UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Google's expansion into security

Platforms, infrastructure, (in)visibility

van Hardeveld, A.A.

Publication date
2025

Link to publication

Citation for published version (APA):
van Hardeveld, A. A. (2025). *Google's expansion into security: Platforms, infrastructure, (in)visibility*. [Thesis, fully internal, Universiteit van Amsterdam].

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:11 Feb 2026

CHAPTER 1

Introduction

> Google encounters lawsuits from governments around the world with some frequency over alleged breaches of copyright or national laws, and it works hard to assure its users that Google serves their interests first and foremost, while staying within the boundaries of the laws itself. But if Google stopped all product developments whenever if it found itself with a government suit, it would never build anything. - Eric Schmidt, then Executive Chairman of Google, and Jared Cohen, then Director of Google Ideas (2013, p. 66)

> The central truth of the technology industry-that technology is neutral but people are not-will periodically be lost amid all the noise. But our collective progress as citizens in the digital age will hinge on our not forgetting it. - Eric Schmidt, then Executive Chairman of Google, and Jared Cohen, then Director of Google Ideas (2013, p. 66)

Introduction

Big Tech companies[1], which include Alphabet-Google, Amazon, Microsoft, Apple and Meta-Facebook, are deeply entangled in our daily digital lives. We use their social media and commerce platforms, cloud infrastructure, email clients, operational software, search engines, smart assistants, laptops and most recently their artificial intelligence (AI) powered large language models such as ChatGPT and Gemini. Concerned with Big Tech's impact on society, literatures in new media studies have examined how these "free" platforms and services affect "institutions, economic transactions, and social and cultural practices" (van Dijck et al., 2018, p. 2). Recognizing Big Tech's position in society, regulators from both the United States and (members of) the European Union attempt to reign in their power. For example, the European Union adopted a new regulation focused on protecting the European digital market by limiting Big Tech's power as "gatekeepers" (Regulation (EU) 2022/1925, 2022). In the United States, Big Tech are faced with antitrust lawsuits for monopolizing search and digital advertising (Robins-Early, 2024).

1 With the term Big Tech, I refer to US-based multinational technology companies that, through the scope and scale of their ecosystem of software and hardware products, have come to dominate their respective sectors and as such have signifcant socio-political influence on digital society.

While these regulations and lawsuits are important to curb Big Tech power, as the first quote at the start of this chapter illustrates, these regulations are not likely to stop Big Tech from expanding their businesses.

Now, Big Tech are becoming increasingly involved in matters of security and war. This involvement initially seemed reluctant and hidden. As was revealed by Edward Snowden in 2013, Big Tech were secretly sharing the data that they collect through their various platforms and services with United States police forces and the National Security Agency (NSA) (Ackerman, 2014). In Europe, the European Commission had to repeatedly pressure Big Tech companies like Google and Facebook to remove extremist content from their social media platforms (Gibbs, 2017, 2018). But in the last few years, Big Tech's involvement in security and war has become more proactive and prominent. In 2018, Google assisted the United States Department of Defense with developing AI for its drone program in Project Maven (Conger & Cameron, 2018). Despite protests by employees, Google and Amazon are taking part in Project Nimbus, a cloud project of the Israeli government (Scheer, 2021). Since the Russian invasion of Ukraine in February 2022, Amazon has been working with the Ukrainian government to safeguard their sensitive data in Amazon's cloud computing system (Mitchell, 2022). Microsoft and Google have been assisting the Ukrainian government to fend off cyberattacks and to remove state-sponsored disinformation from its platforms (Smith, 2022; Walker, 2022a, 2022b). Next to these involvements in war, Big Tech are also putting their stamp on cyber security practices (Liebetrau & Monsees, 2023) and are providing their cloud infrastructure and computational resources to third parties to facilitate the transition from AI research to "practical, real-world commercial products and services in a variety of industry sectors" (van der Vlist et al., 2024, p. 1). As a result, Big Tech put their stamp on how and for what (security) purposes AI can be used.

Through these involvements, Big Tech companies are getting even more powerful as they have power over what needs to be secured or protected, from whom and how. As the second quote at the start of this chapter illustrates, Big Tech present their involvements and technologies to the world as neutral and inevitable. It could be argued that Big Tech are, at times, simply better positioned and equipped to address certain (digital) security issues. For instance, Big Tech like Google, Amazon and Microsoft were able to quickly offer their products and services to the Ukrainian government in support of their fight against the Russian invasion. But as critical security studies

literature - a subdiscipline of International Relations (IR) - has shown, both defining (in)security (Bigo, 2008; Bigo & Tsoulaka, 2008; Peoples & Vaughan-Williams, 2010) and the development of technology is fundamentally political (Aradau, 2010; Leese & Hoijtink, 2019). Through their involvements in security and war, Big Tech companies are thus engaging in deeply political practices without there being clear measures to keep them accountable for the impact their practices have on global politics, societies, marginalized groups, and individuals (van Dijck et al., 2018). Big Tech's turn to artificial intelligence (AI) as an all-round security solution even has a significant impact on the climate due to its carbon emissions and energy consumption (Crawford, 2021; Dhar, 2020).

Critical voices ranging from European Union and United States regulators, academics and NGOs, to Big Tech's own employees are raising concerns about Big Tech's involvement in security and war. Google especially received a lot of critique in response to its collaboration with the United States Department of Defense (DoD) in the AI drone program called Project Maven. Lucy Suchman and colleagues in a pressing opinion piece in *The Guardian* asked:

> Should Google, a global company with intimate access to the lives of billions, use its technology to bolster one country's military dominance? Should it use its state of the art artificial intelligence technologies, its best engineers, its cloud computing services, and the vast personal data that it collects to contribute to programs that advance the development of autonomous weapons? Should it proceed despite moral and ethical opposition by several thousand of its own employees? (Suchman et al., 2018)

Big Tech's involvement in security and war relates to several existing themes in critical security studies and new media studies. One of these themes is the role of commercial expertise in security, which focuses on how private military and security companies can shape what can be understood as security threats and solutions as states have come to rely on their expertise, technology, and other resources (see e.g. Leander, 2005b). Closely related to this is the theme of algorithmic security, which explores how the turn to (commercially built) algorithms in security (re-) shapes practices and understandings of security (Roberts & Elbe, 2017). Another theme is the socio-political role of Big Tech

platforms that have reached infrastructural importance. This theme explores how platforms expand to new sectors through their technical innerworkings and examine the socio-political impact of this expansion (see e.g. Helmond et al., 2019; Plantin et al., 2018). Lastly, but not finally, it is important to mention the emerging theme of the relationship between Big Tech companies and governments, which focuses on how to regulate Big Tech's increasing power position in society (van Dijck et al., 2018; see e.g. van Dijck, 2021). But despite extensive research on Big Tech by new media studies literature and a rich literature in critical security studies literature on private security and the role of security technology, research on Big Tech's position in and impact on security and war remains minimal.

In this PhD thesis, I engage with and contribute to critical security studies and new media studies by addressing the gap in the literature around Big Tech's role in and impact on security. I do so through an empirical focus on Google, which is arguably the most deeply entangled with digital life and the most publicly critiqued Big Tech. More specifically, it poses the following research question:

> ***How does Google build on its digital dominance to expand and navigate its position in the security domain?***

As this introductory chapter will explain, this thesis addresses this question from an interdisciplinary perspective that combines insights from both critical security studies and new media studies over the course of four interrelated but stand-alone empirical chapters. This joint perspective enables an analysis of Google's knowledge practices and a deep exploration of the platforms and infrastructures that Google mobilizes in its security work.

Algorithmic war and security

While Big Tech's involvement in security and war is increasingly growing more prominent, it does not come out of the blue. In this section I engage with literature from critical security studies, a subdiscipline of International Relations (IR), to position Big Tech's involvement in the broader context of Big Data, algorithmic security, and the commercialization of security. Doing so helps us understand why Big Tech have both the data and the data analysis

capabilities that are deemed essential to modern day security and war (Hoijtink, 2022).

Within critical security studies researchers like Louise Amoore and Marieke de Goede have illustrated how after 9/11 national security actors have been collecting and analyzing more and more data to preempt security threats (Amoore, 2009a; Amoore & de Goede, 2005, 2008; de Goede et al., 2014; Wesseling et al., 2012). Preemption is understood as "security practices that aim to act on threats that are unknown and recognized to be unknowable, yet deemed potentially catastrophic, requiring security intervention at the earliest possible stage" (de Goede et al., 2014, p. 412 building on Aradau and Van Munster, 2007, 2011). With the threat being unknown, security actors turn towards collecting as much data as possible and relying on algorithms to make these data sets actionable. As put by Louise Amoore: "[b]y connecting the dots of probabilistic associations, the algorithm becomes a means of foreseeing or anticipating a course of events yet to take place" (2009b, p. 22). This turn towards large scale data analysis is made possible, and in turn reinforces, the datafication of social reality (Mayer-Schonberger & Cukier, 2013).

When the Snowden revelations showed us that actors like the National Security Agency of the United States (NSA) and the British equivalent Government Communications Headquarters (GCHQ) collect so-called "Big Data", discussions around how data collection impacts security practices intensified. Big Data sets are marked by their volume, variety and the velocity of the data collected that require significant computing power to analyze (Kitchin, 2014). Critical data studies and critical security studies scholars have explored how policy makers were convinced that Big Data was to be game changer for both security (through predictive policing) and governance (Andrejevic & Gates, 2014; Aradau & Blanke, 2015; Beer, 2016; Crawford et al., 2014; Crawford & boyd, 2012; Lyon, 2014; Metcalf & Crawford, 2016; Ridgeway, 2017). In the hands of security professionals, Big Data would be able to predict crime and thus inform security practices (Aradau & Blanke, 2017). New media scholar José van Dijck describes this believe as dataism, which she defines as "a widespread belief in the objective quantification and potential tracking of all kinds of human behavior and sociality through online media technologies" (van Dijck, 2014, p. 198). The possibility to collect Big Data sets reinforced and expanded security professionals' belief in dataism

and their desire to develop algorithmic technology (Roberts & Elbe, 2017; Suchman et al., 2017). Algorithms would help to discover the needles in the proverbial haystack and inform "near-real-time decision making" (Aradau & Blanke, 2018, p. 384).

Critical security studies researchers contest this narrative and have developed a rich literature that problematizes algorithmic security and war (Bellanova et al., 2021; Bode et al., 2024; Gould et al., 2024; Schwarz, 2021; Suchman, 2020; Wilcox, 2017). As succinctly put by Louise Amoore and Rita Raley, we need to examine what happens when we approach security through algorithms because "they filter, expand, flatten, reduce, dissipate and amplify what can be rendered of a world to be secured" (2017, p. 5). Algorithms might seem neutral, or at least less biased than human beings, but since the data they draw from can never be complete the decisions they inform are inherently political. As algorithms are inherently opaque (Burrell, 2016) and humans tend to believe computers, it becomes difficult to recognize and combat their political impact. It is widely acknowledged that the Big Data discourse originated in the commercial sector (Elish & boyd, 2018). However, relatively little attention went out to the platforms and digital services that made the collection of new types of data possible in the first place.

I argue that the literature on algorithmic security and war has not yet sufficiently focused on the role of Big Tech. However, there *is* a rich literature within critical security studies that has examined the role of private military and security companies. These contributions have explored how such private military and security companies define new threats that their expertise and technologies can counter (Abrahamsen & Williams, 2007; Leander, 2005b, 2005a, 2010). Their impact on security is significant. As Anna Leander has summarized:

> [t]he trouble is that the growing weight of security experts and their discourses in the production of legitimate knowledge risks overshadowing the kinds of 'long term' solutions everyone sees the importance of. The dominance of private military discourses crowds out the prior question of whether or not a problem is really a security problem, and if so, whether or not military/policing is the most adequate response. (2005b, p. 824)

That said, critical contributions to this literature do not argue that private military and security companies nessecarily erode state power and authority. Instead, the involvement of private military and security companies has led to global security assemblages, which are "settings where a range of different global and local, public and private security agents and normativities interact, cooperate and compete to produce new institutions, practices, and forms of security governance" (Abrahamsen & Williams, 2009, p. 3). Building on the private security literature, scholars have increasingly been drawing attention to the involvement of non-security actors like banks, airlines, and hospitals (Amicelle & Jacobsen, 2016; Bures & Carrapico, 2017; Carrapico & Farrand, 2017; Favarel-Garrigues et al., 2008; Heath-Kelly, 2017). In contrast to the security/defense industry, these companies and organizations are often ambivalent if not outright reluctant to be tasked with security responsibilities (de Goede, 2018). But the more that large-scale data analysis becomes central to security and war, the more that these companies and organizations are (t)asked to scan, collect, and share data with national security actors. It is within this context that some researchers have focused on the role that social media companies (which are largely owned by Big Tech) are forced to take up through content moderation. Rocco Bellanova and Marieke de Goede have illustrated how despite initial reluctance, social media platforms and EU security authorities co-produce security decisions, e.g. whether and when content needs to be referred, removed, flagged, or filtered (Bellanova & de Goede, 2022a). This finding is in line with earlier work that stressed how the boundary between public and private actors becomes blurry as they work together on security.

The development of Big Tech becoming involved in security and war thus builds on earlier and broader developments that critical security studies researchers have studied extensively. Only a handful, however, focus on those who develop the underlying technologies and data production are at the core of these developments: Big Tech (Gilbert, 2019; Hoijtink, 2022; Suchman, 2020). The involvement of Big Tech in security and war could be read as a continuation or expansion of these developments. But Big Tech's involvement *does* raise new questions and concerns. As the next section shows, there is good reason to assume that Big Tech's role in security and war warrants specific attention, given their already powerful position in society.

Platform power and digital dominance

Where critical security studies literature touches on Big Tech in passing, other literatures in new media studies – and to a lesser extent International Political Economy - focus on Big Tech's significant socio-political impact on society and the economy at large, which is also referred to as Big Tech's digital dominance (Moore & Tambini, 2018). In this section I build on these literatures to argue why Big Tech's involvement in war and security requires close examination.

At the center of Big Tech's power is their ability to collect and analyze user data throughout their seemingly free ecosystem of platforms (van Dijck et al., 2019). To visualize how platform companies function within an hierarchical and interdependent ecosystem, José van Dijck introduces the metaphor of the tree (van Dijck, 2021). This tree "consists of three interconnected layers: the roots of digital infrastructures all leading to the trunk of intermediary platforms which branches out into industrial and societal sectors that all grow their own twigs and leaves" (van Dijck, 2021, p. 5). The wealth of data that these interoperable ecosystems produce all serve as input for Tech machine learning algorithms. In turn, Big Tech can use these algorithms to develop new products and/or platforms to expand into various new markets. Or to use van Dijck's metaphor of the tree: to grow new branches, twigs and leaves. As these new platforms in turn generate new data, it becomes clear that expansion and diversification is an essential part of the Big Tech logic (Plantin & Punathambekar, 2019).

In a more zoomed in look into these processes of expansion and diversification, new media researcher Anne Helmond has explored how Big Tech expand into other markets through the technical architecture of their platforms. She argues that Big Tech platforms lock-in third parties by offering them ways to connect and make use of their platform features (2015). For third parties this is rather convenient: they can make use of the functionalities of successful platforms and do not have to develop their own. Giving third parties these abilities in turn strengthens Big Tech: it allows them to collect user data on the websites of these third parties in a format that suits Big Tech objectives. This, Helmond argues, leads to platformization, which she defines as "the rise

of the platform as the dominant infrastructural and economic model of the social web and the consequences of the expansion of social media platforms into other spaces online" (2015, p. 5). Through platformization, Big Tech platforms have become so entangled with many other markets and industries that they have reached infrastructural scale and ubiquity (Plantin et al., 2018; Plantin & Punathambekar, 2019). Their platforms have transformed into platforms-as-infrastructures (Helmond et al., 2019). In summary, new media studies has shown that through "the vertical integration of platforms, the infrastructuralization of intermediary platforms, and the cross-sectorization of platforms" Big Tech have developed a dynamic ecosystem of powerful platforms (van Dijck, 2021, p. 8).

There is a developing literature in International Political Economy (IPE) that also states the political importance of Big Tech. While most of IPE has a self-proclaimed blind spot when it comes to Big Tech companies (LeBaron et al., 2020), a number of them have drawn attention to Big Tech's unique economic position (Birch & Cochrane, 2022; Hendrikse et al., 2022). Central to these works is the understanding that the position of Big Tech is "qualitatively different from conventional hierarchically organized corporate, military, or business actors. It is something 'other' than simply a modern iteration of a monopoly-holding corporation, as indeed its own self-definitions insist" (Monsees et al., 2023, p. 11). What makes Big Tech different from previous companies that had infrastructural importance, is that they "enjoy a tight, even intimate, connection to their users" (Culpepper & Thelen, 2020, p. 290). Their users are willingly locked into their ecosystem as this results in a high level of convenience.

Maha Rafi Atal argues that while Big Tech are centralized companies, they deliberately portray themselves as a fragmented and decentralized range of platforms and digital services that are active across a range of sectors (Atal, 2021). This makes it difficult to regulate Big Tech companies on a general level. As Atal states, they "exploit the ambiguity created to thwart both rhetorical and regulatory challenges to their power"(2021, p. 337). Other technology companies struggle to compete with the scale of Big Tech companies, who benefit from network effects and winner-takes-all dynamics (Birch & Bronson, 2022). Finally, Shoshana Zuboff draws our attention to the significant impact of Big Tech on the global economy. In her influential book, she draws out how Google's approach to targeted advertising introduced "surveillance capitalism" (Zuboff, 2019b). This new form of capitalism is

based on a "new logic of accumulation" that is focused on turning user data into a raw material. Going against the common statement that users of free platforms have become the product, Zobuff argues that "users are neither buyers nor sellers nor products. Instead, users are the human natural source of free raw material that feeds a new kind of manufacturing process designed to fabricate prediction products" (2019a, p. 3). These Google products were so successful that this model has since become the "default model for most internet-based businesses" (Zuboff, 2019b, p. 10).

What becomes clear from this literature discussion is that the dominant position of Big Tech companies might originate in the digital, it impacts the economic, social, and political realm. But surprisingly, there is little attention in these literatures regarding the role that Big Tech play in security. Given the political nature of security and technology, and the already significant political role that Big Tech play in society, this gap is both surprising and problematic.

The research question and interdisciplinary approach

Bringing new media studies literature on Big Tech's digital dominance in conversation with debates in critical security studies on private security and the productive role of technology, in this section I draw out new concerns that Google's involvement in security raises and foreground my overarching research question.

In earlier sections of this introduction, I have illustrated that new media studies and wider studies of Big Tech highlight Big Tech's digital dominance to capture the powerful position that these companies have (Moore & Tambini, 2018). The meaning of digital dominance goes beyond Big Tech's respective economic dominance. Rather, it points to the interconnected ecosystem of Big Tech platforms and services, the impact of platformization on society, their infrastructural scale, and the impact of their knowledge practices. I have also shown that critical security studies literatures on private security point us to the essential role commercial actors play in shaping understandings and practices of (in)security through their technical expertise and the technical "solutions" that they offer. Looking at Big Tech's increasing role in security and war through both lenses, the main concerns of this PhD thesis become clear. What happens when (in)security is shaped by digital dominant commercial actors on whose digital platforms and services many individuals, business

and even governments already depend? How do Big Tech's commercial objectives and practices inform what or whom they deem to be security threats, objectives and solutions? How do they position themselves vis-à-vis national security actors? And how do they navigate the increasing public critique that is aimed at these partnerships? Addressing these concerns, this thesis poses the following research question:

> ***How does Google build on its digital dominance to expand and navigate its position in the security domain?***

To unpack how this question addresses the concerns raised above, let me start with explaining the empirical focus on Google. From a pragmatic perspective, considering the scope of this PhD thesis, exploring the role and impact that Big Tech has on (in)security requires a focus on a specific company. As research from IPE and new media studies has shown us, Big Tech companies have similar business models and have reached a comparable level of scale and infrastructural importance. They might be direct competition for certain contracts with the US DoD but, as José van Dijck has argued, they gain power as a collective (van Dijck, 2021), especially when it comes to navigating calls for stricter regulation. As such, Big Tech has become a relevant research object. But that is not to say that Big Tech is a monolithic group. Critical security studies scholars broadly understand political power as relational, situated and thus context dependent. From this perspective, it is important to acknowledge that Big Tech each have their own political power that depends on their unique cocktail of platforms and services, senior management, etc. Therefore, as argued by Monsees and colleagues "the politics of Big Tech cannot be reduced to one overarching logic or explanatory principle" (2023, p. 3). Their platforms each raise their own set of specific questions that deserve attention. To do justice to their comparable but ultimately unique political positions and impact, as well as considering the scope of this PhD thesis, I focus on one Big Tech: Google.

One might ask: why Google? However, the question can just as easily be: why *not* Google? To give a sense of how Google compares to other Big Tech, let me give a short (incomplete) overview of its main devices, platforms and services. Like Microsoft, Google has a search engine (Google Search). Like Amazon and Microsoft, Google is involved in cloud services (Google Cloud) which it leverages to pursue contracts with the US DoD. Like Apple it has an operating system (Android), an app store (Google play), a browser (Google

Chrome), its own hardware devices like smartphones (Pixel Phones), laptops (Chromebooks), tablets (Pixel Tablets), a smart watch (Google Pixel Watch), a digital map (Google Maps), and a smart TV (Chromecast). Like Amazon and Apple, Google has a smart assistant (Google Assistant) and a smart home system (Google Nest Hub). Like Amazon, Google is involved in online shopping and targeted advertising (through Search). Like Meta-Facebook, Google is the owner of a social media platform (YouTube) and thus involved in content moderation (Gorwa et al., 2020a; van Dijck et al., 2023), and an open-source machine learning platform (TensorFlow). Like all other Big Tech, Google is active in cybersecurity and the development of artificial intelligence (Google Gemini, a large language model, being its latest manifestation of that effort).

While not the biggest Big Tech in terms of revenue or market capitalization, which in 2024 are Amazon and Apple respectively (*Largest Tech Companies by Market Cap*, 2024; *Top Publicly Traded Tech Companies by Revenue*, 2024), given the many overlaps Google has with the practices and platforms of other Big Tech, Google is arguably the most deeply and widely entangled with digital life. Additionally, between 2017 and 2019, Google was involved in a highly controversial project with the United States military, known as Project Maven, in which Google assisted the military in adopting machine learning to analyze drone footage. Since then, more so than the others, Google has faced critique from tech workers and regulators alike. A study of how Google becomes involved in security work could therefore be read as a paradigmatic case of how Big Tech become involved in security.

To explore how Google builds on its digital dominance to expand and navigate its position in the security domain, I bring new media studies to International Relations, in particular the literature that sits at the intersection of Science and Technology Studies (STS) and critical security studies. While new media studies and STS-inspired critical security studies are rooted in different disciplines, and each deploy a rich variety in approaches and concepts, what unites these two fields is a socio-technical understanding of technology.

International Relations has traditionally analysed technology from an essentialist or an instrumentalist perspective (Leese & Hoijtink, 2019). These perspectives do not unpack technology, such as how it works or who developed it under which circumstances. Instead, they take technology as a given, as a neutral tool that can be used by states to support their position

(instrumentalist), or as "a central driving force for progress" that impact global politics as a whole (Leese & Hoijtink, 2019, p. 9). In recent years, a rich literature has developed in critical security studies that foreground the role that technology plays in co-constituting security (Amoore & Raley, 2017; e.g. Aradau, 2010; Aradau, Hoijtink, et al., 2019; Aradau et al., 2014a; Bellanova & de Goede, 2022a, 2022b; Bode & Huelss, 2023; de Goede, 2018; Leese & Hoijtink, 2019; Walters, 2014). As summarized by Mathias Leese and Marijn Hoijtink: "technological development and deployment is highly political and subject to social, institutional, economic and material possibilities and constraints, alongside preferences of developers, engineers, and designers" (2019, p. 10). As such, researchers have focused on how i.e. autonomous weapons, drones, and financial algorithms have impacted understandings and practices of (in)security (Amicelle et al., 2015; Amoore & Raley, 2017; Aradau & Blanke, 2018; Suchman, 2020; Suchman et al., 2017; Walters, 2014; Wilcox, 2017).

With a similar focus on the productive and political effect of technology, new media studies scholars have paid attention to Big Tech platforms (Blanke & Pybus, 2020; Gillespie, 2010, 2018, 2020; Helmond, 2015; Helmond et al., 2019; Nieborg & Helmond, 2019; Plantin et al., 2018; Plantin & Punathambekar, 2019; Plantin, 2018; van Dijck, 2020, 2021; van Dijck et al., 2019; van Dijck & Poell, 2015; van Dijck & Rieder, 2019). While individual approaches differ, most of the new media studies literature on platforms points to both the technical and the discursive impact of platforms. Besides a focus on the platform, what this perspective adds is an understanding of "the industry logics, practices, and imaginaries that ensure the reach and global scale of dominant platform companies" (Plantin and Punathambekar, 2019, p. 164). As Google's security involvements do not exist in a vacuum, these insights are essential to contextualize and trace how Google's commercial objectives inform how it *expands* and *navigates* its position in the security domain. By combining critical security studies with new media studies, I thus develop an interdisciplinary theoretical approach that considers the productive effects and affordances of technology, unpacks Google's business logic, and examines its (in)security knowledge practices. Engaging in a dialogue between these two sets of literatures is necessary to answer such an interdisciplinary research question.

My interdisciplinary theoretical starting point has implications for how I understand digital dominance. As IR literature on private security has

shown us earlier in this chapter, the state is still a relevant actor whose authority is not necessarily eroded by closely working together with private security companies. In the case of Google, states can task it with specific responsibilities (content moderation is a good example of this), demand that it follows regulation (such as the EU General Data Protection Regulation or the Digital Markets Act), call its senior management in for hearings (which has happened multiple times in the US Senate), etc. The term dominance is therefore not to suggest that Google is under no state control whatsoever. Instead, I use digital dominance to bring into view how Google's pervasive ecosystem of platforms, the infrastructural scale of its services, and expertise in AI come to matter in its attempt to expand and navigate its position in the security domain.

The overarching research question is addressed over the course of four separate but closely related research articles, which all have their own literature reviews, conceptual frameworks, methods, and empirical material. These articles, which are included in this PhD thesis as chapters 2 to 5, answer the following sub questions:

1. How does Google appropriate security throughout its ecosystem of platforms, products and projects?
2. How can we account for the growing role of machine learning in the military domain?
3. How does Google navigate (in)visibility dynamics around its military AI practices to render possible its military investment and maintain its corporate image as a neutral responsible leader in AI?
4. How do browsers, especially Google-Chrome, as platforms-as-infrastructures exercise their infrastructural power in the CAB forum to shape the requirements for public web certificates?

Together, these sub questions unpack aspects of the larger puzzle at hand. While expansion and navigation go hand in hand, sub question 1 and 2 explore aspects of *expansion* and sub questions 3 and 4 examine aspects of *navigation*.

Let me start with explaining my focus on "expansion" in the overarching research question. Some have argued that Google's founders have been entangled with the US intelligence community since before they launched Google (Nesbit, 2017). While this is fascinating and worthy of closer examination, given my interest in how Google builds on its digital dominance,

I am interested in the various ways in which Google *expands* its position in the security domain. By taking this perspective, I can zoom in on how Google brings its security involvements in conversation with the commercial objectives of its existing platforms and services and navigates the frictions that exist between these two (the theme of chapter 2). Examining how Google expands into security also draws attention to the ways in which Google leverages its already successful products and platforms in collaborations with the United States military. This helps us understand how these platforms impact how the machine learning is picked up in the military domain (the theme of chapter 3). Then, I am interested in how Google *navigates* its position in the security domain.

With "navigation" in the terms of the overarching research question, I refer to the actions that Google takes to steer around and respond to critique and controversy. As Google cannot fully control the social context or situation it finds itself in, Google's senior management - like a ship at sea - can plot a course, but it needs to deal with the tides and sudden gusts of wind. A focus on navigation invites an exploration of *how* Google does this, and how this in turn impacts the position in takes up in the security domain. Sub questions 3 and 4 enable me to capture aspects of this navigation. More specifically, with the third sub question, I examine how Google engages with the increasing critique it receives regarding its security involvements (the theme of chapter 4). And with the fourth sub question, I examine how Google navigates the domain of internet standardization by firmly positioning its browser Chrome as the to-go infrastructure for online browsing and shaping cybersecurity standards for all those who make use of this infrastructure (theme of chapter 5). Taken together, I argue that by examining how Google builds on its digital dominance to *expand* and *navigate* its position in the security domain reveals the security politics of Google, its impact on algorithmic security, and the various ways in which Google relates to national security actors.

Methodology

This PhD thesis is theoretically situated in an emerging tradition within critical security studies that focuses on how technologies such as digital platforms and machine learning play a role in shaping (in)security understandings and practices. Methodologically, this PhD thesis builds on the "material turn" in critical security studies (Mutlu, 2013). Despite the focus on the agency of

technology, this "turn" is not underpinned by technological determinism. Instead, it argues for a relational view on technology and human actors (Aradau et al., 2014a; Aradau et al., 2014). This means that it considers discourse and materiality to be co-constitutive of (in)security, e.g. who or what needs to be secured from what and how (Aradau et al., 2014a; de Goede et al., 2020; Salter & Mutlu, 2013a). As such, discourse and materiality must not be separated (Aradau, Hoijtink, et al., 2019; Leese & Hoijtink, 2019). For this PhD thesis, this means that both the narratives present in the documents that introduce Google's security involvements, and the technical underpinnings of concrete projects and platforms co-constitute how Google expands and navigates the security domain. I therefore unpack how Google's security technologies work and the promises with which they are introduced. In other words, throughout this PhD thesis, I examine how Google *speaks* and *does* security.

A relational approach also means that research is not aimed at finding universal truths but examining situated practices. In the words of Aradau et al.:

> rather than trying to make general determinations as to the political significance of 'things', it is important to recognize that the relations between discourses and materialities are not universal but undergoing constant rearrangement according to the elements gathered together and the circumstances under which this occurs. (Aradau et al., 2014, p. 63)

When it comes to examining technogies, a relational approach means that "the practices of building AI systems – of doing machine learning or data science – cannot be divorced from the social contexts in which these technologies are situated" (Elish & Boyd, 2018, pp. 71–72).

Informed by these overarching methodological principles, I examine how Google expands and navigates its position in the security domain by adopting a relational, situated, and explorative approach (de Goede et al., 2020). In the following two subsections, I draw out the two interrelated methodological approaches that I deploy to answer my research question: following Google and decoding the technobabble. While this PhD thesis comprises four research articles that each have their own specific methods and empirical

material, the methodological approaches set out in this chapter are the basis of all of them.

Following Google

My first methodological approach to examining Google's involvement in security is *following* Google. Such an approach is helpful because instead of predefining what counts as security involvements, I can draw out what Google perceives as such (de Goede, 2018). What Google sees as a security issue or solution is an essential part of how it speaks and does security. But then, who or what is Google? There is a broad variety of and fragmentation between Google projects, platforms, and subsidiaries (Atal, 2021). Google also has an upward of 180.000 employees and is itself owned by its parent company Alphabet. This issue is further complicated by the velocity at which Google develops new projects and cancels others (296 initiatives have been cancelled as of October 2024 (see Ogden, 2024)). There is also the element of secrecy. The first aspect of Google's secrecy is based in the fact that Google is a commercial entity with commercial secrets. The second aspect comes from Google having classified contracts with national security actors through which it becomes enrolled in national security.

From a theoretical perspective that recognizes the agency of both technical materialities and human actors, one cannot understand Google to be one clearly defined monolith. Some have therefore tried to deploy the metaphor of the octopus or squid to as a thinking tool, where the many arms of the octopus represent the various arms of the company (Anne Helmond as cited in Cristofari, 2023). Such a thinking tool allows us to visualize how Google locks in users with its many suction cups or how it obfuscates its actions using the excretion of ink. Furthermore, as argued by Monsees and colleagues "Big Tech [in my case Google] is continuously envisioned, performed, and enacted at heterogeneous sites, places, and times in need of constant coordination and negotiation" (2023, p. 6). Consequently, I do not put predefined limits on who or what to follow. Instead, I adopt an exploratory approach to study the ways in which Google shows up in technical ways, through the products and platforms puts out in the world, the security discussions it gets involved in, etc. That said, as Maha Rafi Atal has argued, Big Tech like Google benefit from being seen as fragmented and decentralized (2021). As she puts it, these companies "exploit the ambiguity created to thwart both rhetorical and regulatory challenges to their power" (Atal, 2021, p. 337). While I do not consider Google to be not a monolith but a complex ecosystem of platforms

and people, there is value in referring to this ecosystem as “Google the company”. Doing so draws attention to how the diverse platforms, products, and projects that exist under the banner of Google are connected and together empower the company as a whole. Whenever I refer to “Google”, I thus refer to “Google the company”. When and where it is relevant and possible to specify who is speaking, I use more specific terms like “Google employees” or “Google’s senior management”.

To navigate Google’s secrecy practices, I follow a rich literature in critical security studies that considers secrecy not something that always needs to be overcome in one way or another. This literature argues that “[i]t can be revealing in itself to map and analyse secrecy, obfuscation and the blurry boundaries of the visible and invisible” (de Goede et al., 2020, p. 10; see also de Goede & Wesseling, 2017; Van Veeren, 2018; Walters, 2021). I thus stay attentive to how Google is engaged in black boxing (Straube, 2020), but it is not the aim of this thesis to define or capture all of Google. Following Google also entails that I did not adopt a predefined geographical scope at the start of this PhD thesis. However, recognizing that Google is mostly involved with the United States government and the (members of the) European Union and that my own geographical location is The Netherlands, means that my results regarding Google’s involvement with state actors is limited to these areas of the world.

Adopting an inductive, exploratory approach where the sub questions were not predefined but identified throughout the research, allowed me to “keep up” with Google. However, given that Google is constantly changing, chronologically tracing and mapping everything that Google builds on its digital dominance to expand and navigate its position in the security domain would not be feasible. Instead, I aim to identify the semi-stable logics and socio-technical practices that broadly characterize how Google builds on its digital dominance to expand and navigate its position in the security domain. Here I am particularly interested in the seemingly mundane, technical ways in which Google is involved in security. While decisions made by Google’s senior management are important, in the words of Jef Huysmans, I also pay attention to “the little security nothings” (Huysmans, 2011). In the case of Google, these little nothings consist of small policy changes, small seeming side projects, email discussions about the right interpretation of security standards, details of the technical innerworkings of platforms, etcetera. Together, these mundane, often technical details impact how Google speaks

and does security. To capture and analyze these details, I relied on an extensive qualitative document analysis of a large amount of publicly available primary Google sources, such as technical documentation, policy documents, blogs, official announcements, news articles, product descriptions, product demos, instruction videos, GitHub documents, public email lists, etc. To make this collection of sources available to other researchers, I placed them in a publicly available online repository (see Appendix A). This repository can be filtered on date of publication, author, title, item type, and website title.

Each chapter has a slightly different approach to the document analysis given the different objective and question, but in general I analyzed my material by paying attention to how things were described as security challenges or solutions. I examined how Google representatives – or Google documents without a clear author – presented their arguments. By examining many materials, I could identify and trace the logic that was embedded in the texts. Over time, I could identify core themes, concerns, and promises that kept coming back (Aradau et al., 2014b; Salter & Mutlu, 2013b). Simultaneously, I contrasted these concerns and promises by examining how the underlying technologies work and whom or what these projects favored. For instance, I examined whether and how proposed policy changes or new features would lock in new users. To do so, I unpacked what the technical terms meant and how these would function in practice (which I did by "decoding the technobabble", my second methodological approach which is explained in the next sub section). I complemented this analysis by examining press statements by spokespersons, as well as public letters or public appearances of Google's senior management and executives. These documents might not tell the entire story, as it is impossible to know if there are products and projects that Google keeps secret. When possible and relevant, I therefore examined documents and emails leaked by critical employees. Exploring the discrepancies between Google's public narrative and the internal narrative sheds additional light on how Google wants to be known in the security domain. This combined approach enabled me to tease out how various types of Google texts, statements, and the underlying technologies together shape how Google does and speaks security (van der Vlist et al., 2024 have recently referred to this as technography).

The research loosely spans Google's involvement in security between 2014 and 2023. In 2014, following the spread of terrorist propaganda by ISIS on social media, Google, Facebook, Twitter and Microsoft were tasked with

content moderation responsibilities by for example the European Commission (European Commission, 2014; Bellanova & de Goede, 2022a). Back then, these companies were reluctant to become involved in deciding what content was unacceptable as such decisions are inherently political (de Goede, 2018). In 2023, however, Google is involved in military contracts with the Unites States (Welch, 2024) and Israel (Perrigo, 2024), and is providing various cyber security services to Ukrainian organizations (Zmuda, 2022). Further, Google takes part in expert groups that advice policy making by the European Union, such as the High-Level Expert Group on Artificial Intelligence (Bode & Huelss, 2023). This timespan thus allowed me to capture a change in Google's approach to security.

Lastly, a note on positionality. It is not this thesis' intension to paint the picture of Google as "bad". Instead, I examine "situated sociotechnical practices [...] to make conclusions and judgments about [Google's] politics" (Monsees et al., 2023, p. 7). I do so because the main concern of this PhD thesis is Google's involvement in security given its powerful position in society. It is, however, important to recognize that through my research, I can potentially reinforce this power position (see Hoijtink, 2020). To strike a balance between problematizing Google's power position and not reinforcing it, I draw attention to Google's failures and the technical limits to it platforms wherever relevant and necessary.

Decoding the technobabble

To follow Google, I needed to be able to deal with the complexity of the technology that Google develops and deploys in name of security. Google engages in cybersecurity practices that include complex (encryption) protocols and uses algorithms that are becoming more complex as machine learning/artificial intelligence becomes more prominent. The technical documents that describe Google's products, projects, and platforms are thus steeped in technical jargon that assume a certain level of computer science knowledge from its readers. To deal with the complexity of the technology, my second methodological approach is what I call "decoding the technobabble"[2].

2 In science fiction, such as my beloved Star Trek, "technobabble" is meant to capture the nonsensical technical jargon that is rapidly shared by the characters to explain why the starship is facing an immeasurable threat and what needs to be done to counter it (see Tremeer, 2019). While I do not suggest that the technical jargon I unpack in this PhD thesis is nonsense, I use the term technobabble because to outsiders it can come across as illegible.

In critical security studies there is a rich but emerging literature in which scholars explore the functioning of technology and immerse themselves in the professional lifeworld's to gain access to the field of their interest and specific security practices (Amoore & Raley, 2017; Gusterson, 2008; Hoijtink, 2022; Salter & Mutlu, 2013a; Suchman et al., 2017). While I build on these approaches, I also push them forward by "decoding the technobabble". I do so by bringing in the emerging methodological approaches in new media studies that unpack the technical innerworkings of platforms in even more detail (Helmond, 2015; Helmond et al., 2019; Helmond & van der Vlist, 2021; Helmond & Vlist, 2019; van der Vlist et al., 2022).

Throughout the research, I explored the basics of Big Data, algorithms, machine learning and the platforms they require, the intricacies of open-source platforms, and internet protocols. Inspired by Rob Kitchin's work on how to study algorithms (2017), I did so by familiarizing myself on the innerworkings of machine learning platforms, following an online Coursera course called "AI For Everyone" by cofounder and former head of Google Brain Andrew Ng (2020), watching educational videos and conference streams, walking through machine learning tutorials, reading tech blogs and newsletters, reading professional literature, technical documentation. All these materials are part of the online data repository which, together with the primary Google sources, consists of almost 700 items (see Appendix A). Additionally, I read a book on asymmetrical encryption by encryption expert Bruce Schneier (2015), and – perhaps most importantly - continuously double checking my technical understandings through informal chats with the cybersecurity experts, computer scientists, and coders that are part of my social circle.

While information about some of Google's platforms and products is proprietary, I build on insights by Claudia Aradau and Tobias Blanke, who remind us of the fact that even if you had access that does not mean that you could see or understand more as algorithms based on machine learning/AI are often inherently opaque (Aradau & Blanke, 2017). They have also shown us that these technologies are not as secret as we often think they are. As Aradau explains: "it is very unlikely that the NSA [or in my case Google] will have technologies that are more developed than the stateof-the-art in computer science" (2019, p. 200). This state of the art is something I have been able to access, and so – albeit indirectly – I have learned about the innerworkings of for instance a particular machine learning method.

Getting a better grip on the technologies that Google uses and develops to expand into the security domain also helped me navigate the fast-changing technology discourse. Back in 2018, the discussion was all about the promises and challenges of Big Data and algorithms. In 2024, the discourse has moved on to artificial intelligence and large-language-models (LLMs). Instead of immediately going along with hypes arounds new technology, I asked: what type of machine learning is used here? What kind of platform technicalities or computational infrastructure is needed for this? Asking these questions helped me to situate the latest technological improvements and understand on which foundations it builds.

For chapter 5, I supplemented my research with 8 in-depth semi-structured background interviews[3] with a set of practitioners and encryption experts on online certificate management (a cybersecurity practice). Most of my interviewees, whom I interviewed over the course of the period between November 2022 and July 2023 (see Appendix B), had either been directly involved in the cybersecurity standardization forum I was interested in (the Certificate Authority Browser Forum) or were familiar with its policies. As most of the interactions between the forum members happens out in the open (their email conversations are largely public and so are the incident reports and the minutes of their face-to-face meetings), most of what they told me was not sensitive. However, what did make the interviews sensitive is the fact that the world of certification is rather small. Most of them know each other, be it personally, by name, from public email conversations, or from the face-to-face meetings of the forum. Asking them about their personal views on the work being done by the forum, what they found to be relevant developments, and how they experience the dynamics between the members, was more sensitive. Given the wealth of other available data, I therefore decided that it would be sufficient to use the interviews as background interviews.

To gain access to the community, I first reached out to the cybersecurity experts in my social circle, who referred me to an expert with the relevant experience and expertise. From there, I "snowballed" from one interviewee to the next, as all of them were willing to refer me to someone they thought

3 The way in which I conducted and stored these background interviews has been approved by the Ethics Review Board of the Faculty of Social and Behavioral Sciences of the University of Amsterdam, "2021-AISSR-14084 Big Tech: emerging security actors".

would be able to add a different perspective. I continued this approach until my interviewees confirmed that I had a good comprehension of the technology, when the same themes kept coming back, and the same issues and incidents were brought up. As Hugh Gusterson has pointed out, using snowballing in this way can create an echo chamber (2008, p. 98). But as I had access to publicly available emails in which I could directly see how people communicated with each other, I was confident that my understanding of the community was valid. The email lists and the interviews confirmed my interpretation of each.

To keep the interviews engaging for my interviewees, I used the methods of "branching" and "building" as suggested by Hugh Gusterson (2008, p. 104). Starting with the latter, I was able to "build" my interviews by structuring them around three core themes: i) the technology (how it works, its relevance for cybersecurity), ii) the innerworkings of the internet standardization forum, and iii) specific security/compliance incidents in the domain of certification. By discussing these themes with each interviewee, my knowledge and understanding of these themes developed, which meant I could ask more detailed questions about specific situations. This, in turn, allowed me "branch": I could tailor my questions to the positions and backgrounds of my interviewees. For instance, to the Dutch experts I asked more about the Dutch case I was interested in.

In summary, following Google and decoding the technobabble enabled me to examine both Google's security discourse and the technical underpinnings of its security involvements, and draw attention to the seemingly mundane technical ways in which Google is involved in security. My overarching methodological approach also enabled me to explore, to go back and forth between theory and empirics, and deploy a multiplicity of concepts.

Thesis structure

This PhD thesis is a collection of four chapters that each have their own specific research questions and empirical material. These research questions were identified inductively throughout the research as relevant sub questions. That means that while they mobilize different concepts and analyze different empirical data, the chapters are closely connected as one chapter led to the next.

Chapter 2 starts from the assumption that non-security actors, other than private security and military companies whose business model is focused on addressing security threats, are reluctant to take up security responsibilities. This reluctance comes from an (initial) tension between their pre-existing logic, whether it serves commercial or public objectives, and the security logic. Building on Tarleton Gillespie's work on the platform logic (2010), in this chapter I argue that Google is such a non-security company and explore how Google makes security fit its platform practices and objectives. It does so by asking: *How does Google appropriate security throughout its ecosystem of platforms, products and projects?* As overviews of Google's products are hard to come by, this question required an extensive mapping exercise of Google's security involvements between 2014 and 2018. This mapping exercise sheds light how Google bridges the tension between its aim to be seen as a neutral yet progressive platform and its need to make inherently security judgements to expand into the security domain. The chapter shows the breadth of Google's security involvements and how Google upfronts artificial intelligence as a supposed neutral solution to the security problems it identifies.

Chapter 3, which is co-authored by Marijn Hoijtink, builds on the mapping exercise of the previous chapter which drew my attention to Google's open-source machine learning platform TensorFlow. This platform assists the development of real-world machine learning applications, which requires large amount of labelled data, expertise in building machine learning layers and digital infrastructure to be able to scale the resulting machine learning model. We examined how Google shares its expertise in machine learning through TensorFlow and how it builds on the contributions of the open-source community to TensorFlow's codebase. As TensorFlow was used by Google in its collaboration with the US DoD in Project Maven, this exploration allowed us to answer the following question: *How can we account for the growing role of ML in the military domain?* By answering this question, this chapter shows how TensorFlow allowed the US military to find solutions to the difficulties it was facing in building algorithms for its drone program. We explore how the DoD's use of TensorFlow leads to the platformization of the military. With this comes the involvement of Big Tech, start-up companies, and the open-source community that brings its expertise to TensorFlow.

Throughout the chapter 2 and 3, it became clear how Google's AI initiatives are paradoxically marked by both hypervisibility and invisibility. Google both

pushes its expertise in AI and obfuscates how and where it capitalizes on this expertise, especially when this involves working with the US military. Based on these observations, chapter 4 asks: *How does Google navigate (in)visibility dynamics around its military AI practices to render possible its military investment and maintain its corporate image as a neutral responsible leader in AI?* Asking this question enabled me to zoom in on Google's attempts at *navigating* its position in the security domain when it had to face critique on its collaboration with the United States DoD in Project Maven. The chapter explores how Google defends its position as a leader in AI and whose voices it attempts to stifle. But it also illustrates that despite its dominance in this field Google needs to relate to the world around it: Google cannot ignore the criticisms that it receives.

In chapter 5, I take a more zoomed in look at how Google's technical expertise works in practice and how it impacts the security practices of others. More specifically, I explore how Google's knowledge practices and its infrastructural position together impact cybersecurity practices. I do so by asking: *How do browsers, especially Google-Chrome, as platforms-as-infrastructures exercise their infrastructural power in the CAB forum to shape the requirements for public web certificates?* Through in-depth interviews with encryption and certificate experts and an extensive analysis of various email lists, this chapter explores how Big Tech infrastructural power manifests itself and how Google's authority and expertise directly impacts the cybersecurity practices of governments through internet standardization.

In the concluding chapter of this PhD thesis, I draw out what these chapters bring into view, both empirically and conceptually. Here, I outline the three core arguments of this PhD thesis. First, I argue that Google's expansion into and navigation of the security domain enables the platformization of security. This includes both bringing security into its ecosystem of platforms and bringing the platform to places of security, such as the US military. Through this development, Google foregrounds its approach to AI as a neutral-seeming fix-all solution to security issues. Second, I argue that as Google entangles its platforms with security, the infrastructural position of Google's platforms and products is reinforced and expanded. I illustrate that this infrastructural

expansion happens through Google's open-source platforms and how Google sets de facto security standards for foundational security protocols. Third, I posit that Google navigates its position in the security domain by deploying (in)visibility politics. The fact that Google needs to balance which of its security involvements it highlights and which it pushes to the background, illustrates that Google is not as impervious to criticism as it is sometimes portrayed. Then, after unpacking these arguments and explaining how these contribute to critical security studies and new media studies, I reflect on what my contributions mean for the possible regulation of Google and Big Tech more broadly. Finally, I draw out three avenues of research that are essential to deepen our understanding of the innerworkings and political implications of Google's increasing involvement in security.