "repeatable methodologies" for quantifying risk:

> To the extent possible and practical, determinations to disclose or restrict will be based on repeatable techniques or methodologies that enable benefits and risks to be objectively evaluated by VEP participants. This process employs techniques that include assessment factors such as prevalence, reliance, and severity (VEP Charter, 2017, p. 7)

Categorising risk was to be a formative element of the VEP: "understanding risk was critical" to "ensure an equitable review of vulnerability information," and that the VEP did so by making "consistent, informed determinations" (VEP Charter, 2017, p. 8). All of the 'equity considerations' listed in Annex A of the 2017 VEP Charter document are a long form attempt to assess 'likelihood', 'impact' and 'harm', measures traditionally associated with risk assessments (VEP Charter, 2017, pp. 13–14). In other words, "…[d]efense risk equations […] account for a threat multiplied by one's vulnerability to that threat multiplied, in turn, by the consequences of that threat's exploitation." (Hennessey, 2016 n.p). As the former legal counsel to the NSA, Hennessey was here articulating the NSA's rationale for deciding on the risks posed by vulnerabilities. The implication here was that if they could be quantified and rationalised, then vulnerabilities could be made amenable to clear methodologies that in turn set parameters on their disclosure. On technical grounds, given the 'non-fungible' characteristics of vulnerabilities and exploits discussed earlier, attempts to develop 'repeatable techniques and methodologies' reflected a rationalist desire to impose prescriptive models of risks and their relationship to people (Wynne, 1996, p. 57). The VEP was a manifestation of this desire to quantify and therefore regularise or standardise the decision to disclose.

Over the course of its development, the VEP would make its methodological and rational parameters more explicit. The 2010 VEP contained tacit criteria for the Equities Review Board to make its determinations based on determinations of its subject matter experts of what their respective agencies' interests would be. Despite the VEP having been established as a procedure in 2010, it emerged that it "…had not been implemented to the full degree that it should have been," with the result that the administration had "…re-invigorated our efforts to implement existing policy with respect to disclosing vulnerabilities," (Daniel, cited in Zetter, 2014c n.p). Earlier incarnations of the VEP had set bounds too constrictively upon disclosure as a binary state, and while the VEP had been instigated, not all the agencies were communicating as consistently or in as coordinated a fashion as the policy called for (Daniel, cited in Zetter, 2014c n.p). This 'reinvigorated' 2014 VEP made these criteria and methods more explicit, and Daniel used the blogpost to draw out some of the questions and interests that the Equities Review Board would consider to make its determination (Daniel, 2014). The VEP thus made parameters of disclosure more explicit by incorporating more questions and more explicit thresholds for disclosure over time, whilst also broadening disclosure's parameters by expanding its possible permutations along a spectrum.

6.3.3 Disclosure as unbiased, free of interagency politics

Another attribute that the VEP sought to institutionalise into governmental disclosure practices was a putative freedom from inter-agency politics and agency bias. In order to articulate its independence from parochial agency interests, each iteration of the VEP therefore outlined a clearer set of leadership structures. The 2010 policy initially made this ambition clear when it stated that while the NSA was to act as the Executive Secretariat for the procedure, this function was to be "executed so as to remain neutral and independent of the organization's equities in any particular case."(VEP, 2010, p. 7). This duty would be housed within the NSA's 'Information Assurance Directorate' (IAD). As the defensively-oriented segment of the agency at that time, the IAD's designation as the home for these decisions (as opposed to the intelligence-oriented Signals Intelligence Directorate) was the result of both organisational inertia and a desire to allay the concerns of civilian federal agency bodies. Since the 1990's, the IAD already had its own internal process for weighing whether to withhold or disclose vulnerabilities and so their acting as the VEP's Executive Secretariat would have been the easiest organisational option, in effect grafting the formalisation of the 'VEP procedure' onto extant processes. Meanwhile, as we saw in the debates in Chapter Four in which representatives of DHS had lamented the unequal funding and resources of the NSA dominating the DHS's nascent cybersecurity efforts, the defensively-minded IAD would have been a more palatable process leader for these non-intelligence agencies.

However, the 2013 President's Review Panel would question the impartiality of the NSA's role in decision-making about vulnerability disclosures. In one of their recommendations to the President, they were the first unclassified report to outline the need for a formalised process to adjudicate the government's use of vulnerabilities. They also argued that there was an inherent conflict between the NSA's two missions of gathering intelligence and protecting cybersecurity, where the "…SIGINT [signals intelligence] function and the information assurance function conflict more fundamentally than before." (The President's Review Group on Intelligence and Communications Technologies, 2013, p. 185). As a result, they recommended that the White House should have an oversight role in the process rather than the NSA, implying in their report that the intelligence community had been the sole arbiter of decisions about the use or disclosure of vulnerabilities to that point. This meant that in the 2014 iteration of the VEP, Daniel would confirm that the National Security Council oversaw the process, in an effort to underscore the impartiality of the process (Zetter, 2014c). By expanding the range of government agencies involved in the process, and by shifting the locus away from the NSA, the VEP was thus working to produce a decision-making process that was intended to be biased in favour of disclosure, rather than biased by agency interests.

The WannaCry incident in 2017 would again trigger administration officials to further advocate for the VEP's putatively impartial features. This was due in large part to Congressional lawmakers introducing a bicameral and bipartisan bill in Congress called the Protecting our Ability To Counter Hacking (PATCH) Act. The PATCH Act was described as intending to add "transparency and accountability to the U.S. government process for retaining or disclosing vulnerabilities" because the government's current decision-making process was "…opaque, unaccountable to Congress, and unestablished in law or Executive Order", and this was something that undermined "…trust with the American people and private sector and potentially jeopardize[d] our nation's cybersecurity." (Johnson, 2017 n.p) The decision to disclose was about nothing less the trust of the American people and the nation's cybersecurity, illustrating the extent to which wider debates (discussed in Part One) were shaping the conceptual and political importance of 'disclosure' for constituting cybersecurity.

Despite the Obama administration's claims to the VEP's objectivity, Congressional and thinktank pressure to codify the VEP into law would be suffused with assumptions about law's capability to make the procedure more formalised and therefore more objective. For a former Director for Cybersecurity Policy at the White House National Security Council, moving "…from what is an interagency agreement to substantiate VEP into law" would be an important step for improving accountability, given that there were "no penalties for individuals to hold back information" from the VEP (Knake, cited in Spring, 2017 n.p.). A desire to impose a "legal framework around this process" indicated the extent to which speakers outside of the government felt there was still too much ambiguity around what constituted disclosure (Knake, cited in Spring, 2017 n.p.). Putting legal parameters upon the VEP was intended to codify and regularise the process and was presumed to add an extra layer of rigour and impartiality. As a case in point, the statements in support of the PATCH Act from the Open Technology Institute described how legislation like the PATCH Act was "crucial in establishing confidence and trust" in the VEP process and "…would codify what the White House claims it has had all along: a rigorous process" (Bankston and Wilson, 2017 n.p.). Putting legal parameters on disclosure was intended to impose a framework, or set the bounds, of government disclosure practices. While the PATCH Act failed to progress beyond first reading, Congressional efforts to regulate the government's uses of vulnerabilities and to legally constitute their own readings of disclosure in its importance for ensuring national cybersecurity led the White House to release the VEP Charter later that year.

Institutionalising the bounds of 'disclosure' through law as advocated by Congress and civil society was a step too far for those in the intelligence community. The 2017 VEP Charter was therefore an effort to preserve the autonomy of federal agencies to arbitrate their use, independently of this kind of external interference. Building on the reorientation of the VEP outlined by Daniel in 2014, the VEP shifted the emphasis in leadership of the process from the NSA as in 2010, to an increased role

for a 'VEP Director' based within the National Security Council, overseeing the NSA's role as Executive Secretariat (VEP Charter, 2017, p. 4). The 2017 Charter even echoed the phrasing of the 2010 document when it stated that "Executive Secretariat function will be executed so as to remain neutral and independent" (VEP Charter, 2017, p. 4). The 2017 VEP and its associated public statements were intended to head off Congressional efforts at regulation and law, with the aim of preserving the autonomy of these agencies to make their own deliberations. In this sense, the VEP was intended to grant government agencies more latitude in the decision-making process, as legal requirements would have enforced oversight and reporting commitments.

While keeping the VEP from being regulated in law was an important element in enabling the Executive Secretariat more latitude and freedom in deciding the bounds of disclosure, at the same time the VEP would also work to set limits upon disclosure's scope. Unlike the 2010 VEP policy that was so oriented around establishing interagency lines of communication, the 2017 Charter consistently articulated its rationale in terms of external interests. Thus, the 2017 incarnation of the VEP signified an even more explicit shift of disclosure in the name of 'public interests.' Accordingly, the 2017 described "the primary focus of this policy" being to:

> …prioritize the public's interest in cybersecurity and to protect core Internet infrastructure … absent a demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes. (VEP Charter, 2017, p. 1)

Demarcating between 'national security' and 'the public's interest in cybersecurity' was thus intended to set procedural and political limits upon the role of disclosure in constituting 'cybersecurity.' In other words, by making these distinctions, the VEP Charter was setting limits on how far and how much disclosure would produce cybersecurity, in effect setting limits on cybersecurity's otherwise all-encompassing scope (such as in the thesis' Chapters so far). Joyce made such a distinction explicit when he rationalised that:

> What we're trying to carefully weigh is having those capabilities, to be able to use them for national security, while at the same time making sure that it's not a major liability for our economy, for the international community, for our national security." (Joyce, cited in Bing, 2017 n.p)

Disclosure was important for cybersecurity, but there would be limits to its scope in the name of 'our national security.' By emphasising the independence of the procedure from parochial agency interests, and repeatedly invoking ideals of transparency and accountability by describing the policy's 'primary focus' as institutionalising into policy deliberations the public's interest in cybersecurity, the VEP was working to constitute 'disclosure' in ways that would maintain the autonomy of federal

agencies to use vulnerabilities. After all, according to the associated statements released with the VEP Charter, "conducting this risk/benefit analysis" was "a vital responsibility of the Federal Government," implying that they were the most qualified to make these determinations. (Joyce, 2017 n.p) The VEP was institutionalising a set of procedural and substantive boundaries on vulnerability disclosure, with a view to demarcating and managing the credibility of government commitments to 'cybersecurity.'

6.3.4 Enlarging disclosure's scope, making vulnerabilities intelligible.

Segregating governmental discovery and use of vulnerabilities from the risks they posed to wider society was an 'imperative' part of the VEP's stated purpose. The sense of external time pressures, of imperatives stemming from a fast-moving technological frontier, were thus implicit throughout the VEP and its accompanying justifications. In this vein, Rob Joyce reflected on the tensions that cybersecurity's 'imperatives' for patching posed with the instrumental withholding of information from vendors, given that the "…reasons you want to patch, you want to disclose are because our society has grown intertwined with our IT technology, so if there's a flaw in those systems there is an imperative to close that hole and make sure it's not exploited." (Joyce, cited in Newman, 2017). The VEP was thus suffused with references to timing and urgency. The implication here was that if American society was intertwined with information technologies, then they were also intertwined with technological vulnerabilities. As a result, the VEP was intended to act as a means to temporarily set their use apart and to functionally demarcate vulnerabilities from a society 'intertwined' with them. As Rob Joyce later defended the VEP at a public event, it was "…just a fact that the government is going to work to develop vulnerabilities and find them for operations. The ecosystem continues to find new and innovative ways to exploit." (Joyce, cited in Newman, 2017). Implied here was that government actors were responding to external pressures of 'the ecosystem' changing and innovating. Similarly, the NSA general counsel described how,

> Physically, and logically, the domain is in *a state of perpetual transformation*. It enables the transmission of data across international boundaries in nanoseconds—controlled much more by individuals or even machines than by governments... (Ney, 2020 n.p., emphasis added)

In the face of the kinds of criticisms discussed in Parts One and Two, processes taking place in nanoseconds and controlled by individuals and machines rather than governments would prompt novel questions for state actors trying to both articulate and justify the role of vulnerabilities in their cyberspace operations. As systems evolved, the assumption was that discovery, exploitation and patching would also speed up, lending an urgency to government actions.

The VEP is demonstrative of some of the unique challenges that government actors have articulated in bounding cybersecurity, in this instance the distinctive problems of managing interfaces between 'network' time and 'bureaucratic' or 'political' time. Typical of this framing was Admiral Rogers' responses to advanced questions for his confirmation hearings as head of the NSA and CYBERCOM, where he told congress that "transparency can be ensured by establishing procedures" in "real-time," that leveraged "…technology that enables a transparent, policy-based, *machine-speed infrastructure*" (Rogers, in US Senate, 2014c, p. 527, emphasis added). Here, 'machine speeds' apparently stood in tension with the 'political speeds' of interagency government processes , and the desire to pause or control the flow of knowledge for tactical or strategic reasons, even temporarily. Disclosing and sharing information in "…a space this transformative and this disruptive" would challenge institutionalised practices that took place at 'political-speed' (Ratcliffe, in US House of Representatives, 2017a, p. 2). This was expressed in the VEP as an articulation of distinctive time pressures of the role that disclosure played, where:

> …the VEP balances whether to disseminate vulnerability information to the vendor/supplier in the expectation that it will be patched, or to *temporarily restrict the knowledge* of the vulnerability to the USG, and potentially other partners, so that it can be used for national security and law enforcement purposes." (VEP Charter, 2017, p. 1, emphasis added)

By temporarily restricting knowledge, the VEP was intended to give the government a time advantage. As Michael Daniel had phrased the matter, "…the trade-offs between prompt disclosure and withholding knowledge of some vulnerabilities for a limited time can have significant consequences" (Daniel, 2014). The 'significant consequences' here hinged upon the matter of *timing* the disclosures: keeping the vulnerability secret would give government actors a functional advantage, enabling them to take advantage of the knowledge before the vulnerability was detected or patched. The VEP is thus one of the most 'visible' elements of the government's efforts at producing and negotiating an interface between these different tempos.

The VEP was thus intended as a practical strategy of timing, of controlling information as a means of helping government actors to impose a sense of order on a messy ecosystem in ways conducive to orientation and control (Hom, 2018). Controlling information and being able to make functional distinctions between 'secret' and 'disclosed' are based upon a widespread organisational culture within national security circles in the US which share the presumption that "secrets produce security." (Dean, 2004). In the VEP, this was expressed as "…the root of the tension that exists between the desire to publicize every vulnerability discovered by the Federal Government […] and the need to preserve some select capability for action against extremely capable actors" (Joyce, 2017, p. n.p.). Restricting knowledge of vulnerabilities was thus to be a constitutive part of these 'select

capabilities for action' on the assumption that it would help government actors produce security, or defend against adversaries. This was a capability that was predicated upon distinctly time-oriented practices of restricting or 'locking away' knowledge of those vulnerabilities. Here, the VEP was working to translate institutionalised 'political speed' government practices of classification secrecy into the 'new' context of cyberspace operations. Symptomatic of a tendency for state actors to approach 'keeping secrets' as a form of political time management (Horn, 2011), the VEP thus instituted disclosure as a form of bureaucratic and procedural time management in the face of these putative exterior time (and political) pressures to patch vulnerabilities in the networked nation.

Through the VEP, 'disclosure' would not be immediate in the temporal sense then, but neither would it be immediate (self-evident) in the political or democratic sense. With each iteration of the VEP, the arguments of those in the private sector and policy advocacy communities about the importance of 'disclosure' for constituting cybersecurity were increasingly accommodated into federal initiatives, shaping their imaginaries and the ways that they were actualised through initiatives such as the VEP. The VEP was intended to allay some of those criticisms. At the same time however, the VEP would build into its process a broader spectrum of what would count as 'disclosure' by institutionalising exceptions. In 2014, Michael Daniel was reported as implying that the VEP would put vulnerabilities that had been discovered by contractors through the process (Zetter, 2014c). However, the 2017 Charter made a certain range of exceptions explicit when it stated that:

> The USG's decision to disclose or restrict vulnerability information could be subject to restrictions by foreign or private sector partners of the USG, such as Non-Disclosure Agreements, Memoranda of Understanding, or other agreements that constrain USG options for disclosing vulnerability information. (VEP Charter, 2017, p. 9)

This distinction is important, because it provides one possible means for the federal agencies to side-step the VEP in their decision-making process. In the case of the unlocked iPhone discussed in Chapter Five belonging to a San Bernardino shooting suspect, the FBI did not submit to the VEP the vulnerability that permitted their access to the phone because they paid an outside contractor to decrypt the phone (Cox, 2016). As discussed above, in working to constitute disclosure as a spectrum of possible variations rather than a binary state, the VEP here was also circumscribing the immediacy of the government's responsibility to disclose in instances where they paid for the vulnerability but did not 'see it' themselves. Without concretised thresholds for what counts as 'disclosure,' agencies would thus have more room for autonomy. By making the parameters of disclosure less clear cut in this way, government actors were able to reassure outsiders by hailing disclosure-as-transparency, but without setting strict thresholds for agencies to be held accountable to by outsiders.

There were other ways in which what counted as 'disclosure' was expanded and reconfigured by the VEP. The VEP was an institutionalisation of boundary work that sought to emphasise disclosure's ambiguity more as time passed. While technical and operational programs may be in place to share information, like government secrecy and disclosures in other contexts (Stampnitzky, 2020), 'information' still requires political context and human actions to translate it into 'cybersecurity' measures. One of the problems with vulnerabilities is that they do not speak for themselves: they are not self-evident or fungible objects in a familiar sense and are social and organisational entities as much as they are technical. Summarising a principle from the technical security community, one security researcher stated that:

> *It is a well-known fact* that security vulnerabilities are not purely technical problems. They usually arise as a result of the interaction of several components, including technical issues, processes, management, and human errors. (Civaner, 2020 n.p, emphasis added)

As with many matters of risk assessment, different communities expressed competing (and subjective) expressions of the risks calculated by the VEP. Schemes for evaluating and rating risks posed by vulnerabilities have been a matter of debate even within the de facto industry standard for assessing the severity of vulnerabilities (Taylor, 2015). Here, the security researcher community has highlighted the limitations of categorising vulnerabilities and their risks as quantifiable entities (Robinson, 2019; Ross, 2019). Rather than making vulnerabilities and their risks a quantifiable entity, such a dissenting conception of vulnerabilities as 'not purely technical problems' meant that the VEP and attendant government discourses about vulnerabilities were to play an important part of strategic efforts by federal actors to render vulnerabilities meaningful and actionable.

The difficulties of information 'not speaking for itself' were illustrated by the NSA's newly formed Cybersecurity Directorate's (CSD's) first public cybersecurity advisory regarding a vulnerability. In May 2020, the CSD announced the news that a severe vulnerability in one of the internet's most prevalent email server software packages Exim had been exploited since August of 2019 by a state-linked Russian 'advanced persistent threat' (APT) group called Sandworm. Exim is software that receives, routes and delivers email messages, and the NSA used its first cybersecurity advisory to detail how a bug in the software had been exploited by Sandworm actors to enable a persistent 'backdoor' access on the targets' networks by sending a carefully crafted email. In fact, a patch for this bug had been developed two months before Sandworm had started exploiting it, and nearly a year before CSD released their advisory. To be protected from the risks posed by this vulnerability, network operators had to install the patch, but for all kinds of reasons, many organisations had not done so (Ilascu, 2020; NSA, 2020). Some may not have been aware of the vulnerability amongst all the streams of security information available to them, and not had automatic updates enabled, some may not have been able

to take the systems offline to update with the patch, some may not have had the resources spare to address every single security issue in their systems and had to prioritise (Gooding, 2020). This Exim bug was not new information, nor even classified, but by linking it to exploitation campaigns by Russian state actors, the CSD sought to give this information a political context intended to convince practitioners of the urgency of this information. 'Disclosure' thus necessitated an important amount of interlocution by government agencies, even while it was becoming an increasingly important part of government agencies' efforts to defend their credibility in matters of national 'cybersecurity.'

As well as instituting disclosure in ways that would enable government agencies to maintain some of their political and tactical autonomy, the VEP was both formed by and a formative part of broader normative and political debates about the role that disclosure should play in government efforts to 'do' cybersecurity. Disclosure's role as a means of defending the government's cybersecurity credibility was reflected in the NSA's Cybersecurity Directorate (CSD) disclosure of a vulnerability in Windows 10 operating systems in January 2020. Rather than simply publishing the details online and sending out a press release, the CSD announced details of the flaw by hosting a press conference, where the CSD's head, Anne Neuberger, told reporters that the bug "makes trust vulnerable" (BBC, 2020; Newman, 2020). This contrasted with how the NSA had traditionally approached disclosure. The CSD was the culmination of a series of initiatives designed to 'open' the NSA up for the purposes of constituting a distinctive role for itself in matters of cybersecurity. As the head of the directorate made explicit to reporters at a press tour of the CSD's new site, the CSD was evidence of an approach "a little bit different for us than the traditional No Such Agency approach." (Neuberger, cited in Konkel, 2019 n.p). In telling the story of the CSD's rationale, Neuberger traced the inflection point for the agency's 'new approach' to Edward Snowden's disclosures in 2013, and suggested that intelligence agencies in a democracy face specific challenges in legitimising their missions (Konkel, 2019; Sebenius, 2019). In addition to such imperatives to be more 'transparent' stemming from historically resonant narratives of democratic openness, disclosure had become a functional requirement in managing trust.

By 2020, the VEP and the attendant political debates over the parameters of disclosure indicate the broader shift in instrumental notions of 'disclosure.' The CSD's public disclosure of the Windows vulnerability in 2020 signified a turning point for the agency: during the press conference call, Neuberger highlighted that "this was the first time Microsoft will have credited NSA for reporting a security flaw." (Neuberger, cited in Konkel, 2019 n.p) While NSA may have done so with previous vulnerability disclosures, it had never been publicly acknowledged by either party. In discussing the VEP, Michael Daniel had pointed out in 2014 that while disclosure was the 'default position,' the difference was that "[w]e just don't take credit for it for a variety of reasons and have no desire to take credit for it." (Daniel, cited in Zetter, 2014c n.p). Similarly, a former technical director of the NSA's

Information Assurance Directorate (that was now subsumed into the CSD) described how during the 1990s the agency "mostly gave away vulnerabilities — but never claimed public credit." (George, cited in Nakashima and Riley, 2020 n.p). One former NSA information assurance executive suggested that the disclosure marked a deliberate shift, and though it would not happen every time, "this is not just for show. They're trying to signal that cybersecurity is really important" (Sagar, cited in Nakashima and Riley, 2020 n.p). For those at the NSA concerned with demarcating the agency's credibility as a defensive force for good and to signal its increased openness, 'disclosure' could thus act as a useful device, even while they explicitly underscored that this vulnerability had not been subject to the VEP. In discussing the disclosure, CSD agency officials suggested that subjecting the vulnerability to the procedure would "risk something going wrong." (cited in Nakashima and Riley, 2020 n.p) and that the VEP injected uncertainty. As well as a procedure, disclosure had become a political resource for defending the defensive cybersecurity credentials of government agencies, even if the VEP had made what counted as a threshold for 'disclosure' a matter of procedural ambiguity.

Over time, by working *for* boundaries the VEP has thus sought to reconfigure the bounds of disclosure in order to accommodate both the federal visions of cybersecurity as well as some of the dissenting narratives discussed earlier. To begin with, federal actors did not articulate the boundaries of 'disclosure' as it was classified, and called 'dissemination,' but as time has passed 'disclosure' has become an increasingly salient matter of contention. With each iteration of the VEP, and with each round of debate with those outside of government, vulnerability 'disclosure' as a practice and concept became an increasingly important symbol and resource for government actors to draw upon as a means of highlighting their cybersecurity credentials. Disclosures about the VEP were a means for the Administration to keep the American people minimally informed of its activities, and to characterise these activities in ways intended to solicit public support by invoking normatively laden ideals of transparency, accountability and responsibility (Pozen, 2013). At the same time, the VEP worked to avoid any substantive alternatives to government actions by keeping details of vulnerabilities from being made public. Those that government did reveal still required interpretation and translation into something politically meaningful, as the case of the Exim bug indicated. Normatively and procedurally, revealing the VEP under the guise of transparency was a strategic effort at legitimising the government's actions. Although it is dressed up as transparency for democratic accountability, it sought to focus attention on the processes, rather than questioning why this process was necessary in the first place. It also helped to show that government agencies possess these offensive capabilities (perhaps as a form of deterrence signalling), but without really addressing the contents of the disclosure. Over time then, disclosure has been mobilised as both a symbolic resource as well as a procedural method for federal efforts to set limits, or bound, their vision of cybersecurity.

6.4 Conclusion

The largely competitive boundary work analysed in this chapter was concerned with demarcating the boundaries of 'disclosure' to defend (but also co-produce) the political legitimacy of federal visions of cybersecurity, and what 'cybersecurity' means. The chapter argued that this boundary work has been about making technologies and vulnerabilities legible in ways that support 'classical' responsibilities of the state, whilst also defending the autonomy of government agencies to undertake intelligence and law enforcement operations in cyberspace. For administration officials and those involved in the procedure itself, the VEP was an important part of making 'vulnerabilities' and 'disclosure' intelligible both for government actors and for the wider public. By translating disclosure into political-speed classification processes, the VEP also helped administration officials translate vulnerabilities into an idiom of national security secrecy.

However, the episodes of competitive boundary work analysed in this chapter suggests how a typology of (competitive, collaborative, configurational) boundary work are not mutually exclusive strategies nor set clear-cut parameters of what happens to boundaries during these episodes. In fact, the ways that the bounds of 'disclosure' have been reconfigured through of the VEP's development shows how conceptual, operational, or institutionalised boundaries can shift over time without necessarily being *the* strategic goal in support of collaborative boundary work. Put another way, collaborative boundary work typically seeks to reconfigure and downplay boundaries to facilitate collaboration, but this chapter has shown how competitive boundary work may also reconfigure those boundaries for different (competitive and defensive) ends too, thus indicating how the typology of boundary work strategies is not a strict characterisation.

As this chapter has shown, 'vulnerabilities' are not just technical, they are social and human too, made up of a uniquely non-fungible interplay of technologies, people and processes. Implicit within the VEP were concerns about the technological and networked future, with all its potential vulnerabilities and unknown risks. It found that the VEP constituted 'disclosure' in ways intended to forestall the ill-effects of time passing, a way of managing both the competing 'equities' and articulations (from Parts One and Two) of what cybersecurity *meant*. At the same time, the VEP was a strategic and tactical means of articulating the problems of a networked nation in terms of 'balancing' national security and cybersecurity by framing it in terms of competing 'equities.' Like other chapters that have shown how different characteristics are ascribed to cybersecurity at different times, depending on the interests and background of the speaker, this chapter finds that 'disclosure' has been used to demarcate political and operational bounds of 'cybersecurity.' As the concluding chapter will now draw together the findings of this and the preceding empirical chapters, insofar as 'cybersecurity' can be characterised as any one thing, the final chapter will draw out the implications

that follow from the project's findings that what cybersecurity *is* has been constituted by boundary work.

Chapter Seven: Conclusion. Cybersecurity, boundary work, bounding the state

7.0 Introduction

The first argument in this thesis has been that what cybersecurity 'is,' and how its boundaries are drawn, are not overdetermined by strategic or technological imperatives, so much as they reflect the efforts of different entities to defend and extend their own organisational and symbolic boundaries. Rather than trying to 'fix' cybersecurity with substantive definitions, the analysis so far of these accumulations of people, organisations, institutions and technologies has taken a uniquely processual view of 'cybersecurity.' By illustrating the continuous political *processes* involved in demarcating this open-ended and continually becoming thing of 'cybersecurity' and by focusing on the ways that boundaries have been articulated, problematised and mobilised in cybersecurity politics, the thesis has provided important insights into the political and cultural assumptions animating this context. It has also outlined a productive analytical framework for security studies scholars looking to denaturalise technologically determinist security discourses. Having used the methodological and analytical framework of boundary work, the argument will conclude in this chapter by examining the premise that like the state itself, cybersecurity is made up of contingent processes and emergent properties, embedded in heterogenous initiatives and programs.

'Cybersecurity' has been contested because ubiquitous computing and widespread interconnected networks and infrastructures have led governments – and as illustrated in this thesis, multiple agencies of the US government – to grapple with the tensions between the opportunities afforded by 'cyberspace' against the challenges these technologies appear to pose to historically resonant categories and distinctions. Indeed, the policy discourses of agencies of the US government concerned with cybersecurity often explicitly testify to such processes of 'fixing' the meaning, significance and boundaries of cyberspace. Policymakers complain about a lack of conceptual clarity or clearly defined parameters for what counts as 'cyber,' and so more precise, or more 'accurate' definitions of the parameters of 'cybersecurity' are entreated by policymakers and security actors to better 'fix' the problems posed by cyberspace. In the process, as each of the empirical chapters demonstrated, specific consequential boundaries and institutional responsibilities of both the US state and its agencies have been amplified and problematised by actors in these debates. Despite various efforts at fixing substantive definitions, cyberspace, in many ways, seems to exceed and evade those definitions. For state actors, this has provided significant contention and debate. Cybersecurity politics are thus the forum and form that these concerns about bounding cyberspace take place.

The second argument in this project has been that key actors have engaged in forms of 'boundary work' to 'fix' the boundaries of 'cybersecurity' as part of their efforts to stabilise state practices in this matter. Cybersecurity politics have therefore been concerned with turning the empirical and conceptual complexity of 'cybersecurity' into more governable organizational arrangements and discrete agency projects, coproduced in turn by technologies, political cultures, and bureaucratic politics. In other words, cybersecurity politics have sought to 'bound' the matter in particular ways, to make 'cybersecurity' amenable to state orientation and control. Here, 'cybersecurity politics' are not just rhetorical and discursive efforts to build support for preferred courses of action in 'formal' arenas or places of politics, such as Congressional hearings and judicial processes. The analytical concept of cybersecurity politics has also captured how social actors direct heterogenous elements of people and technologies towards concrete ends, as exemplified in each of the chapters' analysis of the security imaginaries animating those efforts (Jasanoff and Kim, 2015; Jones-Imhotep, 2017). These are efforts that have sought to make sense of, but also produce the state's roles and responsibilities in cyberspace, efforts at making cybersecurity amenable to the 'classical responsibilities' of the state.

As we have seen, because cyberspace is conceptualized in spatialised terms in cybersecurity politics, all sorts of consequential distinctions and boundaries come to be challenged. As each of the chapters showed, different organisational and cultural imaginaries would strategically problematise or mobilise boundaries according to their interests and their orientation to the problems at hand. At the same time, those boundary distinctions act as prime cultural resources, working as formative and sometimes intuitive cognitive and political frameworks for actors trying to make sense of new concepts and phenomena. The work of establishing and stoking this conception of networked communication technologies in terms of boundary-blurring risks and threats served to instigate demand for frameworks that could be used for guiding change (Pfotenhauer and Jasanoff 2017). In each of the chapters, the specific boundaries blurred, downplayed, or problematised in imaginaries of insecurity would therefore depend upon who was speaking, what they wanted, and which agency or institution had shaped their characterisations. By articulating cybersecurity as a problem that 'blurred' 'traditional notions' of boundaries and remits, security imaginaries sought to create the social and political conditions in which proposed initiatives could 'make sense.' Boundary work thus emphasised particular traits and characteristics of 'cybersecurity' to rationalise particular courses of action.

7.1 Competing imaginaries and visions of the future

As discussed in, for example, Chapter Three, efforts at the NSA to institutionalise hacking capabilities challenged how actors in the US had traditionally governed demarcations between

'wartime' and 'peacetime' activities. In the US, these distinctions have both normative and procedural ramifications. Procedurally and institutionally, they are distinguished (though not rigidly separated) in legal authorities and congressional oversight, which profoundly shapes the institutionalised activities that the military or the intelligence community can undertake. Normatively, such distinctions also serve to legitimate certain actions at the national and international levels. While boundaries between intelligence and offensive capabilities had been technically and organisationally downplayed as a result of initiatives that sought to make the NSA the dominant 'understander' of those technologies, those historically resonant distinctions meant that the intelligence agency was circumscribed from keeping a unique organisational hold over those hacking capabilities. As a result of collaborative boundary work describing cybersecurity in terms of a structural and strategic imperative to develop offensive cyber capabilities, working *at* such distinctions became both a subject of uncertainty and a source of authority. The historical and Constitutional resonance of such distinctions could act as productive resources. An imaginary was thus coproduced between those initiatives at the NSA and broader military strategic narratives to make the case for a military cyber command.

In fact, we saw how the development of distinctively 'military' cyberspace capabilities has not been the result solely of a 'natural trajectory' of cyberspace or technologies. Having established CYBERCOM, over time advocates of distinctly *military* cyber capabilities would subsequently work hard *for* boundaries to *reinscribe* distinctions between intelligence and military capabilities. Such competitive boundary work sought to defend and contest the boundaries that had initially been mobilised and downplayed in the imaginary that had facilitated CYBERCOM's establishment. Only as CYBERCOM has taken shape has a narrative emerged that 'persistent engagement' is the strategy that best justifies or fits conceptions of military cyberspace capabilities. Contrary to a great deal of the mainstream policy discourse, Chapter Three's argument was that the technological environment of cyberspace did not overdetermine the shape or the development of these distinctively military capabilities. The doctrine of persistent engagement has instead gradually emerged as a means of demarcating CYBERCOM from their progenitors in intelligence agencies and practices, and for establishing authority and autonomy for the new command. Persistent engagement iterated out of fraught processes of social, bureaucratic, legal, cultural and technical efforts to produce the state's and military's role in 'cyberspace.' The chapter highlighted that this doctrine is a condition for, and a condition of, the military's cultural and organisational dispositions, as much as through bureaucratic politics or any 'essential characteristics' of the operating environment. Actors struggled to articulate the distinctiveness of military cyber operations and to fit them into pre-existent notions of what military capabilities 'should' look like based on long held peacetime-wartime distinctions. Thus, to differing extents at different moments in time, capabilities have informed strategy and organisational boundaries, while institutionalised boundaries have informed capabilities and strategies.

Unlike the military's framing of the (cyber)security imaginary in terms of 'domains,' and often in direct competition with that imaginary, in Chapter Four we saw how the DHS would articulate a very different vision of 'cyberspace' and 'cybersecurity.' Their initiatives were oriented around constituting cyberspace as an 'ecosystem' and an 'environment' instead of a 'domain.' Competitive boundary work here was both a product of DHS' organisational culture and history as much as a commitment to a particular vision of the future. Culturally speaking, territorial and spatial distinctions between 'internal' and 'external' have long played a constitutive role in shaping how the national security apparatus organises itself in the US. This was a habitual understanding of the importance of being able to demarcate the bounds of the nation or territory to be defended. In this case, it was the "global movement of threat activity in and through cyberspace" that was said to challenge "the U.S. Government's traditional understanding" of how to demarcate between and address domestic and foreign activities (Rogers, cited in US Senate, 2015a, p. 15). Such essentialised claims about the nature of cyberspace or the nature of threats formed the basis for competing claims over which federal agency should have responsibility for domestic cybersecurity. The DHS' authority on matters of cybersecurity had consistently been contested in several respects, including whether they were functionally capable and possessed the right resources and expertise, or whether the 'nature' of the threats and the 'nature' of cyberspace made DoD the more appropriate agency.

Chapter Four therefore showed how such boundary distinctions have played a constitutive role in shaping the programs and policies that have emerged in US cybersecurity politics. Contrary to the cultural, political, institutional, and financial interests at stake in the military's (cyber)security imaginary of cyberspace's essentially 'borderless' nature, this chapter found that boundary distinctions of 'internal' and 'external' served as productive strategic resources for actors working to defend the legitimacy, credibility and authorities of the DHS. DHS actors were thus able to 'domesticate' and 'reterritorialise' cybersecurity by shifting the focus onto managing the nation's internal vulnerabilities through a risk-based framing. Here, competing visions and goals were embedded by boundary work in technical and organisational infrastructures, in distinction to efforts by the DoD and CYBERCOM's advocates. The DHS' federal cybersecurity imaginary helped define priorities and allocate resources for carrying out a distinctive way for the DHS to constitute their vision of cybersecurity. In this sense, while military actors had tried to produce a vision of the homeland by enacting and managing the 'external' boundaries of that homeland, and so constitute a cybersecurity oriented around external threats and a 'terrain' to be maneuvered on or through, in the end the DHS' boundary work was more successful in embedding and enacting links between the 'homeland' and 'cybersecurity' with a framing of 'territory' to defend an exclusive operational and political space for itself.

While Chapter Four showed how the DHS was struggling to defend its credibility and legitimacy in internal turf battles, Chapter Five outlined how contemporaneously the DHS and the federal government were working to mobilise symbolic, normative and social distinctions of 'public' and 'private' to make the case for 'extending' cybersecurity through 'public-private partnerships.' The government's reliance on the infrastructure of cyberspace – and by extension the operators of this infrastructure – for the nations' security and prosperity has been a recurring theme in US cybersecurity politics, commonly articulated in terms of distinctions between 'public' and 'private' actors and values. This chapter showed how making distinctions between 'public' and 'private' therefore set expectations about what the US government can – and cannot – do in cybersecurity.

An analysis of federal strategy and vision documents found configurational boundary work to orchestrate and produce collective action in the name of 'cybersecurity,' in which a federal and DHS articulation of 'public-private partnerships' would work to devolve political authority for security away from the state. Boundary distinctions were therefore mobilised by government actors to set up the conditions for a reconstitution and shift of roles and responsibilities over time, rationalising a vision of a secure future they hoped to see built, but one they could not build by themselves alone. This meant they would mobilise those distinctions, and undertake boundary work *through* boundaries, to variously enlist, motivate or compel the involvement of actors beyond the government. In the other chapters, the project has looked at federal initiatives that have followed from official strategies and visions of insecurity. In contrast, this chapter showed how government and private actors used distinctions and categories of 'public' and 'private' to actualise but also modify those federal visions of 'cybersecurity.' Both case studies were examples of state actors working to orchestrate and mobilise intermediaries in pursuit of their stated goals of distributing political authority for 'cybersecurity.' The main difference lay in how willing representatives of the two companies were to engage with the government: in the case of attribution, elements of the private sector were actively endorsing a role for themselves where both state and non-state actors carefully downplayed boundary distinctions with collaborative boundary work *at* those boundaries. In the second case of encryption, this was an example of the technology companies pushing back and of technology resisting the efforts of law enforcement to stabilise boundaries in new ways with competitive boundary work *for* such distinctions. Here, Apple were working to produce a dissenting vision of cybersecurity – and who it was for – on the basis of distinctions between 'public' and 'private' values.

The findings of this chapter do not suggest a zero-sum shift of political authority from 'public' to 'private', but an diffusion and reorganisation of political authority that favours the interests of those who can mobilise and embed those distinctions with their resources. The failed boundary work of congressional lawmakers in this chapter also reflects the overall argument in this thesis that cybersecurity practices are not as structurally and technologically driven as federal discourses suggest.

Instead, competing imaginaries of 'cybersecurity' have emerged at the point of cybersecurity politics and boundary work, not all of it by state actors, and not stemming simply from putatively self-evident technological 'realities.' In both cases and the empirical chapters as a whole, we can see how boundaries were simultaneously the source and the result of contestation: boundaries here are a constant 'work-in-progress.'

Chapter Six analysed how the drawing the bounds of 'disclosure' played a productive part in government efforts to distinguish and demarcate cybersecurity's political and operational limits. Chapter Six saw the boundaries of 'disclosure' become an important and constitutive element in government efforts to articulate where the limits of 'cybersecurity' lay in relation to 'national security.' As opposed to internal turf battles amongst different state agencies as in the first two chapters, boundary work in this chapter was directed towards those outside the government. Here, the bounds of 'disclosure' were articulated through competitive boundary work *for* such boundaries as a way to contest the government's use and retention of 'vulnerabilities' by technologists and civil society advocates who were critical of the government's conceptions of 'cybersecurity.'

The argument in this chapter was that the boundary work analysed here was an important part of making technologies and vulnerabilities legible in ways that support 'classical' responsibilities of the state, whilst also defending the autonomy of government agencies to undertake intelligence and law enforcement operations in cyberspace. 'Disclosure,' with its normative and culturally significant associations in the US with liberal democratic ideals of 'transparency' and 'accountability,' (Dean, 2004; Bratich, 2006; Birchall, 2011; Fenster, 2015) thus became the site for different groups to contest what cybersecurity *meant* according to different conceptions of 'security.' Demarcating the boundaries of disclosure was used here to defend (but also shape) the political legitimacy of federal visions of cybersecurity, and whether cybersecurity means to patch or to spy for the greater national good. For government actors 'disclosure' connoted a national security threat to their ability to keep secrets and produce 'national security,' while for those contesting the government's use of vulnerabilities, disclosure was a constitutive part of producing 'cybersecurity.' With each iteration of the VEP, and with each round of debate with those outside of government, vulnerability 'disclosure' as a practice and concept became an increasingly important symbol and resource for government actors to draw upon as a means of highlighting their cybersecurity credentials, accommodating those dissenting imaginaries in some ways.

This chapter's findings that 'vulnerabilities' are not just technical, but made up of an interplay of social, political and organisational practices, supports the project's overall argument against technologically determinist framings of cybersecurity. Implicit within the VEP were concerns about the technological and networked future, with all its potential vulnerabilities and unknown risks. For

administration officials and those involved in the procedure itself, the VEP was an important part of making 'vulnerabilities' and 'disclosure' intelligible both for government actors and for the wider public, even if those disclosures to the public were limited. Disclosures about the VEP were a means for the Administration to keep the American people minimally informed of its activities, and to characterise these activities in a manner designed to build support by invoking normatively laden ideals in their articulation of a security imaginary. At the same time, the VEP worked to avoid any substantive alternatives to government actions by keeping details of vulnerabilities from being made public. Those that government did reveal still required interpretation and translation into something politically meaningful, as the case of the Exim bug indicated. At the same time, the VEP was a strategic and tactical means of articulating the problems of a networked nation in terms of 'balancing' national security and cybersecurity by framing it in terms of competing 'equities.'

The chapters have thus come full circle, starting with imaginaries of a vulnerable networked nation in which the US military must develop its own hacking capabilities, only for those hacking capabilities to trigger subsequent vulnerabilities and boundary work by those contesting those visions of insecurity. This summary of the preceding chapters showcases how charges and counter-charges in US cybersecurity politics, articulations of specific boundaries, distinctions of how it 'fits' into one category rather than another category have each demonstrated the project's premise that boundaries stand in for and also help produce choices of one future over another.

Cybersecurity politics in this context have been about fixing the bounds of cyberspace so that they conform to (but also at times challenge or reconfigure) ideas about the state as security provider, and the state's relationship with cyberspace. The chapters have shown how by becoming so widespread in US security discourses, the different imaginaries of cybersecurity have directed funding, the employment and development of particular technologies, the viability of specific policies, and the interplay of social and technical and institutional arrangements. While the first parts of each of the empirical chapters have been concerned with showing how security actors have articulated, drawn and contested how cybersecurity maps onto boundaries of the state and its roles and responsibilities, the later parts have each then demonstrated how this boundary work has become stabilised with initiatives and programs. It is to the potential wider significance of this boundary *work,* though which actors have sought to embed competing organisational goals and visions of cybersecurity into technical programs and initiatives, that this chapter now turns.

7.2 Cybersecurity is all about boundaries (of state action)

Rather than trying to explain away all the different definitions and conceptualisations of what 'cybersecurity' *is*, this thesis has instead outlined its emergent properties. Cybersecurity is not one

thing but emerges at the point of boundary work that emphasises its different boundaries and characteristics and different times, depending on the interests of the people or initiatives drawing its boundaries. This has a number of important and interesting broader implications that parts two and three of this Conclusion will seek to draw out. An important corollary of the findings in the empirical chapters is that these efforts at bounding the parameters of cybersecurity are more than simply rhetorical, but are institutionalised, enacted and materialised. As Markham (2003, p. 1) has underscored, the choices and discursive framing at work in talking about the internet and communication technologies have practical consequences on how these technologies are perceived and used: as these discursive frames and metaphors of cyberspace become more embedded and taken for granted, "alternatives are shut out, cut off and left behind." The preceding chapters have demonstrated how in some important respects, the ways that state actors imagine and project 'cybersecurity' has played a constitutive part in shaping the policies and initiatives that have followed.

The symbolic, organisational and political boundaries discussed so far have been argued in the thesis to provide the conceptual tools that groups use to compete over the production, diffusion and institutionalisation of different narratives and principles in their social relations. Importantly, moreover, these sense-making efforts are enabled or constrained by the already constructed social world, such as particularly evocative discourses, or powerful organizations (Kinchy and Kleinman, 2003), or what Law (2004) would describe as 'method assemblages'. Ideas such as 'the state' and political authority derived from 'public' and 'private' distinctions are examples of the kinds of categories that can have profound social implications, and the boundary work that actors have undertaken that reference these boundaries also serve to constitute them, in incremental and recursive ways.

The boundary work analysed in this thesis has first of all been about all kinds of actors, federal agencies, policy advisers, advocacy groups, corporations, technologists, and politicians competing for power and resources and political authority. But for state and federal actors, this boundary work has been informed by, and in turn shaped imaginaries of insecurity, in an ongoing and recursive way, so that it is no longer simply instrumental or strategic but deeply culturally meaningful and unconscious. The findings in the chapters have led me to argue in each of them that boundary work has played a productive role in making technologies legible in ways that support 'classical' responsibilities of the state, whilst also extending or remaking the parameters of some of those 'classical' responsibilities.

The initiatives discussed in Chapter Three demonstrate the extent to which boundary work at the distinctions between peacetime and wartime activities have enlarged the roles, responsibilities and capabilities legitimated by military cybersecurity imaginaries. Boundaries that govern peacetime activities have thus been reconfigured and enlarged in this context. The strategy of 'persistent

engagement' and 'defend forward' have worked to extend the military roles and activities beyond military networks not just figuratively but literally, where in 2010 they were proscribed from operating beyond military networks because of restraints on military actions outside of peacetime. By expanding definitions of 'TMA' to incorporate cyber operations and working to reinscribe the technical and organisational differences between intelligence and military roles in cybersecurity, the United States is working hard to demarcate how these emerging capabilities can be bound within distinctions demarcating peacetime and wartime activities, whilst simultaneously expanding the bounds of national cybersecurity to include military cyber capabilities and cyber 'defense' policy. 'Persistent engagement' has thus been the product of, and has acted as, boundary work.

The particular disposition of the United States military in terms of its large funding and organisational heft have meant that in its reading of cyber insecurity, the military has gradually produced the parameters of its role in terms of military commands and a doctrine of persistent engagement, where other countries with other institutional predispositions and biases would probably produce slightly different outcomes from their culturally-specific boundary work. In the US, this has worked to produce a distinctly military reading of cybersecurity capabilities based upon distinguishing between 'intelligence' tools and capabilities, and 'military' tools so as to defend the credibility of (and therefore the resources for) that military command. Yet despite the widespread technologically deterministic narratives in US cybersecurity politics about cyberspace's essential characteristics driving strategy, this chapter has shown a more nuanced and instructive account of social, bureaucratic, legal, cultural and technical efforts to produce the state's and military's role in 'cyberspace.'

The initiatives analysed in Chapter Four exemplified how other federal agencies have sought to 'translate' cybersecurity into more organisationally intuitive frameworks for them. Consequently, the competitive boundary work in Chapter Four was concerned with embedding the DHS' competing visions and goals into technical and organisational infrastructures. This boundary work also helped define priorities and allocate resources for carrying out different tasks related to cybersecurity. In this sense, the discussion of the emergent and co-productive relationships between the DHS' technical programs and its risk-based approaches indicated that this boundary work took an iterative form. Programs and organisations were designed to enact boundaries; those programs subsequently informed organisational and conceptual boundaries. Here, the NCPS was shaped by boundaries to begin with, designed as a program that was trying to 'bound' and consolidate networks. Producing the boundaries of networks in such spatialised ways was difficult though, and this informed the DHS' shift in its institutional focus away from external threats to internal risks. Technical programs like the NCPS thus shaped (and was shaped by) risk-based approaches. DHS actors were able to 'domesticate' and 're-territorialise' cybersecurity by shifting the focus onto managing the nation's internal vulnerabilities

through a risk-based framing. By mapping the American homeland as a field of vulnerabilities (Lakoff and Collier, 2008), the DHS' domestication of cybersecurity sought to 'bound' cyberspace according to national and territorial distinctions that set limits on the military's reach into domestic networks.

Throughout this thesis, the ways that cybersecurity has been articulated and negotiated as a matter of national security are emblematic of broader debates about political authority across historically resonant notions of a 'public' and 'private' divide in the US. Chapter Five showed some of the ways that actors have sought to make sense of, but also build, desirable technological realities implied by their conceptions of 'cybersecurity.' As a result of the ways that these historically resonant distinctions have been mobilised and contested, government actors have undertaken configurational boundary work that sought to variously enlist, compel, borrow, appropriate, delegate or recruit the skills, toolsets, and resources of non-government actors. In other words, they have sought to 'make space' for non-government actors to partake in cybersecurity roles and responsibilities. However, as others have noted and this chapter bears out, this boundary work does not signify a "zero-sum shift, but an unbundling and reconfiguration of political authority" (Genschel and Zangl, 2017, p. 63; Weiss and Jankauskas, 2019). Cybersecurity practices and imaginaries have not emerged simply as the result of a series of technical features or fixes. Similarly to Chapter Four, Chapter Five demonstrated the ways that boundary work builds on a recursive relationship between practice and symbolic and social boundaries. Technologies can make some practices available, which drive and constitute changes in conceptions of boundaries, while these new configurations of boundaries in turn can legitimise new practices. Cybersecurity politics have both drawn upon and reconstituted how some of these distinctions between 'public' and 'private' operate in matters of cybersecurity. Here, such distinctions have been mobilised by state actors wishing to act as orchestrators of security, as a means of re-mapping their 'traditional' responsibilities into a decentralised network of public and private actors, so that attribution is no longer a sole responsibility for the federal government as it was outlined in the 2003 *Strategy to Secure Cyberspace*. Such an unbundling of political authority from the configurational boundary work of federal actors also blurs lines of accountability so that no single entity is held responsible for cybersecurity.

Just as boundary distinctions of public and private were utilised to make state responsibilities for cybersecurity legible, the VEP as described in Chapter Six was an important part of making 'vulnerabilities' and 'disclosure' intelligible both for government actors and for the wider public. For administration officials and those involved in the procedure itself, the VEP was a means of trying to both control and make sense of broader social and technical processes. By translating disclosure into political-speed classification processes instead of so called 'network speed' cyberspace technologies, the VEP also helped administration officials make vulnerabilities 'sensible,' by 'translating' them into a more familiar idiom of national security secrecy. Like the chapters before it, this was a matter of

collective sense-making about the state's role in cyberspace, though it was one of the more contested cases of state efforts analysed here. This again highlights one of the project's broader findings about the extent to which these collective efforts are reciprocal and emergent processes rather than dominant discourses imposed unidirectionally from above by state actors. Moreover, state-centric discourses of security are a prominent example of powerful discourses (Weldes et al., 1999), but by addressing the different (competitive, collaborative, configurational) boundary work strategies, we can begin to trace the limits of those powers, with important and perhaps more generalisable insights into other contexts of security politics more broadly.

7.3 Cybersecurity for a Networked Nation

Rather than working to constitute a single 'vision' or monolithic cybersecurity, for government actors and agencies trying to articulate and legitimise their imaginaries of cybersecurity (and therefore secure power, funding and authority), this boundary work produced and embedded overlapping logics of boundaries into programs and institutions at political, strategic, operational and tactical layers. These multiple boundaries and layers of cybersecurity are not simply an inventory of different approaches that constitute a whole. In a way, they work as an aggregate, an interwoven compilation of concepts, practices, initiatives, processes, technologies and people. These initiatives are part of an effort by state actors to downplay functional, operational and technical boundaries of ideas of 'the state' as a way to produce but also accommodate these different articulations and imaginaries of cybersecurity. Government actors have worked, and are working, to reconfigure and manage the bounds of 'cybersecurity' to make it more intuitively recognisable and governable as a matter for state interventions. After all, 'cybersecurity' is not a singular 'thing,' but is shaped by (and shapes) a whole range of political, technological, and cultural meaning-making efforts.

This thesis contends that cybersecurity politics have been concerned with marking out and enacting the (organisational, practical bounds of) 'the state' in the context of cyberspace. Of course, there is far more to the boundaries of the state than matters of cyberspace and cybersecurity. But in lots of important places and ways, this is about making 'cyberspace' amenable to state management, governance and orchestration. This thesis has outlined how cybersecurity, in its various contested formulations, thus forms a key site for sociotechnical attempts to link cyberspace to ordering of territory and 'stateness'. Cyberspace is a metaphor, an imaginary, but it is also made up of technology, people, institutions, norms, protocols and practices. This is an expansive approach to cyberspace, but it begins to illustrate what is at stake in cybersecurity politics, concerned as it has been with articulating and producing the state's relationship to cyberspace. The discussion of the chapters so far

has underscored how 'cybersecurity' is playing a constitutive part in articulating and producing the state's roles, responsibilities and visions of cyberspace.

Cybersecurity politics in the US have been suffused with claims about the radical novelty of information communication technologies and the destabilising or disturbing effects that they are thought to have on the state's boundaries and parameters. This conceptualisation of a state in crisis has also featured in mainstream policy circles and international relations literatures (including, but not limited to Kello, 2013; Buchanan, 2016). While 'the state' is undoubtedly undergoing transformations and intensified global processes of exchange and movement (Sassen, 2008), this thesis is an attempt to temper those technologically determinist claims to radical novelty in both the security discourses and the literature (Kello, 2013). Claims that 'the state' is in crisis are often implicitly invoking a 'time before,' the equivalent of the old saying of 'in my day…' In fact, the logical conclusion of the research in this thesis reinforces the literature that has shown the state has never really been a stable edifice, that it has always been a socially contingent and emergent set of granular processes (Carroll, 2006, 2012; Sassen, 2008; Mayrl and Quinn, 2016).

In the American case analysed by this thesis, the initiatives developed and iterated in the name of 'cybersecurity' have been directed towards coordinated and concrete ends, but there may be some wider consequences to the ways that this boundary work has become temporarily stabilised or concretised. Understanding boundary work and discourse as having a constitutive or productive power also means that we can think through the implications that cybersecurity politics have for ideas of the state, its policies, but for culture and society more widely too. As this chapter so far has underscored, discourses and boundary work that demarcate between 'domestic' and 'foreign,' between 'internal' and 'external' security amongst many others have important relationships with ideas of the American 'home' and 'self' to be secured. Here, ideas and cultural reference points about what it is to be a (liberal, capitalist) American citizen are mobilised in these discourses as the referent. This kind of analysis can help us unravel the relations that technologies, cybersecurity politics and practices have with the (re)production of state identity. This is a conception of identity depending on enactment, rather than having some sort of foundational essence.

7.4 Conclusion - To what extent and in what ways are boundaries reconstituted in and by US cybersecurity politics?

The premise of this thesis has been that cybersecurity is all about boundaries. It has contended that the selective attribution of this or that characteristic to 'cybersecurity' cannot be explained by

what cybersecurity 'really' is in practice or policy, but only by the pragmatic utility and cultural context of any given boundaries at particular moments of time. To paraphrase Gieryn's discussion of science (1999), the question is not 'is it accurate,' but 'is it useful, and if so, for whom or what?' The 'cybersecurity' label has thus been an object of boundary work by those who want to demarcate (in the sense both of defining and claiming) security on their own terms.

By using the analytical and methodological framework of boundary work, this project has explored the ways that 'cybersecurity' is an arena for struggle over the political imagination, and has provided evidence of multiple narratives-in-the-making about cybersecurity, in which state-based (and military) readings of cybersecurity appear inevitable, the only judicious response to a looming crisis of technological vulnerabilities and the external agency of adversary actions. In each of the chapters, cybersecurity imaginaries have as acted as sets of "orienting assumptions and operationalizable propositions" (Sadowski and Bendor, 2019) about the state and its security, about the relevant security 'actorness' of those involved. Though the counter imaginaries of the DHS, of civil liberties advocates, of technologists and computer security experts appeared to be dwarfed by the scale and resources of the DoD, the chapters each showed processes of contestation and internal competition that point to the contingency of the security imaginaries discussed therein.

Each chapter critically analysed the multiple imaginaries concerned with articulating the vulnerabilities of the networked nation. As we saw, these insecurities were typically represented in terms of blurred national boundaries, blurred domestic and external boundaries, blurred boundaries between peacetime espionage and offensive hacking capabilities, blurred public and private spheres, blurred or limited boundaries of disclosures. If the security imaginary is that part of the social imaginary that frames understanding of the security world and thus makes specific security practices possible (Pretorius, 2008, p. 117), then the chapters showed how each of these imaginaries framed the initiatives, programs and boundary work that followed.

Boundaries are not essential categories or 'things' in the world, so it would be paradoxical for this thesis to end with a definitive statement of how boundaries have been reconstituted, and in what ways. It is hardly possible to say that boundary work concerned with such a specific set of policy matters in US politics has radically reconfigured notions of public or private spheres. However, what this thesis has sought to show is the ways that such boundary distinctions have served as productive resources for those seeking to make 'cybersecurity' amenable to state orientation, direction and governance (or indeed as a resource to challenge those efforts). In some important respects, we have seen how cyberspace has put all kinds of distinctions up for grabs, that the materiality of cyberspace in some important ways has challenged historically resonant and institutionalised boundaries. At the same time, some boundaries have an historical salience, a culturally specific 'baggage' that mean even

the most well-resourced and determined actors have not (yet) been able to challenge or reconfigure their political salience: history matters, shaping visions of desirable futures.

Thus, in Chapter Three we saw a mix of competitive and collaborative boundary work that sought to make computer hacking capabilities fit within legal, normative and institutionalised distinctions that have traditionally governed distinctions between wartime and peacetime activities, and military and intelligence agency remits. In this instance, organisational boundaries were reconstituted to fit the technologies, but institutionalised boundaries governing military activities were also reconstituted in turn to make the cyber command work beyond its DoD networks.

In Chapter Four, competitive boundary work that policed categorical distinctions of 'external security,' and 'internal security' and 'homeland' worked to embed into technical and organisational infrastructure visions and goals that dissented from those of the DoD's. Such distinctions were co-produced between programs and boundary work, where programs and organisations were designed to enact boundaries which in turn informed boundaries and programs. DHS actors were thus able to 'domesticate' cybersecurity by shifting the focus onto managing the nation's *internal* vulnerabilities through a risk-based framing rather than the DoD's focus on the *external* agency of threats. This chapter has highlighted that rather than being reconfigured in cybersecurity politics, historically resonant distinctions concerned with bordering the nation state and drawing out the boundaries of where military actions are permissible were reconstituted (as in, reproduced) in the context of US cybersecurity policies. Here the DHS and others were largely successful in challenging the DoD's imaginaries, despite their overbearing resources.

In Chapter Five, the distribution of cyberspace infrastructures amongst a range of non-government entities triggered configurational boundary work by federal actors. Here, cyberspace and cybersecurity were articulated as a challenge to the state's 'traditional' role as security provider, so that government actors used their articulation of distinctions between 'public' and 'private' to configure and *orchestrate* actors towards producing cybersecurity as a public good. However, as we saw, not all actors acquiesced to those official problem framings and mobilisation efforts in the case of Apple, while other corporate actors undertook collaborative boundary work to materially benefit from those reconfigurations. In this chapter, distinctions of public and private have not been reconstituted so much as reconfigured, so that political authority has been unbundled rather than simply shifted. Government actors have sought to empower a range of non-government actors, but generally this has been to the benefit of corporations like Mandiant and other security companies. This chapter reinforces the findings of other critical security scholars who have found that corporate interests and commercial logics on the one hand, and those of public 'national interest' on the other,

are not mutually exclusive rationalities in the US – configurational boundary work by federal actors and congressional interests showed the two are often mutually informed in official discourses.

Chapter Six found that the retention of software and hardware vulnerabilities for exploitation in the course of law enforcement, intelligence and military activities would challenge distinctions government actors made between cybersecurity and national security. 'Disclosure' thus became the locus for competitive boundary work that sought to preserve the autonomy of these federal agencies to use vulnerabilities. Over time, and in response to outside criticisms, we saw in this chapter that how government actors set the bounds of disclosure changed, partially accommodating competing imaginaries in order to rationalise and legitimise the institutionalised use of vulnerabilities. However, while what counted as 'disclosure' was expanded and reconfigured by the VEP in procedural terms, in other ways, 'disclosure' was used or enacted in ways intended to minimise any substantive alternatives to the government's use of vulnerabilities. Disclosure thus acted as a way of redirecting political attention, a category fundamentally unchanged by government claims to transparency, accountability and responsibility.

This final chapter, and the thesis, thus concludes that what cybersecurity 'is,' how its boundaries are drawn, has depended upon on the pragmatic utility of any given borders or boundaries for the protection, expansion or denial of political authority. With this analytical lens we saw how cybersecurity is emergent, a thing of boundaries, and boundary work has been concerned with getting different (often incommensurate) versions and security imaginaries 'hang together' (Mol, 2002). Cybersecurity – like the boundaries it is made up from – is an epiphenomenon of boundary work. For both, their characteristics and traits are contingent, context dependent, and culturally significant. The visions and versions of cybersecurity sketched in this project are also culturally specific: different countries will come down on different answers, and actors in those countries will undertake boundary work differently to the US, according to their specific legal, institutional, organisational, and social peculiarities. For example, because of the ways that distinctions of public and private mean different things, or the ways that a particular country's military or intelligence agencies are particularly powerful or differentially arranged, these suggest the ways that culturally specific boundary work will result in different configurations, settling controversies along different knife edges. The findings in this project show that this boundary work is not necessarily intentional or instrumental either, just a result of aggregated social, cultural, institutional 'common-sense' factors feeding into boundary work.

This suggests where future research would be productive: it is hoped that the analytical and methodological framework advanced by this project would provide the basis for comparative research into other national contexts on the topic of 'cybersecurity', or indeed act as a useful heuristic for critically unpacking the fraught political processes surrounding any number of other matters of

'security' that may be essentially contested. Furthermore, the 'boundary work' framework outlined here could be fruitfully utilised for investigating the emergent and fraught relations amongst non-government actors involved in devising 'cybersecurity' policies and practices, such as standards organisations, civil society, infrastructure operators and corporate security firms amongst others. Utilising this framework could contribute to a wider project of understanding cybersecurity 'in translation' across those different national, organisational, and procedural contexts too. In contrast to approaches like this project that have sought to point to how contested or apparently meaningless the term 'cybersecurity' is, concerned as it has been with tracing the narrative and socio-technical processes of people trying to make sense of, and draw the conceptual and political boundaries of this category 'cybersecurity' as a relatively passive entity, the boundary work framework could also investigate the work this term does as an active entity, perhaps treating the term itself like a 'mutable mobile' (Law and Mol, 2001) with its own political economy, and perhaps even agency. This boundary work framework could investigate the work the term does as it travels, moves, is clicked, circulated and also how it gets anchored to particular locations and centres of technological production and exchange. This could begin to trace, or map, the commercial, political, economic and circulatory value of a term as an abstracted entity, akin to tracing a 'data journey' (Bates, Lin and Goodale, 2016).

Each chapter has been just a small window into these complicated processes of meaning-making. The thesis has showcased its boundary work framework through some critical insights and moments as evidence of the overall argument that cybersecurity is all about boundary work that has sought to make cyberspace legible in ways that make it amenable to state governance, sometimes more successfully producing those federal goals than at others. This is important because, rather than being overdetermined by technologies or strategic imperatives, this project has shown how cybersecurity is processual, emerging at the point of fraught processes of social, bureaucratic, legal, cultural and technical boundary work.

References

Abbott, A. (1995) 'Things of boundaries', *Social Research*, 62(4), pp. 857–882. Available at: https://www.jstor.org/stable/40971127.

Abbott, K. W. *et al.* (2016) 'Two Logics of Indirect Governance: Delegation and Orchestration', *British Journal of Political Science*, 46(4), pp. 719–729. doi: 10.1017/S0007123414000593.

Agre, P. E. (2002) 'Cyberspace As American Culture', *Science as Culture*, 11(2), pp. 171–189. doi: 10.1080/09505430220137234.

Aitel, D. (2016) *The value of an 0day stockpile to the country versus the value of feeling self-righteous. February 12, 2016.*, *CyberSecPolitics blog*. Available at: https://perma.cc/KT8L-AEHK (Accessed: 28 February 2021).

Alexander, K. (2011) *'AFCEA HS-General Alexander Keynote-Feb 2011'*, *YouTube*. YouTube. Available at: https://perma.cc/3B7V-DD26 (Accessed: 28 February 2021).

Allen, D. (2000) 'Doing Occupational Demarcation', *Journal of Contemporary Ethnography*, 29(3), pp. 326–356. doi: 10.1177/089124100129023936.

Amoore, L. (2006) 'Biometric borders: Governing mobilities in the war on terror', *Political Geography*, 25, pp. 336–351. doi: 10.1016/j.polgeo.2006.02.001.

Amoore, L. and de Goede, M. (2005) 'Governance, risk and dataveillance in the war on terror', *Crime, Law and Social Change*, 43, pp. 149–173. doi: 10.1007/s10611-005-1717-8.

Anderson, B. (2006) *Imagined communities: Reflections on the origin and spread of nationalism*. London: Verso Books.

Andress, J. (2014) *The basics of information security: understanding the fundamentals of InfoSec in theory and practice.* Waltham, MA: Syngress.

Apple (2016) *Answers to your questions about Apple and security*, *Apple.com*. Available at: https://perma.cc/4Y32-H7UY (Accessed: 28 February 2021).

Apuzzo, M. (2016) 'FBI Used Hacking Software Decade Before iPhone Fight', *The New York Times*, 13 April. Available at: https://perma.cc/ZW5H-5992 (Accessed: 12 July 2021).

Aradau, C. (2010) 'Security That Matters: Critical Infrastructure and Objects of Protection', *Security Dialogue*, 41(5), pp. 491–514. doi: 10.1177/0967010610382687.

Armerding, T. (2013) *Mandiant gains instant fame after Chinese hack report*, *CSO.com*. Available at: https://perma.cc/8VSG-EWJD (Accessed: 28 February 2021).

Arquilla, J. and Ronfeldt, D. (1993) 'Cyberwar is coming!', *Comparative Strategy*, 12(2), pp. 141–165. doi: 10.1080/01495939308402915.

Austin, J. L. (2017) 'We have never been civilized: Torture and the materiality of world political binaries', *European Journal of International Security*, 23(1), pp. 49 –73. doi: 10.1177/1354066115616466.

Baldwin, D. (1997) 'The Concept of Security', *Review of International Studies*, 23(1), pp. 5–26. doi: 10.1017/S0260210597000053.

Ball, J., Borger, J. and Greenwald, G. (2013) *Revealed: how US and UK spy agencies defeat internet privacy and security*, *The Guardian*. Available at: https://perma.cc/UM2H-QGBQ (Accessed: 28 February 2021).

Balzacq, T. (2005) 'The Three Faces of Securitization: Political Agency, Audience and Context', *European Journal of International Relations*, 11(2), pp. 171–201. doi: 10.1177/1354066105052960.

Balzacq, T. (2014) 'Legitimacy and the "logic" of security', in Balzacq, T. (ed.) *Contesting Security: Strategies and Logics*. London: Routledge, pp. 1–10.

Bankston, K. and Wilson, A. (2017) *OTI Applauds Introduction of the PATCH Act*, *Open Technology Institute, New America*. Available at: https://perma.cc/Y63Q-RGVN (Accessed: 5 September 2020).

Banusiewicz, J. D. (2011) *Lynn Outlines New cybersecurity Effort*, *DoD News*. Available at: https://perma.cc/2XHE-UY53 (Accessed: 22 May 2020).

Barad, K. (1998) 'Getting Real: Technoscientific Practices and the Materialization of Reality', *differences: A Journal of Feminist Cultural Studies*, 10(2), pp. 87–128.

Barnard-Wills, D. and Ashenden, D. (2012) 'Securing Virtual Space: Cyber War, Cyber Terror, and Risk', *Space and Culture*, 15(2), pp. 110–123. doi: 10.1177/1206331211430016.

Barry, A. (2001) 'The Political and the Technical', in *Political Machines: Governing a Technological Society*. Londan and New York: Athlone Press, pp. 1–34.

Barry, A. (2013) 'The Translation Zone: Between Actor-Network Theory and International Relations', *Millennium - Journal of International Studies*, 41(3), pp. 413–429. doi: 10.1177/0305829813481007.

Bates, J., Lin, Y. and Goodale, P. (2016) 'Data journeys : Capturing the socio-material constitution of data objects and flows', (December), pp. 1–12. doi: 10.1177/2053951716654502.

BBC (2020) *Windows 10: NSA reveals major flaw in Microsoft's code 14*, *BBC News Online*. Available at: https://perma.cc/VZ7B-7LUZ (Accessed: 28 February 2021).

Beaulieu, A., Scharnhorst, A. and Wouters, P. (2007) 'Not another case study: A middle-range interrogation of ethnographic case studies in the exploration of e-science', *Science Technology and Human Values*, 32(6), pp. 672–692. doi: 10.1177/0162243907306188.

Beckstrom, R. (2009) *Beckstrom Resignation Letter*. Available at: https://perma.cc/89RP-3GBV (Accessed: 28 February 2021).

Bejtlich, R. (2015) *Will Sharing Cyberthreat Information Help Defend the United States?*, *Brookings*. Available at: https://perma.cc/S87C-ZJZ4 (Accessed: 2 December 2019).

Bellanova, R., Jacobsen, K. L. and Monsees, L. (2020) 'Critical Studies on Security Taking the trouble : science , technology and security studies', *Critical Studies on Security*. Routledge, 8(2), pp. 87–100. doi: 10.1080/21624887.2020.1839852.

Berling, T. V. (2011) 'Science and securitization: Objectivation, the authority of the speaker and mobilization of scientific facts', *Security Dialogue*, 42(4–5), pp. 385–397. doi: 10.1177/0967010611418714.

Betz, D. J. and Stevens, T. (2013) 'Analogical reasoning and cyber security', *Security Dialogue*, 44(2), pp. 147–164. doi: 10.1177/0967010613478323.

Bigo, D. (2001) 'The Mobius Ribbon of Internal and External Security(ies)', in Albert, M., Jacobson, D., and Lapid, J. (eds) *Identities, Borders, Orders. Rethinking International Relations Theory*. Minneapolis, MN: University of Minnesota Press, pp. 91–116.

Bijker, W. E. (2006) 'The vulnerability of technological culture', in Nowotny, H. (ed.) *Cultures of Technology and the Quest for Innovation (Vol. 9)*. New York, Oxford: Berghahn Books, pp. 52–72.

Bijker, W. E., Hughes, T. P. and Pinch, T. (eds) (2012) *The social construction of technological systems: New directions in the sociology and history of technology*. 2nd edn. Cambridge, Ma.: MIT Press.

Bing, C. (2016) *U.S. Cyber Command director: We want 'loud,' offensive cyber tools*, *FedScoop*. Available at: https://perma.cc/5KHC-XEMV (Accessed: 28 February 2021).

Bing, C. (2017) *Trump administration will shine light on vulnerability disclosure with public charter - CyberScoop*, *CyberScoop*. Available at: https://perma.cc/GSR8-34JQ (Accessed: 28 February 2021).

Bing, C. (2018) *Command and control: A fight for the future of government hacking*, *CyberScoop*. Available at: https://perma.cc/M9QJ-47EW (Accessed: 28 February 2021).

Birchall, C. (2011) '"There's Been Too Much Secrecy in This City": The False Choice Between Secrecy and Transparency in US Politics', *Cultural Politics: an International Journal*, 7(1), pp. 133–156. doi: 10.2752/175174311X12861940861905.

Borghard, E. D. and Lonergan, S. W. (2019) 'Cyber Operations as Imperfect Tools of Escalation', *Strategic Studies Quarterly*, 13(3), pp. 122–145. doi: 10.2307/26760131.

Borup, M. *et al.* (2006) 'The sociology of expectations in science and technology', *Technology Analysis and Strategic Management*, 18(3–4), pp. 285–298. doi: 10.1080/09537320600777002.

Bossong, R. and Wagner, B. (2016) 'A typology of cybersecurity and public-private partnerships in the context of the European Union', *Crime, Law and Social Change*. Crime, Law and Social Change, pp. 219–247. doi: 10.1007/978-3-319-63010-6_10.

Bourdieu, P. (1980) *The Logic of Practice*. Stanford, CA.: Stanford University Press.

Bourdieu, P. (1991) 'The peculiar history of scientific reason', *Sociological Forum*, 6(1), pp. 3–26. doi: 10.1007/BF01112725.

Bourdieu, P. (2014) *On the State*. Malden, MA: Polity Press.

Boutrous Jr, T. J., Hanna, N. and Vandevelde, E. (2016) 'Apple Inc.'s Motion To Vacate Order Compelling Apple Inc. To Assist Agents in Search, and Opposition To Government's Motion To Compel Assistance', pp. 1–32. Available at: https://perma.cc/E2JP-SERC.

Bouwman, X. *et al.* (2020) 'A different cup of TI? The added value of commercial threat intelligence', *29th USENIX Security Symposium*. Available at: https://perma.cc/JS2V-FAKB.

Bowker, G. C. and Star, S. L. (2000) *Sorting things out: Classification and its consequences.* Harvard: MIT Press.

Boyd, A. (2019) *Trump's 2020 Budget Requests About $11 Billion For Cyber Defense and Operations*, *NextGov.com*. Available at: https://perma.cc/P3W3-2H52 (Accessed: 28 February 2021).

Branch, J. (2020) 'What's in a Name? Metaphors and Cybersecurity', *International Organization*. doi: 10.1017/S002081832000051X.

Bratich, J. (2006) 'Public secrecy and immanent security: A strategic analysis', *Cultural Studies*, 20(4–5), pp. 493–511. doi: 10.1080/09502380600708937.

Braun, V. and Clarke, V. (2019) 'Reflecting on reflexive thematic analysis', *Qualitative Research in Sport, Exercise and Health*. Routledge, 11(4), pp. 589–597. doi: 10.1080/2159676X.2019.1628806.

Braun, V., Clarke, V. and Gray, D. (eds) (2017) *Collecting Qualitative Data*. Cambridge: Cambridge University Press. doi: 10.1017/9781107295094.

Brito, J. and Watkins, T. (2014) 'Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy', *Harvard National Security Journal*, 3. doi: 10.1525/sp.2007.54.1.23.

Brunner, E. M. (2013) *Foreign Security Policy, Gender, and US Military Identity*. London: Palgrave Macmillan.

Brunner, E. M. and Dunn Cavelty, M. (2009) 'The formation of in-formation by the US military: articulation and enactment of infomanic threat imaginaries on the immaterial battlefield of perception', *Cambridge Review of International Affairs*, 22(4), pp. 629–646. doi: 10.1080/09557570903325454.

Buchanan, B. (2016) *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford: Oxford University Press.

Bures, O. and Carrapico, H. (2018) *Private security beyond private military and security companies: exploring Diversity within private–public Collaborations and its consequences for security governance*, *Security Privatization*. Edited by Oldrich Bures and Helena Carrapico. Cham: Springer International Publishing. doi: 10.1007/978-3-319-63010-6.

Burr, R. and Feinstein, D. (2016) *Compliance with Court Orders Act of 2016 discussion draft*. Available at: https://perma.cc/V7WZ-PY9F (Accessed: 28 February 2021).

Buzan, B., de Wilde, J. and Wæver, O. (1998) *Security: a New framework for analysis*. Boulder, CO.: Lynne Rienner.

Campbell, D. (1998) *Writing Security: United States Foreign Policy and the Politics of Identity (Revised Edition)*. Minneapolis: University of Minnesota Press.

Campbell, E. (2016) 'Policing and its spatial imaginaries', *Journal of Theoretical and Philosophical Criminology*, 8, pp. 71–89. Available at: https://core.ac.uk/download/pdf/327340464.pdf.

Carberry, S. D. (2017) *Why disclosure rules didn't prevent the WannaCry attack*, *FCW.com*. Available at: https://perma.cc/A6G9-7BWV (Accessed: 28 February 2021).

Carney, T. P. (2011) *Carney: The rise of the cybersecurity-industrial-complex*, *Washington Examiner*. Washington, D.C. Available at: https://perma.cc/VF34-XWPN (Accessed: 28 February 2021).

Carr, M. (2016) 'Public-private partnerships in national cyber-security strategies', *International Affairs*, 1, pp. 190–209. doi: 10.1111/1468-2346.12504.

Carroll, P. (2006) *Science, culture, and modern state formation*. Los Angeles: University of California Press.

Carroll, P. (2009) 'Articulating theories of states and state formation: Issues and agenda', *Journal of Historical Sociology*, 22(4), pp. 553–603. doi: 10.1111/j.1467-6443.2009.01369.x.

Carroll, P. (2012) 'Water and technoscientific state formation in California', *Social Studies of Science*, 42(4), pp. 489–516. doi: 10.1177/0306312712437977.

Carter, A. (2017) *Belfer Center Report. A Lasting Defeat: The Campaign to Destroy ISIS*. Available at: https://perma.cc/6T75-3AR7.

CDT (2016) *Response and Recommendations For the Digital Security Commission Act of 2016*, *Center for Democracy and Technology*. Available at: https://perma.cc/T49J-XN7K.

Cebrowski, A. (2004) 'Transformation and The Changing Character of War', *Transformation Trends*. Available at: https://perma.cc/B6AC-D3T5.

Chabinsky, S. (2014) 'Testimony of Steven R. Chabinsky Before the United States Senate Committee on Homeland Security and Governmental Affairs "Strengthening Public-Private Partnerships to Reduce Cyber Risks to our Nation's Critical Infrastructure"'. Available at: https://perma.cc/PY7L-MHSF.

Chairman of the Joint Chiefs of Staff (2000) *Joint Vision 2020 America's Military: Preparing for tomorrow*. Available at: https://perma.cc/TDS8-XNPT.

Chairman of the Joint Chiefs of Staff (2006) *National Military Strategy for Cyberspace Operations*. Available at: https://perma.cc/F34V-LCUS.

Chappellet-Lanier, T. (2017) *HHS CISO Chris Wlaschin on the importance of cyber-hygiene*, *FedScoop*. Available at: https://perma.cc/AY6Z-BDAS (Accessed: 28 February 2021).

Chun, W. H. K. (2008) 'On "Sourcery," or Code as Fetish', *Configurations*, 16(3), pp. 299–324. doi: 10.1353/con.0.0064.

CISA (2020a) *CISA Cybersecurity*, *Cybersecurity and Infrastructure Agency*. Available at: https://perma.cc/2YUU-5XKH (Accessed: 30 October 2020).

CISA (2020b) *EINSTEIN*, *Critical infrastructure Security Agency*. Available at: https://perma.cc/3HWB-B68U (Accessed: 18 May 2020).

Civaner, F. (2020) *Real-Life Software Security Vulnerabilities And What You Can Do To Stay Safe*, *Hacker Noon*. Available at: https://perma.cc/F7G9-GHMA (Accessed: 28 February 2021).

Clarke, R. A. *et al.* (2013) *Liberty and Security in a Changing World: President's Review Group on Intelligence and Communications Technologies*, *Berkeley Technology Law Journal UNC Legal Studies Research Paper*. doi: 10.3390/molecules14072573.

Clarke, V., Braun, V. and Hayfield, N. (2015) 'Thematic analysis', in Smith, J. A. (ed.) *Qualitative psychology: A practical guide to research methods*. Third Edit. London: Sage Publications, pp. 222–248.

Coburn, S. T. (2015) *A review of the department of homeland security's missions and performance*, *The Department of Homeland Security: Assessment, Recommendations, and Appropriations*. Available at: https://perma.cc/5WKZ-5UZR.

Collier, J. (2018) 'Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision', *Politics and Governance*, 6(2), pp. 13–21. doi: 10.17645/pag.v6i2.1324.

Collier, S. J. . and Lakoff, A. (2008) 'The Vulnerability of Vital Systems: How "Critical Infrastructure" Became a Security Problem', in Dunn, M. A. and Søby Kristensen, K. (eds) *The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation*. London: Routledge, pp. 1–33.

Committee on National Security Systems (2015) 'CNSSI 4009 - Glossary', (4009). Available at: https://perma.cc/ZP5S-DYFH.

Conger, K. (2016) *Burr-Feinstein encryption bill is officially here in all its scary glory*, *Tech Crunch*. Available at: https://perma.cc/NYD5-HXHT (Accessed: 28 February 2021).

Cook, T. (2016) *A Message to Our Customers*, *Apple.com*. Available at: https://perma.cc/S3KB-Y8HC (Accessed: 29 October 2019).

Corrin, A. (2012) *DOD to expand public-private cybersecurity project*, *FCW.com*. Available at: https://perma.cc/4J3X-GPQA (Accessed: 28 February 2021).

Cox, J. (2016) *What Happens When the FBI Discovers a Software Security Flaw? An Explainer*, *Vice*. Available at: https://perma.cc/9J8H-MDWS (Accessed: 21 January 2021).

Cox, J. (2018) *How US Military Hackers Prepared to Hack the Islamic State*, *Motherboard (Vice)*. Available at: https://perma.cc/9HX6-DU38 (Accessed: 28 February 2021).

Crocker, A. and Galperin, E. (2014) *EFF Sues NSA , Director of National Intelligence for Zero Day Disclosure Process*, *Electronic Frontier Foundation*. Available at: https://perma.cc/JLG2-4399 (Accessed: 28 February 2021).

Crotty, M. (1998) *The Foundations of Social Research: Meaning and perspective in the research process*. London: Sage Publications. doi: 10.1007/BF00485444.

CYBERCOM (2018) *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. Available at: https://perma.cc/47T3-YD4S.

CYBERCOM (2019) *CYBERCOM Media Roundtable, May 7 2019*. Fort Meade, Maryland. Available at: https://perma.cc/NKS5-WF4H.

Czelusta, M. G. (2008) *EUROPEAN CENTER FOR SECURITY STUDIES Occasional Paper Series Business as Usual: An Assessment of Donald Rumsfeld's Transformation Vision and Transformation's Prospects for the Future*. 18. Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a484266.pdf.

Daniel, M. (2014) *Heartbleed: Understanding when we disclose cyber vulnerabilities*, *White House*. Available at: https://perma.cc/HG36-JGNW (Accessed: 3 October 2018).

Dean, J. (2004) 'Secrecy since september 11', *Interventions*, 6(3), pp. 362–380. doi: 10.1080/1369801042000280023.

Deibert, R. J. and Rohozinski, R. (2010) 'Risking Security: Policies and Paradoxes of Cyberspace Security', *International Political Sociology*, 4(1), pp. 15–32. doi: 10.1111/j.1749-5687.2009.00088.x.

Delina, L. and Janetos, A. (2018) 'Cosmopolitan, dynamic, and contested energy futures: Navigating the pluralities and polarities in the energy systems of tomorrow', *Energy Research and Social Science*. Elsevier, 35(December 2017), pp. 1–10. doi: 10.1016/j.erss.2017.11.031.

Denning, D. E. (2003) 'Cyber Security as an Emergent Infrastructure', in Irvine, C. and Armstrong, H. (eds) *Security Education and Critical Infrastructures: IFIP TC11 / WG11.8 Third Annual World Conference on Information Security Education (WISE3) June 26–28, 2003, Monterey, California, USA*. Springer, pp. 1–19.

Department of Homeland Security (2007) *National Preparedness Guidelines*. Available at: https://perma.cc/XVT6-HBCZ.

Department of Homeland Security (2015) *National Preparedness Goal Second Edition*. Available at: https://perma.cc/9MBQ-AYVY.

Deppisch, B. (2019) 'Politico DHS Was Finally Getting Serious About Cybersecurity. Then Came Trump.', *Politico*, 18 December. Available at: https://perma.cc/RMG8-EHSM (Accessed: 28 February 2021).

DHS (2002) *National Strategy for Homeland Security*. Available at: https://perma.cc/29VN-W342.

DHS (2003) *The Physical Protection of Critical Infrastructures and Key Assets*. Available at: https://perma.cc/PAL3-4UMM.

DHS (2008) *One Team, One Mission, Securing Our Homeland*. Available at: https://perma.cc/UT47-JCMU.

DHS (2011) *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise*, *U.S. Department of Homeland Security*. Available at: https://perma.cc/9QCZ-N4XE.

DHS (2013) *CONTINUOUS DIAGNOSTICS & MITIGATION PROGRAM*. Available at: https://perma.cc/N6JY-9UFP.

DHS (2020) *CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM) (Original release date: August 12, 2013; Last revised: March 13, 2020)*, *Cybersecurity and Infrastructure Security Agency*. Available at: https://perma.cc/WE4L-VPWZ.

DHS Inspector General (2014) *Implementation Status of EINSTEIN 3 Accelerated*. Available at:

https://perma.cc/2QJU-VPQJ.

Dunn Cavelty, M. (2007) *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age.* London: Routledge.

Dunn Cavelty, M. (2013) 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse', *International Studies Review*, 15(1), pp. 105–122. doi: 10.1111/misr.12023.

Dunn Cavelty, M. (2018) 'Cybersecurity Research Meets Science and Technology Studies', *Politics and Governance*, 6(2), pp. 22–30. doi: 10.17645/pag.v6i2.1385.

Dunn Cavelty, M. and Leese, M. (2019) 'Politicising Security at the Boundaries: Privacy in Surveillance and Cybersecurity', *ERIS – European Review of International Studies*, 5(3–2018), pp. 49–69. doi: 10.3224/eris.v5i3.03.

Dunn Cavelty, M. and Wenger, A. (2020) 'Cyber security meets security politics: Complex technology, fragmented politics, and networked science', *Contemporary Security Policy*. Taylor & Francis, 41(1), pp. 5–32. doi: 10.1080/13523260.2019.1678855.

Ebert, H. and Maurer, T. (2013) 'Contested Cyberspace and Rising Powers', *Third World Quarterly*, 34(6), pp. 1054–1074. doi: 10.1080/01436597.2013.802502.

Edwards, P. N. (1996) *The Closed World: Computers and the Politics of Discourse in Cold War America.* Cambridge, Ma.: MIT Press.

Egloff, F. J. (2020) 'Contested public attributions of cyber incidents and the role of academia', *Contemporary Security Policy*, 41(1), pp. 55–81. doi: 10.1080/13523260.2019.1677324.

Eichensehr, K. E. (2017) 'Public-Private Cybersecurity', *Texas Law Review*, 95, p. 467. doi: 10.3868/s050-004-015-0003-8.

Electronic Frontier Foundation (2016) *Notice of Motion and Cross Motion for Summary Judgement and Opposition to Defendants' Motion for Summary Judgement, 18th February 2016*, *United States District court for the Northern District of California, San Francisco Division*. Available at: https://perma.cc/R4GV-2D8Q.

ESET (2016) *En Route with Sednit*. Available at: https://perma.cc/K9PF-F98S.

EUROPOL (2017) *Wannacry Ransomware*, *EUROPOL EC3*. Available at: https://perma.cc/HQ42-9NB5 (Accessed: 29 July 2020).

Evans, M. S. (2009) 'Defining the public, defining sociology: Hybrid science-public relations and boundary-work in early American sociology', *Public Understanding of Science*, 18(1), pp. 5–22. doi: 10.1177/0963662506071283.

Evans, S. *et al.* (2020) *STS Research Platform Sociotechnical Imaginaries Methodological Pointers*, *Program on Science, Technology and Society at the Harvard Kennedy School of Government.* Available at: https://perma.cc/X2ND-Z4KL (Accessed: 21 November 2020).

Evans, S. W., Leese, M. and Rychnovská, D. (2020) 'Science, technology, security: Towards critical collaboration', *Social Studies of Science*, 00(00), pp. 1–25. doi: 10.1177/0306312720953515.

Executive Office of the President; OMB (2019) *A budget for a better America : fiscal year 2020 budget of the U.S. government*. Government Publishing Office. Available at: https://perma.cc/8C52-LL5B.

Executive Office of the President of the United States (2013) *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*. Available at: https://perma.cc/6FFQ-J8JD.

FBI (2011) *Federal Bureau of Investigation Situational Information Report, Cyber Activity Alert, Going Dark: Law Enforcement Problems in Lawful Surveillance*. Albany, New York, New York. Available at: https://perma.cc/BGL9-FCJC.

Feenberg, A. (2002) *Transforming Technology: A Critical Theory Revisited*. Oxford: Oxford University Press.

Feinstein, D. (2016) *Intelligence Committee Leaders Release Discussion Draft of Encryption Bill*, *feinstein.senate.gov*. Available at: https://perma.cc/9ZKQ-CW4K (Accessed: 29 November 2019).

Felt, U. *et al.* (2017) *The Handbook of Science and Technology Studies*. Fourth. Cambridge, Ma.: MIT Press.

Fenster, M. (2015) 'Transparency in search of a theory', *European Journal of Social Theory*, 18(2), pp. 150–167. doi: 10.1177/1368431014555257.

Finkle, J. (2014) *FireEye buys cyber forensics firm Mandiant for about $1 billion*, *Reuters*. Available at: https://perma.cc/65FA-DW5P (Accessed: 28 February 2021).

Finkle, J. (2020) *Mandiant goes viral after China hacking report*, *Reuters*. Available at: https://perma.cc/S36P-MA36 (Accessed: 28 February 2021).

Finklea, K. (2016) 'Encryption and the "going dark" debate', *CRS Reports*, p. 21 pages. Available at: https://www.everycrsreport.com/files/20170125_R44481_640e6b18cd637ca6dd5a9f22271bb1914eea0ad4.pdf.

Fischer, E. A. (2016) *Cybersecurity issues and challenges: In Brief*, *Congressional Research Service*. Washington, D.C. Available at: https://perma.cc/SCJ7-77HF.

Fischerkeller, M. P. and Harknett, R. J. (2018) *Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace*, *Lawfare Blog*. Available at: https://perma.cc/Y9E4-KKY5 (Accessed: 10 March 2021).

Fitzgerald, M. (2003) *Homeland Cybersecurity Efforts Doubted*, *SecurityFocus*. Available at: https://perma.cc/Z7LX-TG8B (Accessed: 28 February 2021).

Flaherty, A. (2013) *A look at Mandiant , allegations on China hacking*, *Associated Press*. Available at: https://perma.cc/VP5A-WRNJ (Accessed: 28 February 2021).

Fuller, M. (2003) *Behind the Blip*. New York: Autonomedia.

Futter, A. (2018) '"Cyber" semantics: why we should retire the latest buzzword in security studies', *Journal of Cyber Policy*, 3(2), pp. 201–216. doi: 10.1080/23738871.2018.1514417.

General Accountability Office (2016) 'DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System', (January). Available at: https://perma.cc/JJ7P-F3CT.

Genschel, P. and Zangl, B. (2017) 'The Rise of Non-State Authority and the Reconfiguration of the State', in King, D. and Le Galès, P. (eds) *Reconfiguring European States in Crisis*. Oxford: Oxford University Press.

Georgieva, I. (2020) 'The unexpected norm-setters: Intelligence agencies in cyberspace', *Contemporary Security Policy*. Taylor & Francis, 41(1), pp. 33–54. doi: 10.1080/13523260.2019.1677389.

Gieryn, T. F. (1983) 'Boundary-Work and the Demarcation of Science from Non-Science: Strains and Interests in Professional Ideologies of Scientists', *American Sociological Review*, 48(6), p. 781. doi: 10.2307/2095325.

Gieryn, T. F. (1995) 'Boundaries of science', in Jasanoff, S. et al. (eds) *Handbook of Science and Technology Studies (Revised Edition)*. Thousand Oaks: Sage, pp. 393–443.

Gieryn, T. F. (1999) *Cultural Boundaries of Science: Credibility on the Line*. Chicago: University of Chicago Press.

Giles, K. and Hagestad, W. (2013) 'Divided by a common language: Cyber definitions in Chinese, Russian and English', *International Conference on Cyber Conflict, CYCON*. Available at: https://perma.cc/GV9J-JT6E.

Godwin III, J. B. *et al.* (2014) 'Critical Terminology Foundations 2 Russia-U.S. Bilateral on Cybersecurity Policy Report', *EastWest Institute and the Information Security Institute of Moscow State University*, 2, pp. 1–82. Available at: https://perma.cc/H7KN-CD4A.

de Goede, M. (2020) 'Critical Studies on Security Engagement all the way down', *Critical Studies on Security*. Routledge, 00(00), pp. 1–15. doi: 10.1080/21624887.2020.1792158.

Gooding, M. (2020) *Exim Vulnerability: GRU Widely Exploited Critical 2019 Bug, Warns NSA*, *cbronline.com*. Available at: https://perma.cc/4W79-L8DS (Accessed: 28 February 2021).

Government Accountability Office (2010) *Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, *Report to Congressional Requesters*. Available at: https://perma.cc/RG5Z-4EHD.

Graham, S. and Thrift, N. (2007) 'Out of Order: Understanding Repair and Maintenance', *Theory, Culture & Society*, 24(3), pp. 1–25. doi: 10.1177/0263276407075954.

Gray, C. S. (2006) *Recognizing and understanding revolutionary change in warfare : the sovereignty of context*. Strategic Studies Institute and U.S. Army War College Press. Available at: https://perma.cc/69MF-5DMZ.

Hagmann, J., Hegemann, H. and Neal, A. (2019) 'The politicisation of security: Controversy, mobilisation, Arena Shifting', *European Review of International Studies*, 5, pp. 3–21. doi: 10.3224/eris.v5i3.0.

Halperin, M. H. and Clapp, P. (2007) *Bureaucratic politics and foreign policy*. Second Edi. Washington, D.C.: Brookings Institution Press.

Hansen, L. and Nissenbaum, H. (2009) 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53(4), pp. 1155–1175. doi: 10.1111/j.1468-2478.2009.00572.x.

Harris, S. (2014) *@War: The Rise of Cyber Warfare*. London: Headline.

Hayden, M. W. (2011) 'The Future of Things "Cyber"', *Strategic Studies Quarterly*, 5(1), pp. 3–7. Available at: https://perma.cc/VC9Z-YFKL.

Hayden, M. W. (2016) *Playing to the Edge: American Intelligence in the Age of Terror*. New York: Penguin Books (USA).

Hecht, G. (2009) *The radiance of France: Nuclear power and national identity after World War II*. Boston: MIT Press.

Hecht, G. and Edwards, P. N. (2007) *The technopolitics of Cold War: Toward a transregional perspective*. Washington, D.C.: American Historical Association.

Hellegren, Z. I. (2017) 'A history of crypto-discourse: encryption as a site of struggles to define internet freedom', *Internet Histories*. Taylor & Francis, 1(4), pp. 285–311. doi: 10.1080/24701475.2017.1387466.

Hennessey, S. (2016) *Good Defense is Good Offense: NSA Myths and the Merger*, *Lawfare*. Available

at: https://perma.cc/GP8B-TY5P (Accessed: 1 August 2020).

Henriksen, A. (2019) 'The end of the road for the UN GGE process: The future regulation of cyberspace', *Journal of Cybersecurity*, 5(1), pp. 1–9. doi: 10.1093/cybsec/tyy009.

Hofmann, M. and Timm, T. (2012) *"Zero-day" exploit sales should be key point in cybersecurity debate*, *Eff.Org*. Available at: https://perma.cc/ZPV9-LUUA (Accessed: 30 July 2020).

Hom, A. R. (2018) 'Timing is everything: Toward a better understanding of time and international politics', *International Studies Quarterly*, 62(1), pp. 69–79. doi: 10.1093/isq/sqx090.

Hopper, D. and Waldman, D. (2017) *How Washington evaluates software vulnerabilities*, *Christian Science Monitor*. Available at: https://perma.cc/3TNW-XAPY (Accessed: 28 February 2021).

Horn, E. (2011) 'Logics of Political Secrecy', *Theory, Culture & Society*, 28(8), pp. 103–122. doi: 10.1177/0263276411424583.

Hosenball, M. and Volz, D. (2016) *Exclusive: White House declines to support encryption legislation - sources*, *Reuters*. Available at: https://perma.cc/F3QG-9LHQ (Accessed: 28 February 2021).

Hudson, J. L. (2015) *Declaration of Jennifer L. Hudson, Director, Inofrmation Management Division, Office of the Chief Information Officer, Office of the Director of National Intelligence, 30th October 2015*, *United States District court for the Northern District of California, San Francisco Division*. Available at: https://perma.cc/H58T-2GK9.

Hudson, J. L. (2016) *Declaration of Jennifer L. Hudson, Director, Inofrmation Management Division, Office of the Chief Information Officer, Office of the Director of National Intelligence, 14th January, 2016*, *United States District court for the Northern District of California, San Francisco Division*. Available at: https://perma.cc/8554-LDLU.

Hutchby, I. (2001) 'Technologies, Texts and Affordances', *Sociology*, 35(2), pp. 441–456. doi: 10.1177/S0038038501000219.

Huysmans, J. (2002) 'Defining social constructivism in security studies: The normative dilemma of writing security', *Alternatives*, 27(1), pp. 41–62. doi: 10.1177/03043754020270s104.

Huysmans, J. (2006) 'International Politics of Insecurity: Normativity, Inwardness and the Exception', *Security Dialogue*, 37(1), pp. 11–29. doi: 10.1177/0967010606064134.

Huysmans, J. (2011) 'What's in an act? On security speech acts and little security nothings', *Security Dialogue*, 42(4–5), pp. 371–383. doi: 10.1177/0967010611418713.

Huysmans, J. (2014) *Security unbound: Enacting democratic limits*. London: Routledge.

Ilascu, I. (2020) *Critical Exim bugs being patched but many servers still at risk*, *Bleeping Computer*. Available at: https://perma.cc/VKM5-GCAM (Accessed: 28 February 2021).

Influence Watch (2019) *Center for Democracy and Technology (CDT)*, *InfluenceWatch.org*. Available at: https://perma.cc/QMV5-B2YG (Accessed: 29 November 2019).

Jaikaran, C. (2018) *DHS' s Cyber security Mission — An Overview*. Available at: https://perma.cc/ZEV2-55DY.

Jarvis, C. (2020) *Crypto Wars: The Fight for Privacy in the Digital Age: a Political History of Digital Encryption*. Boca Raton: CRC Press.

Jasanoff, S. (1987) 'Contested Boundaries in Policy-Relevant Science', *Social Studies of Science*, 17(2), pp. 195–230. doi: 10.1177/030631287017002001.

Jasanoff, S. (2004) 'Ordering Knowledge, Ordering Society', in Jasanoff, S. (ed.) *States of Knowledge:*

the Co-production of Science and the Social Order. London: Routledge, pp. 13–45.

Jasanoff, S. (2005) *Designs on Nature: Science and Democracy in Europe and the United States*. Princeton, N.J.: Princeton University Press.

Jasanoff, S. (2009) *The fifth branch: Science advisers as policymakers*. Harvard: Harvard University Press.

Jasanoff, S. (2015) 'Future Imperfect', in Jasanoff, S. and Kim, S. H. (eds) *Dreamscapes of modernity: Sociotechnical imaginaries and the fabrication of power*. Chicago: Chicago University Press, pp. 1–33.

Jasanoff, S. and Kim, S. H. (2009) 'Containing the atom: Sociotechnical imaginaries and nuclear power in the United States and South Korea', *Minerva*, 47(2), pp. 119–146. doi: 10.1007/s11024-009-9124-4.

Jasanoff, S. and Kim, S. H. (2015) *Dreamscapes of modernity: Sociotechnical imaginaries and the fabrication of power*. Chicago: Chicago University Press.

Jensen, E. T. (2010) 'Cyber warfare and precautions against the effects of attacks', *Texas Law Review*, 88(7), pp. 1533–1569.

Johnson, S. R. (2017) *Protecting our Ability to Counter Hacking 'PATCH' Act of 2017*, *United States Senate Committee on Homeland Security and Governmental Affairs*. Available at: https://perma.cc/2XUX-X7PN.

Jones-Imhotep, E. (2017) *The unreliable nation: Hostile nature and technological failure in the Cold War*. Cambridge, Ma., Mass.: MIT Press.

Jones, R. (2009) 'Categories, borders and boundaries', *Progress in Human Geography*, 33(2), pp. 174–189. doi: 10.1177/0309132508089828.

Jones, R. (2010) 'The spatiality of boundaries', *Progress in Human Geography*, 34(2), pp. 263–267. doi: 10.1177/0309132509340610.

Joyce, R. (2017) *Improving and Making the Vulnerability Equities Process Transparent is the Right Thing to Do*, *White House*. Available at: https://perma.cc/7ANC-PB2Z (Accessed: 23 January 2019).

Kaplan, F. (2016) *Dark territory: The secret history of cyber war*. New York: Simon and Schuster.

Kearns, O. (2017) 'Secrecy and absence in the residue of covert drone strikes', *Political Geography*. Elsevier Ltd, 57, pp. 13–23. doi: 10.1016/j.polgeo.2016.11.005.

Kello, L. (2013) 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft', *International Security*, 38(2), pp. 7–40. doi: 10.1162/ISEC_a_00138.

Kinchy, A. J. and Kleinman, D. L. (2003) 'Organizing Credibility', *Social Studies of Science*, 33(6), pp. 869–896. doi: 10.1177/0306312703336003.

Kinsella, W. J., Kelly, A. R. and Autry, M. K. (2013) 'Risk, Regulation, and Rhetorical Boundaries: Claims and Challenges Surrounding a Purported Nuclear Renaissance', *Communication Monographs*, 80(3), pp. 278–301. doi: 10.1080/03637751.2013.788253.

Koh, H. H. (2012) 'International Law in Cyberspace', *U.S. Department of State Diplomacy in Action*, p. 15. Available at: https://perma.cc/JL59-3T5C.

Konkel, F. (2019) *Inside the NSA's New Cybersecurity Directorate*, *NextGov.com*. Available at: https://perma.cc/P24R-YKAC (Accessed: 28 February 2021).

Konrad, K. *et al.* (2017) 'Performing and Governing the Future in Science and Technology', in Felt, U. et al. (eds) *The Handbook of Science and Technology Studies*. Cambridge, Ma.: MIT Press, pp. 464–

493.

LaGrone, S. (2012) *Retired General Cartwright on the History of Cyber Warfare*, *USNI*. Available at: https://perma.cc/P22N-J733 (Accessed: 28 February 2021).

Lakoff, A. and Collier, S. J. (2008) 'Distributed preparedness: The spatial logic of domestic security in the United States', *Environment and Planning D: Society and Space*, 26(1), pp. 7–28. doi: 10.1068/d446t.

Lamont, M. and Fournier, M. (eds) (1992) *Cultivating differences: Symbolic boundaries and the making of inequality.* Chicago: Chicago University Press.

Lamont, M. and Molnár, V. (2002) 'The Study of Boundaries in the Social Sciences', *Annual Review of Sociology*, 28(1), pp. 167–195. doi: 10.1146/annurev.soc.28.110601.141107.

Langevin, R. J. R. *et al.* (2008) *Securing Cyberspace for the 44th Presidency*, *A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. Available at: https://perma.cc/DYN3-LHMW.

Langley, A. *et al.* (2019) 'Boundary work among groups, occupations, and organizations: From cartography to process', *Academy of Management Annals*, 13(2), pp. 704–736. doi: 10.5465/annals.2017.0089.

Langley, A. and Tsoukas, H. (2017) *The Sage Handbook of Process Organization Studies*. London: Sage Publications.

Lapointe, A. (2011) 'When Good Metaphors Go Bad: The Metaphoric "Branding" of Cyperspace', *Center for Strategic & International Studies*, (July). Available at: https://perma.cc/A9FN-3TTF.

Lardner, R. (2002) 'After 40 Years at NSA, Bill Black is SIGINT World's Agent for Change', *Inside the Pentagon*, 18(27), pp. 1, 14–19.

Latour (2005a) 'From realpolitik to dingpolitik or how to make things public', *Human Relations*, 69(5), pp. 4–31. doi: 10.1177/0018726715600230.

Latour (2005b) *Reassembling the social: an introduction to actor-network-theory.* Oxford: Oxford University Press.

Latour, B. (2000) 'When Things Strike Back: A Possible Contribution of "Science Studies" to the Social Sciences', *British Journal of Sociology*, 51(1), pp. 107–123.

Latour, B. and Woolgar, S. (2013) *Laboratory life: The construction of scientific facts*. Princeton: Princeton University Press.

Law, J. (1992) 'Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity', *Systems Practice*. Kluwer Academic Publishers-Plenum Publishers, 5(4), pp. 379–393. doi: 10.1007/BF01059830.

Law, J. (2004) *After method: Mess in social science research*. London: Routledge.

Law, J. (2008) 'On sociology and STS', *Sociological Review*, 56(4), pp. 623–649. doi: 10.1111/j.1467-954X.2008.00808.x.

Law, J. (2017) 'STS as Method', in Felt, U. et al. (eds) *The Handbook of Science and Technology Studies*. Fourth. Cambridge, Ma.: MIT Press, pp. 31–58.

Law, J. and Mol, A. (2001) 'Situating technoscience : an inquiry into spatialities', 19, pp. 609–621. doi: 10.1068/d243t.

Law, J. and Singleton, V. (2005) 'Object lessons', *Organization*, 12(3), pp. 331–355. doi: 10.1177/1350508405051270.

Leander, A. (2008) 'The Power to Construct International Security: On the Significance of Private Military Companies', *Millennium: Journal of International Studies*, 33(3), pp. 803–825. doi: 10.1177/03058298050330030601.

Leander, A. (2014) 'Understanding US national intelligence: analyzing practices to capture the chimera.', in Best, J. and Gheciu, J. (eds) *The Return of the Public in Global Governance.* Cambridge: Cambridge University Press, pp. 197–221.

Ledgett, R. (2017) 'No, the U.S. Government Should Not Disclose All Vulnerabilities in Its Possession', *Lawfare Blog*, 7 August. Available at: https://perma.cc/W3JN-T2YR (Accessed: 10 March 2021).

Leonardi, P. M. (2012) 'Materiality, Sociomateriality, and Socio-Technical Systems: What Do These Terms Mean? How Are They Different? Do We Need Them?', *Materiality and Organizing: Social Interaction in a Technological World*, pp. 25–48. doi: 10.1093/acprof:oso/9780199664054.003.0002.

Lin, H. S. (2016) 'Attribution of Malicious Cyber Incidents: From Soup to Nuts', *Columbia Journal of International Affairs*, Hoover Ins. Available at: https://perma.cc/26QQ-823N.

Lohaus, P. (2018) *A New Blueprint for Competing Below the Threshold: The Joint Concept for Integrated Campaigning*, *War on the Rocks*. Available at: https://perma.cc/6XLE-MPXM (Accessed: 28 February 2021).

Lopez, C. T. (2019) *Persistent Engagement, Partnerships, Top Cybercom's Priorities*, *Defense.Gov*. Available at: https://perma.cc/74T5-7329 (Accessed: 28 February 2021).

Lotrionte, C. (2015) 'Countering State-Sponsored Cyber Economic Espionage under International Law International Law; Commercial Law; Law Countering State-Sponsored Cyber Economic Espionage Under International Law', *North Carolina Journal of International Law and Commercial Regulation*, 40(2), pp. 444–538. Available at: https://perma.cc/CM6V-9P6Y.

Lundborg, T. and Vaughan-Williams, N. (2015) 'New Materialisms, discourse analysis, and International Relations: a radical intertextual approach', *Review of International Studies*, 41(1), pp. 3–25. doi: 10.1017/S0260210514000163.

Lute, J. H. and McConnell, B. (2011) *Op-Ed: A Civil Perspective on Cybersecurity*, *Wired*. Available at: https://perma.cc/3NYS-Z89X (Accessed: 10 March 2021).

Lyngaas, S. (2015) *CDM, Einstein aren't enough, security experts say*, *GCN.com*. Available at: https://perma.cc/UW8P-C8QG (Accessed: 10 March 2021).

Lynn, W. J. (2010) *Defending a new domain*, *U.S. Department of Defense*. Available at: https://perma.cc/DXA4-PM2F (Accessed: 27 November 2020).

MacKenzie, D. A. (1993) *Inventing accuracy: A historical sociology of nuclear missile guidance*. Cambridge, Ma.: MIT Press.

Mandiant (2013) *APT1 Exposing One of China's Cyber Espionage Units*. Available at: https://perma.cc/47TJ-L3MV.

Markham, A. (2003) 'Metaphors Reflecting and Shaping the Reality of the Internet: Tool, Place, Way of Being', *Association of Internet Researchers …*. Available at: https://perma.cc/U5YW-TKY4.

Martelle, M. (2018) 'Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL', *National Security Archives*. Available at: https://perma.cc/NAR7-4Z4Q (Accessed: 22 January 2020).

Martin, L. and Simon, S. (2008) 'A Formula for Disaster: The Department of Homeland Security's Virtual Ontology', *Space and Polity*, 12(3), pp. 281–296. doi: 10.1080/13562570802515127.

Mayer, M. and Acuto, M. (2015) 'The Global Governance of Large Technical Systems', *Millennium* -

Journal of International Studies, 43(2), pp. 660–683. doi: 10.1177/0305829814561540.

Mayer, M., Carpes, M. and Knoblich, R. (2014) 'A Toolbox for Studying the Global Politics of Science and Technology', in Mayer, M., Carpes, M., and Knoblich, R. (eds) *The Global Politics of Science and Technology Vol. 2*. Berlin, Heidelberg: Springer, pp. 1–17.

Mayrl, D. and Quinn, S. (2016) 'Defining the State from within: Boundaries, Schemas, and Associational Policymaking', *Sociological Theory*, 34(1), pp. 1–26. doi: 10.1177/0735275116632557.

McCarthy, D. R. (2018) 'Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order', *Politics and Governance*, 6(2), pp. 5–12. doi: 10.17645/pag.v6i2.1335.

McCaul, M. and Warner, M. (2015) *How to unite privacy and security — before the next terrorist attack*, *Washington Post*. Available at: https://perma.cc/X9V2-SA5C (Accessed: 28 February 2021).

McConnell, M., Chertoff, M. and Lynn, W. (2015) *Why the fear over ubiquitous data encryption is overblown*, *Washington Post*. Available at: https://perma.cc/8WMZ-VFFC (Accessed: 28 February 2021).

McGhee, J. E. (2016) 'Liberating Cyber Offense', *Strategic Studies Quarterly*, (4/2016), pp. 46–63. Available at: https://perma.cc/D48E-LMAQ.

McNeil, M. *et al.* (2017) 'Conceptualizing Imaginaries of Science, Technology, and Society', in Felt, U. et al. (eds) *The Handbook of Science and Technology Studies*. Fourth. Cambridge, Ma.: MIT Press, pp. 435–465.

McWhorter, D. (2013) *Mandiant Exposes APT1 - One of China's Cyber Espionage Units & Releases 3,000 Indicators*, *FireEye*. Available at: https://perma.cc/39L4-EU3F (Accessed: 24 August 2020).

Megoran, N., Raballand, G. and Bouyjou, J. (2005) 'Performance, Representation and the Economics of Border Control in Uzbekistan', *Geopolitics*, 10(4), pp. 712–740. doi: 10.1080/14650040500318498.

Merriam-Webster (2020) *"Cybersecurity."*, *Merriam-Webster.com Dictionary*. Available at: https://www.merriam-webster.com/dictionary/cybersecurity (Accessed: 2 October 2020).

Metz, S. (2006) 'America's Defense Transformation: A Conceptual and Political History', *Defence Studies*, 6(1), pp. 1–25. doi: 10.1080/14702430600838511.

Migdal, J. S. and Schlichte, K. (2016) 'Rethinking the State', in Schlichte, K. (ed.) *The dynamics of states: the formation and crises of state domination*. London: Routledge, pp. 1–44.

Mol, A. (2002) *The body multiple: Ontology in medical practice*. Durham, N.C.: Duke University Press.

Mol, A. (2010) 'Actor-Network Theory: sensitive terms and enduring tensions', *Kölner Zeitschrift für Soziologie und Sozialpsychologie*, 50(1), pp. 253–269. Available at: https://perma.cc/QJ2L-8EEM.

Molander, R. C., Riddile, A. S. and Wilson, P. A. (1996) *Strategic Information Warfare A New Face of War*, *RAND*. Washington, D.C. Available at: https://perma.cc/6HXH-XAUL.

Monte, M. (2015) *Network attacks and exploitation: A framework.* Indiannapolis: John Wiley & Sons.

Mueller, M. and Kuehn, A. (2014) 'Einstein on the Breach: Surveillance Technology, Cybersecurity and Organizational Change', *Security in Cyberspace : Targeting Nations, Infrastructures, Individuals*, (Weis), pp. 1–26. doi: 10.5040/9781501302237.ch-006.

Muppidi, H. (1999) 'Postcoloniality and the Production of Insecurity', in Weldes, J. et al. (eds) *Cultures of Insecurity: States, Communities and the Production of Danger.* Minneapolis, MN: University of Minnesota Press, pp. 119–146.

Nakashima, E. (2011) *Government, companies taking steps to ward off cyberattacks*, *Washington Post*. Washington. Available at: https://perma.cc/4G4C-JZZK (Accessed: 28 February 2021).

Nakashima, E. (2012a) *Cyber defense effort is mixed, study finds*, *Washington Post*. Available at: https://perma.cc/XWB5-GVAM (Accessed: 28 February 2021).

Nakashima, E. (2012b) *When is a cyberattack a matter of defense?*, *The Washington Post*. Washington, D.C. Available at: https://perma.cc/Q884-86ZS (Accessed: 28 February 2021).

Nakashima, E. (2012c) *White House, NSA weigh cybersecurity, personal privacy*, *Washington Post*. Washington, D.C. Available at: https://perma.cc/3LKP-CKQL (Accessed: 26 February 2021).

Nakashima, E. (2013) *Dual-leadership role at NSA and Cyber Command stirs debate*, *The Washington Post*. Available at: https://perma.cc/KL86-S323 (Accessed: 28 February 2021).

Nakashima, E. (2016) 'National Security Agency plans major reorganization', *Washington Post*, 2 February. Available at: https://perma.cc/6VR7-GBLM (Accessed: 28 February 2021).

Nakashima, E. (2019) 'At nations' request, U.S. Cyber Command probes foreign networks to hunt election security threats', *Washington Post*, 8 May. Available at: https://perma.cc/26MG-37MP (Accessed: 5 December 2020).

Nakashima, E. and Peterson, A. (2016) *NSA's use of software flaws to hack foreign targets posed risks to cybersecurity*, *Washington Post*. Available at: https://perma.cc/KF7H-S2JE (Accessed: 28 February 2021).

Nakashima, E. and Riley, T. (2020) *The Cybersecurity 202: Here's why NSA rushed to expose a dangerous computer bug*, *The Washington Post*. Available at: https://perma.cc/QFG3-KL57 (Accessed: 28 February 2021).

Nakashima, E. and Ryan, M. (2016) *U.S. military has launched a new digital war against the Islamic State*, *Washington Post*. Available at: https://perma.cc/V5VF-65XK (Accessed: 28 February 2021).

Nakasone, P. (2019a) 'A Cyber Force for Persistent Operations', *Joint Force Quarterly*, 92(1), pp. 10–14.

Nakasone, P. (2019b) 'Statement of General Paul M. Nakasone Commander United States Cyber Command Before the Senate Committee on Armed Services 14 February 2019'. Senate Armed Services. Available at: https://perma.cc/U645-D7ZW.

Napolitano, J. (2011) 'Secretary Napolitano's Remarks on "Our Shared Responsibility: The Importance of Strong International Homeland Security Partnerships"'. Available at: https://perma.cc/7KR4-CTRN.

Navarretef, I. and Buchaní, R. (2019) *Out of the legal wilderness: Peacetime espionage, international law and the existence of customary exceptions*, *Cornell International Law Journal*. Available at: https://scholarship.law.cornell.edu/cilj/vol51/iss4/4/?utm_source=scholarship.law.cornell.edu%2Fcilj%2Fvol51%2Fiss4%2F4&utm_medium=PDF&utm_campaign=PDFCoverPages.

Neal, A. W. (2019) *Security as Politics: Beyond the State of Exception*. Edinburgh: Edinburgh University Press.

Newman, D. (2003) 'Boundaries', in Agnew, J., Mitchell, K., and Toal, G. (eds) *The companion to political geography*. Malden, MA: Blackwell, pp. 122–36.

Newman, L. H. (2017) *Feds Explain Their Software Bug Stash—But Don't Erase Concerns*, *Wired*. Available at: https://perma.cc/PAZ3-XX3D (Accessed: 28 February 2021).

Newman, L. H. (2020) *Windows 10 Has a Security Flaw So Severe the NSA Disclosed It*, *WIRED*. Available at: https://perma.cc/53TZ-MNF2 (Accessed: 28 February 2021).

Ney, P. C. (2020) 'DOD General Counsel Remarks at U.S. Cyber Command Legal Conference. Speech, March 2 2020'. Available at: https://perma.cc/E94K-8AMB.

NICCS (2019) *Explore Terms: A Glossary of Common Cybersecurity Terminology*, *National Initiative for Cybersecurity Careers and Studies*. Available at: https://perma.cc/2NGE-TNSE (Accessed: 10 October 2019).

Nissenbaum, H. (2005) 'Where computer security meets national security', *Ethics and Information Technology*, 7(2), pp. 61–73. doi: 10.1007/s10676-005-4582-3.

Nolte, W. M. (2012) 'Anticipating Cyberspace Security: NSA's Experience, 1992–1997', *Cryptologic Quarterly*, 47, pp. 26–37.

NSA (2020) *Exim Mail Transfer Agent Actively Explouted by Russian GRU Cyber Actors*, *NSA/CSS Cybersecurity Directorate*. Available at: https://perma.cc/KS79-WRYW (Accessed: 9 September 2020).

Ó Tuathail, G. (1999) 'Borderless worlds? Problematising discourses of deterritorialisation', *Geopolitics*, 4(2), pp. 139–154. doi: 10.1080/14650049908407644.

Office of the Chairman of the Joint Chiefs of Staff (2020) 'DOD Dictionary of Military and Associated Terms', *Joint Education and Doctrine Division, J-7*, (January), p. 382. Available at: https://perma.cc/U758-JT5W.

Office of the Director of National Intelligence (2014) *FOIA Response*, *Eff.Org*. Available at: https://perma.cc/8TFB-T472.

Office of the National Counterintelligence Executive (2011) *Foreign Spies Stealing US Economic Secrets in Cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*. Available at: https://perma.cc/G6TX-QPGX.

Oosthoek, K. and Doerr, C. (2020) 'Cyber Threat Intelligence: A Product Without a Process?', *International Journal of Intelligence and CounterIntelligence*. Routledge, 0(0), pp. 1–16. doi: 10.1080/08850607.2020.1780062.

Orsini, A., Louafi, S. and Morin, J. F. (2017) 'Boundary Concepts for Boundary Work Between Science and Technology Studies and International Relations: Special Issue Introduction', *Review of Policy Research*, 34(6), pp. 734–743. doi: 10.1111/ropr.12273.

Otto, G. (2015) *DHS official: Einstein 3A is 15 years behind the times*, *FedScoop*. Available at: https://perma.cc/WGJ6-XEL8 (Accessed: 28 February 2021).

Panetta, S. of D. L. E. (2012) 'Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City. Speech, October 11, 2012.' Available at: https://perma.cc/3AYD-TUUD.

Pereira, M. do M. (2019) 'Boundary-work that Does Not Work: Social Inequalities and the Non-performativity of Scientific Boundary-work', *Science Technology and Human Values*, 44(2), pp. 338–365. doi: 10.1177/0162243918795043.

Persson, A. (2010) 'Soldiers and secretaries: Gendered boundary work in the Swedish Armed Forces', *Scandinavian Journal of Management*. Elsevier Ltd, 26(2), pp. 166–175. doi: 10.1016/j.scaman.2009.12.004.

Pfotenhauer, S. and Jasanoff, S. (2017) 'Panacea or diagnosis ? Imaginaries of innovation and the "MIT model" in three political cultures', *Social Studies of Science*, 46(6), pp. 783–810. doi: 10.1177/0306312717706110.

PGPF.org (2020) *U.S. Defense Spending Compared to Other Countries*, *Peter G. Peterson Foundation*.

Available at: https://perma.cc/A6BM-J33Z (Accessed: 2 December 2020).

Pinch, T. and Leuenberger, C. (2006) 'Studying Scientific Controversy from the STS Perspective', in *EASTS Science Controversy and Democracy*. Available at: https://perma.cc/6KLV-H57G.

Pomerleau, M. (2016) *Services still adapting to the job of weaponizing the network*, *Defense News*. Available at: https://perma.cc/UK4M-K2R7 (Accessed: 28 February 2021).

Pomerleau, M. (2017) *Cyber Command awards first contract under its limited acquisition authority*, *Fifth Domain*. Available at: https://perma.cc/P532-V2G4 (Accessed: 28 February 2021).

Pomerleau, M. (2020) *Pentagon weapons tester hones in on cyber tools*, *Fifth Domain*. Available at: https://perma.cc/E866-MU3X (Accessed: 10 March 2021).

Porche III, I. R. *et al.* (2013) 'Summary', in *Redefining Information Warfare Boundaries for an Army in a Wireless World*. RAND Corporation. Available at: https://perma.cc/74VJ-QAET.

Powner, D. (2009) *Key Improvements Are Needed to Strengthen the Nation's Posture (Testimony Before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives)*. Washington, D.C. Available at: https://perma.cc/9UEY-X22F.

Pozen, D. E. (2013) 'The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information', *127 Harvard Law Review*, 512.

Preda, A. (1999) 'THE TURN TO THINGS: Arguments for a Sociological Theory of Things', 40(2), pp. 347–366.

President's Commission on Critical Infrastructure Protection (1998) *Critical Foundations: Protecting America's Infrastructures. the Report of the President's Commission on Critical Infrastructure Protection*. Available at: https://perma.cc/A5SS-T9AT.

Pretorius, J. (2008) 'The security imaginary: Explaining military isomorphism', *Security Dialogue*, 39(1), pp. 99–120. doi: 10.1177/0967010607086825.

Rankin, W. (2014) 'The Geography of Radionavigation and the Politics of Intangible Artifacts', *Technology and Culture*, 55(3), pp. 622–674. doi: 10.1353/tech.2014.0077.

Reese, T. (2011) *Mandiant welcomes Richard Bejtlich to the team*, *FireEye*. Available at: https://perma.cc/LEG8-HPMS (Accessed: 24 August 2020).

Rein, M. and Schön, D. (1996) 'Frame-critical policy analysis and frame-reflective policy practice', *Knowledge and Policy*, 9(1), pp. 85–104. doi: 10.1007/BF02832235.

Reuters (2010) *US military could play expanded cyber defense role*, *Reuters.com*. Available at: https://perma.cc/PN2F-PMYS (Accessed: 28 February 2021).

Riesch, H. (2010) 'Theorizing Boundary Work as Representation and Identity', *Journal for the Theory of Social Behaviour*, 40(4), pp. 452–473. doi: 10.1111/j.1468-5914.2010.00441.x.

Rip, A. (1986) 'Controversies as Informal Technology A ssessment', *Knowledge*, 8(2), pp. 349–371. doi: 10.1177/107554708600800216.

Robinson, C. (2019) *Why CVSS does not equal risk: How to think about risk in your environment*, *Red Hat Blog*. Available at: https://perma.cc/V7MN-GKYP (Accessed: 1 August 2020).

Rodriguez, M. (2017) *Declaration by Miguel Rodriguez, Representative of Cuba, at the final session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. New York, June 23, 2017*. Available at: https://perma.cc/57KJ-ALHR.

Rogers, A. M. (2014) *Transcript of Admiral Michael S. Rogers Address to Stanford University at the Freeman Spogli Institute for International Studies, November 3rd 2014*, *Speeches and Congressional Testimonies, NSA*. Available at: https://perma.cc/M6U3-ZKV4 (Accessed: 1 August 2020).

Rogers, M. S. (2015) *Beyond the Build: Delivering Outcomes Through Cyberspace*. Available at: https://perma.cc/AU4P-R7Q8.

Ross, A. (2019) *Calling Into Question the CVSS*, *SecurityIntelligence Blog*. Available at: https://perma.cc/4A75-AXAE (Accessed: 1 August 2020).

Saco, D. (1999) 'Colonizing Cyberspace: 'National Security'and the Internet', in Weldes, J. et al. (eds) *Cultures of insecurity: States, communities, and the production of danger*. Minneapolis: University of Minnesota Press, pp. 261–292.

Sadowski, J. and Bendor, R. (2019) 'Selling Smartness: Corporate Narratives and the Smart City as a Sociotechnical Imaginary', *Science Technology and Human Values*, 44(3), pp. 540–563. doi: 10.1177/0162243918806061.

Sala, V. Della (2017) 'Homeland security: territorial myths and ontological security in the European Union', *Journal of European Integration*. Routledge, 39(5), pp. 545–558. doi: 10.1080/07036337.2017.1327528.

Sanger, D. E. (2018) *The Perfect Weapon*. Melbourne, London: Scribe.

Sanger, D. E., Barboza, D. and Perlroth, N. (2013) *Chinese Army Unit Is Seen as Tied to Hacking Against US*, *New York Times*. New York. Available at: https://perma.cc/7BQ3-KRJ4 (Accessed: 28 February 2021).

Sanger, D. E. and Perlroth, N. (2014) *U.S. Denies It Knew of Heartbleed Bug on the Web*, *The New York Times*. Available at: https://perma.cc/9JM3-H62P (Accessed: 28 February 2021).

Sanger, D. E. and Perlroth, N. (2019) 'U.S. Escalates Online Attacks on Russia's Power Grid', *New York Times*, 15 June. Available at: https://perma.cc/N9Q7-EM4M (Accessed: 28 February 2021).

Sanger, D. E. and Schmitt, E. (2017) *U.S. Cyberweapons, Used Against Iran and North Korea, Are a Disappointment Against ISIS*, *New York Times*. Available at: https://perma.cc/SGR9-N9CQ (Accessed: 28 February 2021).

Sassen, S. (2002) 'Towards a Sociology of Information Technology', *Current Sociology*, 50(3), pp. 365–388. doi: 10.1177/0011392102050003005.

Sassen, S. (2008) *Territory, authority, rights: From medieval to global assemblages*. Princeton: Princeton University Press.

Schneier, B. (2012) *The Vulnerabilities Market and the Future of Security. May 30th 2012.*, *Schneier on Security*. Available at: https://perma.cc/S8E7-A7PX (Accessed: 30 July 2020).

Schneier, B. (2014) *Disclosing vs. Hoarding Vulnerabilities. May 22nd 2014.*, *Schneier on Security*. Available at: https://www.schneier.com/blog/archives/2014/05/disclosing_vs_h.html (Accessed: 30 July 2020).

Schneier, B. (2016) *The NSA is hoarding vulnerabilities. Aug 26th 2016.*, *Schneier on Security*. Available at: https://perma.cc/U2J5-7MDS (Accessed: 30 July 2020).

Schoka, A. (2019) *Cyber Command, the NSA, and Operating in Cyberspace: Time to end the dual hat*, *War on the Rocks*. Available at: https://perma.cc/887K-85JG (Accessed: 28 February 2021).

Schulze, M. (2017) 'Clipper meets apple vs. FBI—A comparison of the cryptography discourses from 1993 and 2016', *Media and Communication*, 5(1), pp. 54–62. doi: 10.17645/mac.v5i1.805.

Scott, J. C. (1998) *Seeing like a state: How certain schemes to improve the human condition have failed.* Yale: Yale University Press.

Sebenius, A. (2019) *Normally Hush-Hush NSA Opens Doors of New Cyber Directorate*, *Bloomberg*. Available at: https://perma.cc/CR94-EXM4 (Accessed: 28 February 2021).

Selyukh, A. (2013) *U.S. officials say NSA leaks may hamper cyber policy debate*, *Reuters*. Available at: https://perma.cc/A532-8R3R (Accessed: 28 February 2021).

Serbu, J. (2018) *DoD, DHS reach accord on new steps to cooperate in cyber defense*, *Federal News Network*. Available at: https://perma.cc/7MZ4-9DYT (Accessed: 28 February 2021).

Shanker, T. (2010) *Cyberwar Chief Calls for Secure Computer Network*, *New York Times*. Available at: https://perma.cc/9TGL-PNG7 (Accessed: 28 February 2021).

Shires, J. (2019) 'Family Resemblance or Family Argument ? Three Perspectives on Cybersecurity and their Interactions', *St Antony's International Review*, 1(1), pp. 18–36. Available at: https://www.ingentaconnect.com/content/stair/stair/2019/00000015/00000001/art00003.

Shires, J. (2020) 'Cyber-noir: Cybersecurity and popular culture', *Contemporary Security Policy*. Taylor & Francis, 41(1), pp. 82–107. doi: 10.1080/13523260.2019.1670006.

Shires, J. and Smeets, M. (2017) *Contesting "cyber"*. Available at: https://perma.cc/HTC8-BE8G.

Simon, S. and de Goede, M. (2015) 'Cybersecurity, Bureaucratic Vitalism and European Emergency', *Theory, Culture & Society*, 32(2), pp. 79–106. doi: 10.1177/0263276414560415.

Sismondo, S. (2010) *An Introduction to Science and Technology Studies*. Second Edi. Chichester: John Wiley & Sons.

Slupska, J. (2020) 'War, Health and Ecosystem: Generative Metaphors in Cybersecurity Governance', *Philosophy and Technology*. Philosophy & Technology. doi: 10.1007/s13347-020-00397-5.

Smith, B. (2017) 'The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack', *The Official Microsoft Blog*, pp. 1–2. Available at: https://perma.cc/M655-XLNJ.

Smith, E. (2009) 'Imaginaries of Development : The Rockefeller Foundation and Rice Research Imaginaries of Development : The Rockefeller Foundation and Rice', *Science as Culture*, 18(4), pp. 461–482. doi: 10.1080/09505430903186070.

Smith, M. (2016) *DHS EINSTEIN firewall fails to detect 94% of threats, doesn't monitor web traffic*, *CSOOnline.com*. Available at: https://perma.cc/XP6N-P6DA (Accessed: 28 February 2021).

Solms, R. Von and Niekerk, J. Van (2013) 'From information security to cyber security', *Computers & Security*. Elsevier Ltd, 38, pp. 97–102. doi: 10.1016/j.cose.2013.04.004.

Spaulding, S. E. (2010) 'No More Secrets: Then What ?', *HuffPost*, 24 June. Available at: https://perma.cc/8SL7-DSP2.

Spring, T. (2017) *Policy Experts Push To Make Vulnerability Equities Process Law*, *ThreatPost*. Available at: https://perma.cc/WV9L-X9UD (Accessed: 28 February 2021).

Squire, V. (2013) 'Attuning to mess', in Salter, M. B. and Mutlu, C. E. (eds) *Research Methods in Critical Security Studies*. London: Routledge, pp. 55–59.

Srnicek, N. (2013) *Representing Complexity: The Material Construction of World Politics*. Thesis submitted to The London School of Economics and Political Science.

Stampnitzky, L. (2020) 'Truth and consequences? Reconceptualizing the politics of exposure', *Security Dialogue*. doi: 10.1177/0967010620904576.

Stanley, M. (2016) *Program Update CDM Strategic Program Approach*. Available at: https://perma.cc/GF5C-G427.

Star, S. L. and Griesemer, J. R. (1989) 'Institutional Ecology, `Translations' and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology, 1907-39', *Social Studies of Science*, 19(3), pp. 387–420. doi: 10.1177/030631289019003001.

Starr, P. (1992) 'Social categories and claims in the Liberal State', *Social Research*, 59, pp. 262–95. Available at: https://www.jstor.org/stable/40970693.

Sternstein, A. (2017) *The secret world of vulnerability hunters*, *Christian Science Monitor*. Available at: https://perma.cc/6Z5P-7YDL (Accessed: 28 February 2021).

Stevens, C. (2020) 'Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet', *Contemporary Security Policy*, 41(1). doi: 10.1080/13523260.2019.1675258.

Stevens, T. (2016) *Cybersecurity and the Politics of Time*. Cambridge: Cambridge University Press.

Stevens, T. (2018) 'Editorial: Global cybersecurity: New directions in theory and methods', *Politics and Governance*, 6(2), pp. 1–4. doi: 10.17645/pag.v6i2.1569.

Sukumar, A. M. (2017) 'The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?', *Lawfare Blog*, 4 July. Available at: https://perma.cc/RE2M-X5S6.

Swedlow, B. (2017) 'Three Cultural Boundaries of Science, Institutions, and Policy: A Cultural Theory of Coproduction, Boundary-Work, and Change', *Review of Policy Research*, 34(6), pp. 827–853. doi: 10.1111/ropr.12233.

Taylor, R. G. (2015) 'Potential Problems with Information Security Risk Assessments', *Information Security Journal*, 24(4–6), pp. 177–184. doi: 10.1080/19393555.2015.1092620.

The President's Review Group on Intelligence and Communications Technologies (2013) *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*. Available at: https://perma.cc/AL48-WL9X.

Thomas, T. L. (2001) 'Information Security Thinking: a Comparison of U.S., Russian, and Chinese Concepts', *The Science and Culture Series, International Seminar on Nuclear War and Planetary Emergencies*, August, pp. 344–356. doi: 10.1142/9789812776945_0032.

Tucker, P. (2017) *What the Announced NSA/Cyber Command Split Means*, *DefenseOne*. Available at: https://perma.cc/L5PX-WR4R (Accessed: 21 January 2020).

U.S. Department of Defense (2004) *The National Military Strategy of the U.S. A strategy for today; a vision for tomorrow*. Available at: https://perma.cc/NYQ3-ZZ38.

UNGA (2013) 'A/68/98 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', *UN General Assembly*, (June). Available at: https://perma.cc/Y4VZ-KBTH.

UNGA (2015a) *A/70/174 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, *UN General Assembly*. Available at: https://perma.cc/V4DU-ELS6.

UNGA (2015b) *Resolution adopted by the General Assembly on 23 December 2015. 70/237. Developments in the field of information and telecommunications in the context of international security*. Available at: https://perma.cc/YN6N-MC49.

United States of America v Apple Inc (2016) 'Government's Ex Parte application for order compelling Apple Inc. to assist agents in search'. Available at: https://perma.cc/4KYG-2X78.

US Army (2010) *The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028*. Available at: https://perma.cc/WBD7-ALRB.

US Department of Defense (2003) *Information Operations Roadmap*. Available at: https://perma.cc/M58P-ZRBQ.

US Department of Defense (2015) *The DoD Cyber Strategy*. Available at: https://perma.cc/6KCD-X4H6.

US Department of Defense (2018) 'Joint Publication 3-12 Cyberspace Operations', (June 2018). Available at: https://perma.cc/T8U8-FMM9.

US House of Representatives (2010) 'U.S. Cyber Command: Organizing for Cyberspace Operations. Hearing, September 23, 2010.' Government Printing Office. Available at: https://perma.cc/ZE99-BPA3.

US House of Representatives (2011) 'Cyber Threats and Ongoing Efforts to Protect the Nation. Testimony compilation, hearing October 4, 2011'. Available at: https://perma.cc/Q7PV-EY6C.

US House of Representatives (2012) *National Defense Authorization Act for Fiscal Year 2012; Conference Report to Accompany H.R. 1540*. Available at: https://perma.cc/UG98-7BTN.

US House of Representatives (2013a) 'Cyber Attacks: an Unprecedented Threat to U.S. National Security, Hearing March 21, 2013'. Government Printing Office. Available at: https://perma.cc/Q3B8-8H9R.

US House of Representatives (2013b) 'Cyber Threats from China, Russia, and Iran: Protecting American Critical Infrastructure. Hearing, March 20, 2013.' Government Printing Office. Available at: https://perma.cc/8YCR-CYRB.

US House of Representatives (2013c) 'Information Technology and Cyber Operations: Modernization and Policy Issues To Support the Future Force, Hearing March 13, 2013'. Government Printing Office. Available at: https://perma.cc/9VJ8-7Y92.

US House of Representatives (2015a) 'Cyber Operations: Improving the Military Cybersecurity Posture in an Uncertain Threat Environment Hearing March 4 2015'. Washington, D.C.: Government Publishing Office. Available at: https://perma.cc/JFW5-KNN6.

US House of Representatives (2015b) 'DHS's Efforts to Secure .Gov, Hearing June 24 2015'. Washington, D.C.: Government Publishing Office. Available at: https://perma.cc/J95L-PPXR.

US House of Representatives (2015c) 'Emerging Threats and Technologies to Protect the Homeland'. Washington, D.C.: Government Printing Office. Available at: https://perma.cc/8PFK-Q3LY.

US House of Representatives (2015d) 'Examining the President's Cybersecurity Information-Sharing Proposal'. Washington, D.C.: Government Printing Office. Available at: https://perma.cc/3WZT-9XHF.

US House of Representatives (2015e) 'Worldwide Threats and Homeland Security Challenges, Hearing October 21 2015'. Washington, D.C.: Government Publishing Office. Available at: https://perma.cc/CBC9-57HF.

US House of Representatives (2016a) 'The Encryption Tightrope: Balancing Americans' Security and Privacy'. Washington, D.C.: Government Publishing Office. Available at: https://perma.cc/N97G-2PAE.

US House of Representatives (2016b) 'Value of DHS's Vulnerability Assessments in Protecting Our Nation's Critical Infrastructure'. Washington, D.C.: Government Printing Office. Available at: https://perma.cc/873D-29MP.

US House of Representatives (2017a) 'Maximising the Value of Cyber Threat Information Sharing,

Hearing November 15, 2017'. Government Publishing Office. Available at: https://perma.cc/9Q5V-W7SU.

US House of Representatives (2017b) 'The Current State of DHS's Efforts to Secure Federal Networks, Hearing March 28 2017'. Washington, D.C.: Government Publishing Office. Available at: https://perma.cc/FN8G-3PT6.

US House of Representatives (2018) *John S. McCain National Defense Authorization Act for Fiscal Year 2019; Conference Report to accompany H.R. 5515*. Available at: https://perma.cc/SB5U-MX5A.

US Senate (2010) 'Nominations Before The Senate Armed Services Committee. Hearing, March-November 2010'. Washington, D.C.: Government Printing Office. Available at: https://perma.cc/9QWQ-VQYE.

US Senate (2012a) 'Hearing To Receive Testimony on U.S. Strategic Command and U.S. Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2013 and the Future Years Defense Program, March 27 2012'. Washington, D.C. Available at: https://perma.cc/6T8G-F9BC.

US Senate (2012b) 'Securing America's Future: The Cybersecurity Act of 2012. Hearing, Feburary 16 2012'. Washington, D.C.: Government Printing Office. Available at: https://perma.cc/K7J3-FBBS.

US Senate (2013a) 'Cybersecurity: Preparing for and Responding to the Enduring Threat, Special Hearing June 12 2013'. Washington, D.C.: Government Printing Office. Available at: https://perma.cc/JE9E-KLJR.

US Senate (2013b) 'Department of Defense Authorization for Appropriations for Fiscal Year 2014 and the Future Years Defense Program, Part 5 Emerging Threats and Capabilities. Hearing March 19, April 9, 18, 23'. Government Printing Office. Available at: https://perma.cc/JQ2P-3WPY.

US Senate (2013c) 'The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting Our National and Economic Security, Joint Hearing March 7 2013'. Washington, D.C.: Government Printing Office. Available at: https://perma.cc/3JYM-P7AC.

US Senate (2013d) 'Threats to the Homeland, Hearing November 14, 2013'. Government Printing Office. Available at: https://perma.cc/92ZS-R4BP.

US Senate (2014a) 'Cyber Security, Hearings on March 26 2014 and April 2 2014'. Government Printing Office. Available at: https://perma.cc/H42G-A7FS.

US Senate (2014b) 'Department of Defense Authorization for Appropriations for Fiscal Year 2015 and the Future Years Defense Program, Pt.1 Hearings Feb - April 2014'. Government Printing Office. Available at: https://perma.cc/A3JF-9NQ5.

US Senate (2014c) 'Nominations Before The Senate Armed Services Committee, Second Session, 113th Congress. Hearings Jan - Dec 2014.' Government Publishing Office. Available at: https://perma.cc/YW6M-6FJG.

US Senate (2015a) 'Department of Defense Authorization for Appropriations for Fiscal Year 2016 and the Future Years Defense Program, Part 5 Emerging Threats and Capabilities, Hearing April 14 2015'. Government Printing Office. Available at: https://perma.cc/68KJ-ZQKE.

US Senate (2015b) 'Department of Homeland Security Appropriations: FY2016. Hearing April 15, 2015'. Washington, D.C.: Government Printing Office. Available at: https://perma.cc/6LSN-HETC.

US Senate (2015c) 'Under Attack: Federal Cybersecurity and the OPM Data Breach, Hearing June 25 2015'. Washington, D.C.: Government Printing Office. Available at: https://perma.cc/3L2T-TVTM.

US Senate (2015d) 'United States Cybersecurity Policy and Threats. Hearing, September 29, 2015'. Government Printing Office. Available at: https://perma.cc/H6UR-LJ73.

US Senate (2016a) ‘Cybersecurity, encryption and United States National Security Matters hearing, July and September 2016’. Washington, D.C.: Government Publishing Office. Available at: https://fas.org/irp/congress/2016_hr/cybersec.pdf.

US Senate (2016b) ‘Department of Defense Authorization for Appropriations for Fiscal Year 2016 and the Future Years Defense Program, Pt.1 Hearings March - April 2015’. Government Printing Office. Available at: https://perma.cc/VT6H-UE8W.

US Senate (2018) ‘Stenographic Transcript Before the Subcommittee on Cybersecurity Comittee on Armed Services: Cyber Posture of the Services, March 13, 2018’. Alderson Court Reporting. Available at: https://perma.cc/3ZPZ-VXFE.

USCC (2012) *2012 Report to Congress of the U.S.-China Economic and Security Review Commission*. Available at: https://perma.cc/4TEM-YMNC.

Valovic, T. (1999) *Digital mythologies: The hidden complexities of the Internet*. New Brunswick: Rutgers University Press.

Vance, C. (2014) *Apple and Google threaten public safety with default smartphone encryption*, *Washington Post*. Washington, D.C., D.C. Available at: https://perma.cc/H929-XAMW (Accessed: 28 February 2021).

VEP (2010) *Commercial and Government Information Technology and Industrial Control Product of system Vulnerabilities Equities and Process*. Available at: https://perma.cc/6Z8V-2RQ8.

VEP Charter (2017) *Unclassified VEP Charter Vulnerabilities Equities Policy and Process for the United States Government, November 15 2017*, *National Security Council*. Available at: https://perma.cc/N3ZH-ZASC.

Vuori, J. A. (2008) ‘Illocutionary logic and strands of securitization: Applying the theory of securitization to the study of non-democratic political orders’, *European Journal of International Relations*, 14(1), pp. 65–99. doi: 10.1177/1354066107087767.

Walters, W. (2014) ‘Drone strikes, dingpolitik and beyond: Furthering the debate on materiality and security’, *Security Dialogue*, 45(2), pp. 101–118. doi: 10.1177/0967010613519162.

Warner, M. (2012) ‘Cybersecurity: A pre-history’, *Intelligence and National Security*, 27(5), pp. 781–799. doi: 10.1080/02684527.2012.708530.

Warner, M. (2015) ‘U.S. Cyber Command’s Road to Full Operational Capability’, in Seidule, T. and Whitt, J. E. (eds) *Stand Up and Fight: The Creation of U.S. Security Organizations, 1942–2005*. Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, pp. 119–138.

Warner, M. R. (2016) *Warner, McCaul Lead Bipartisan Coalition to Establish National Commission on Digital Security*, *warner.senate.gov*. Available at: https://perma.cc/K7ZM-2UTH (Accessed: 30 November 2019).

Weiss, M. and Jankauskas, V. (2019) ‘Securing cyberspace: how states design governance arrangements’, *Governance*, 32(2), pp. 259–275. doi: 10.1111/gove.12368.

Weldes, J. (1998) ‘Bureaucratic Politics : A Critical Constructivist Assessment’, *Mershon International Studies Review*, 42(2), pp. 216–225. Available at: https://www.jstor.org/stable/254413.

Weldes, J. *et al.* (1999) ‘Introduction: Constructing Insecurity’, in Weldes, J. et al. (eds) *Cultures of Insecurity: States, communities and the production of danger*. Minneapolis: University of Minnesota Press, pp. 1–35.

Weldes, J. (1999) ‘The Cultural Production of Crises: U.S. Identity and Missiles in Cuba’, in Weldes, J. et al. (eds) *Cultures of insecurity: States, communities, and the production of danger*. Minneapolis:

University of Minnesota Press, pp. 35–62.

White House (2003) *The National Strategy to Secure Cyberspace*. Available at: https://perma.cc/WA7A-EULD.

White House (2008) *National Security Presidential Directive NSPD-54; Homeland Security Presidential Directive HSPD-23 (The Comprehensive National Cybersecurity Initiative)*. Washington, D.C. Available at: https://perma.cc/CD4M-NGTA.

White House (2009) *Cyberspace Policy Review Assuring a Trusted and Resilient Information and Communications Infrastructure*. Available at: https://fas.org/irp/eprint/cyber-review.pdf.

White House (2010) *The Comprehensive National Cybersecurity Initiative*, *Washington, DC: White House*. Available at: https://perma.cc/D3JV-V4PF.

White House (2011) *International Strategy for Cyberspace*. Available at: https://perma.cc/J5PA-3K8M.

White House (2013) *Executive Order 13636: Improving critical infrastructure cybersecurity*, *Federal Register*. Available at: https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

White House (2018) *National Cyber Strategy of the United States of America*. Washington.

White, S. (2019) *Subcultural Influence on Military Innovation: The Develpment of U. S. Military Cyber Doctrine*. Thesis, submitted to Harvard. Available at: https://dash.harvard.edu/handle/1/42013038.

Wiener, C. (2016) *Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation*. Thesis, submitted to George Mason University. Available at: http://mars.gmu.edu/xmlui/handle/1920/10613.

Williams, M. C. (2003) 'Words, images, enemies: Securitization and international politics', *International Studies Quarterly*, 47(4), pp. 511–531. doi: 10.1046/j.0020-8833.2003.00277.x.

Wilson, A. *et al.* (2016) *BUGS IN THE SYSTEM A Primer on the Software Vulnerability Ecosystem and its Policy Implications*. Available at: https://perma.cc/BGH4-WLY6.

Wolff, J. (2016) *Cyber Is Not a Noun*, *Slate Future Tense*. Available at: https://perma.cc/TL7Y-KYC9 (Accessed: 3 October 2019).

Work, J. (2020) 'Evaluating Commercial Cyber Intelligence Activity', *International Journal of Intelligence and CounterIntelligence*. Routledge, 33(2), pp. 278–308. doi: 10.1080/08850607.2019.1690877.

Wyatt, S. and Balmer, B. (2007) 'Home on the range: What and where is the middle in science and technology studies?', *Science Technology and Human Values*, 32(6), pp. 619–626. doi: 10.1177/0162243907306085.

Wyn Jones, R. (2000) *Security, Strategy, and Critical Theory*. Boulder, CO.: Lynne Rienner. doi: 10.2307/2586105.

Wynne, B. (1988) 'Unruly Technology: Practical Rules, Impractical Discourses and Public Understanding', *Social Studies of Science*, 18(1), pp. 147–167. doi: 10.1177/030631288018001006.

Wynne, B. (1996) 'A reflexive view of the expert-lay knowledge divide.', in Lash, S., Szerszynski, B., and Wynne, B. (eds) *Risk, environment and modernity: Towards a new ecology*. London: Sage Publications, pp. 44–83.

Zajko, M. (2015) 'Canada's cyber security and the changing threat landscape', *Critical Studies on Security*. Routledge, 3(2), pp. 147–161. doi: 10.1080/21624887.2015.1071165.

Zetter, K. (2012) *DHS, Not NSA, Should Lead Cybersecurity, Pentagon Official Says*, *WIRED*. Available at: https://perma.cc/JF6E-SWWN (Accessed: 28 February 2021).

Zetter, K. (2014a) *Has the NSA Been Using the Heartbleed Bug as an Internet Peephole ?*, *Wired*. Available at: https://perma.cc/FMK3-Z4LA (Accessed: 28 February 2021).

Zetter, K. (2014b) *Report: NSA Exploited Heartbleed to Siphon Passwords for Two Years | Threat*, *WIRED*. Available at: https://perma.cc/EAT5-U8C7 (Accessed: 28 February 2021).

Zetter, K. (2014c) *U.S. Gov Insists it Doesn't Stockpile Zero-Day Exploits to Hack Enemies*, *WIRED*. Available at: https://perma.cc/4P7M-TTSQ (Accessed: 28 February 2021).

Appendix 1

- This is a list of the most frequent sources and repositories that I drew and curated my sources from.
- All of the online sources directly referenced in the thesis have been stored in perma.cc for posterity against the risk of link fade.
- Any specific documents or sources that I couldn't obtain from primary or official repositories such as GovInfo could often be found through targeted keyword searches on a web search engine (I used Startpage searches, through Mozilla browsers).
- Many of the official federal sites have been archived too, such as previous administrations' White House pages. The Internet Archive provided an invaluable tool for tracing the changes in websites though – for example looking into how the DoD sites changed over time to reflect doctrinal and organisational changes.
- The list below is not exhaustive, as that detail is reserved for the thesis' References list, but it is indicative of the range of sources that I relied on throughout my methodology described in Chapter Two.

Federal and governmental sources

GovInfo (formerly FedSys): For congressional records, hearing transcripts, legislation and bills, and conference reports. govinfo is a service of the United States Government Publishing Office (GPO), which is a Federal agency in the legislative branch and provides free public access to official publications from all three branches of the Federal Government. https://www.govinfo.gov/

Congress.gov: for specific legislation and records of bills or congressional activities https://www.congress.gov/

Congressional Research Service: For access to topic-specific reports that have informed the legislative process. The CRS serves as shared staff to congressional committees and Members of Congress. CRS experts assist at every stage of the legislative process — from the early considerations that precede bill drafting, through committee hearings and floor debate, to the oversight of enacted laws and various agency activities. https://crsreports.congress.gov/

Library of Congress: access to declassified and historical documents, specific records of programs or operations or FOIAs https://www.loc.gov/

Congressional lawmakers' personal websites, such as Dianne Feinstein, James Langevin or Richard Burr. Specific sources used in thesis archived via perma.cc but also browable via Internet Archive

Defense Technical Information Center: DTIC is the online repository for all DoD-funded research reports, academic materials and doctrinal documents https://discover.dtic.mil/about/

Websites of individual agencies/branches:

The following sites also have archived versions, e.g. https://obamawhitehouse.archives.gov/ or https://trumpwhitehouse.archives.gov/

https://www.dhs.gov/

https://www.cisa.gov/

https://www.gao.gov/

https://www.nsa.gov/

https://www.justice.gov/

https://www.whitehouse.gov/omb/

https://www.defense.gov/

https://www.dni.gov/

Public access repositories

Some transcripts and hearing records were not available through GovInfo, which meant locating those individual hearings once I knew their titles through cross-referencing with other sources:

National Security Archive: Some of these congressional records were available instead from the NSA but this was also an invaluable source of declassified documents https://nsarchive.gwu.edu/

Internet Archive https://archive.org/web/

News and magazine reportage

BBC News

C4ISR.com

Christian Science Monitor

CSO.com

CyberScoop

Dark Reading

DefenseOne

FCW.com

FedScoop

Fifth Domain

New York Times

NextGov.com

Politico

Reuters

Signal Magazine

The Guardian

The Register (El Reg)

Vice/Motherboard

War on the Rocks

Washington Post

WIRED

Private sector and 'infosec' sources

CyberSecPolitics blog https://cybersecpolitics.blogspot.com/

Schneier on Security https://www.schneier.com/

Matt Blaze https://www.mattblaze.org/blog/

Krebs on Security https://krebsonsecurity.com/

Tao Security https://taosecurity.blogspot.com/

WeLiveSecurity https://www.welivesecurity.com/

RiskyBusiness https://risky.biz/about/

GitHub for looking at specific open source projects and their associated comments, changes, branches and developer insights https://github.com/

'Grey literature'

Open Technology Institute

Center for Democracy and Technology

Belfer Center

CSIS

Electronic Frontier Foundation EFF.org

American Civil Rights Union ACLU.org

ESET

Mandiant/FireEye

Crowdstrike

Brookings Institute

Lawfare