Google's expansion into security

Platforms, infrastructure, (in)visibility

van Hardeveld, A.A.

Publication date
2025

CHAPTER 6

Conclusions

Introduction

Since I started my PhD thesis in 2018, Google has only become more involved in security and war. For example, in 2021, Google and Amazon signed a 1.2 billion US dollar contract to build a cloud computing system for the Israeli government and military (Ziv, 2021). This contract, referred to as Project Nimbus, has been heavily criticized by Google and Amazon employees (Anonymous Google and Amazon workers, 2021). Fifty employees were fired after taking part in sit-in protests in 2024 (Sainato, 2024). Less controversial but potentially highly impactful, in July 2024, Google announced a new coalition called "Coalition for Secure AI (CoSAI)" with Amazon, Microsoft, IBM and others to set cybersecurity standards for AI (Adkins & Venables, 2024). As argued by Google's vice-president of Security Engineering, Heather Adkins, and the Chief Information Security Officer of Google Cloud, Phil Venables "AI developers need — and end users deserve — a framework for AI security that meets the moment and responsibly captures the opportunity in front of us. CoSAI [Coalition for Secure AI] is the next step in that journey..." (Adkins & Venables, 2024).

Concerned with these developments, especially when considering Big Tech's deep entanglement with our daily digital lives, this thesis has asked the following research question: *How does Google build on its digital dominance to expand and navigate its position in the security domain?* Asking this question enabled this PhD thesis to contribute to broader themes such as the role of commercial expertise in (in)security, the proliferation of data-driven technology in security practices and the infrastructuralization of Big Tech platforms.

In this final chapter I summarize my empirical contributions and draw out how these findings lead me to three main arguments regarding Google's platformization, infrastructural expansion and (in)visibility politics. In explaining these arguments, I illustrate the main theoretical contributions that this thesis makes to both critical security studies and new media studies. This chapter concludes by reflecting on how the findings of this PhD thesis relate to debates about the regulation of Big Tech and drawing out three avenues for future research.

Summary & empirical findings

By unpacking how Google builds on its digital dominance to expand and navigate its position in the security domain, my PhD research has led to various novel empirical insights. Informed by literature on how non-security actors reluctantly "learn to *see* the world through a security lens" (de Goede, 2018, p. 26; see also Amicelle & Jacobsen, 2016; Bures & Carrapico, 2017), I started my research with the assumption that Google would be similarly reluctant to take up inherently political security responsibilities. This assumption is based on new media studies' understanding of Google's business model, which requires it to be perceived as a neutral, progressive platform that caters to its users, content providers and advertisers (Gillespie, 2010). In chapter two, I therefore asked how Google appropriates security throughout its ecosystem of platforms, products and projects. The concept of appropriation, here, is used to capture how Google makes security fit its commercial platform objectives, assuming that the latter still reign supreme (building on Amicelle & Jacobsen, 2016).

Addressing this question required an overview of Google's security initiatives. Such overviews, however, are far and few between. Even Google's own sites do not provide an overview of its project and platforms. I thus started off with mapping Google's security initiatives between 2014 and 2018, gathering and analyzing over a 160 Google documents, including press releases, blogs, and technical product descriptions (see Appendix A). This revealed thirty-two security products and projects that I mapped into three clusters (see Table 1, p. 44). The first cluster showed how Google locks-in new users by expanding its cybersecurity and privacy tools. The second cluster revealed that Google raises transparency as a security objective to keep its distance from governments that require Google to share user data for security purposes. Stressing its neutrality, Google aims to separate itself publicly from the actions and policies of governments and presents itself as a protector of all. The third cluster showed the ways in which Google approaches its platform moderation efforts, a security responsibility it is tasked with by EU and US regulators. It does so by outsourcing this responsibility to users and other companies and, where possible, to neutral seeming AI applications. Together, these clusters revealed that Google went from being somewhat ambiguous to be involved in security practices in 2014 to becoming more proactive in security in 2018 when it focused on becoming an AI-first company.

Chapter 3, which is coauthored by Marijn Hoijtink, builds on these findings by exploring Google's push for AI as a seemingly fix-all (security) solution and the products it builds to make the transition to AI possible. Building on new media studies' focus on the inner workings of platforms, we examined Google's open-source machine learning platform TensorFlow. We performed a detailed study of this machine learning platform by analyzing TensorFlow's technical documentation, watching educational videos, and walking through its tutorials. Doing so shed light on the work that goes into developing a machine learning model, including how the open-source community is involved in developing machine learning layers, and how such a platform facilitates the compiling of a machine learning application. This study also revealed how this platform enables Google to steer AI development towards deep learning, which is a controversial approach due its inherent invisibility. Examining TensorFlow then informed our analysis of the increased use and impact of machine learning in the military domain, as Google used TensorFlow for its collaboration with the Unites States Department of Defense (DoD) in Project Maven. For this project, Google helped the DoD in its effort to develop AI to analyze drone surveillance footage. The chapter shows that the US DoD turned to Google and its machine learning platform to help it address various issues it was having during the start of Project Maven. TensorFlow enabled the DoD to continuously centralize and label its data so it can be used to (re-)train algorithms. Simultaneously, TensorFlow helped the DoD to develop decentralized machine learning applications to make its data actionable. Exploring the innerworkings of TensorFlow and how it was used in the context of Project Maven thus shed light on how the US military practices become platformized. This includes a closer relation between the military and commercial companies like Google and shows the importance of the innovation done by the open-source community, who become enrolled into military developments without their knowledge.

Google's involvement in Project Maven became public knowledge through information leaked by critical employees to media outlet *Gizmodo*. Up to that point, both Google's senior management and the US DoD tried to keep Google's involvement in Project Maven hidden from the broader public. At the same time, Google gave (and still gives) hypervisibility to its other AI pursuits. From publishing AI research papers and creating free AI courses to starting an AI residency program. Observing these two different strategies, in Chapter 4 I asked how Google navigates (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. To answer this question, I examined how Google's senior management engaged in the controversy about whether Google was involved in developing AI for offensive purposes for Project Maven. By tracing who revealed what to whom, when and how, the chapter shows how the (in)visibility dynamics between the DoD, Google's senior management, and critical Google employees shifted as the controversy developed. At the start of the collaboration, the DoD hinted at its collaboration with a significant commercial partner to make Project Maven a success. The chapter showed that this approach was backed up contractually: any press releases had to be agreed upon by both parties. Together, the DoD and Google's senior management thus had a tight grip on the (in)visibility of Project Maven. After critical employees leaked information about Google's involvement in the project to the press, Google's senior management continued to keep its involvement vague. This triggered a push and pull dynamics between Google's senior management and Google employees, where the latter continued to leak information to critical media outlets like *The Intercept* and *Gizmodo* and the former tried to redirect the narrative towards its AI leadership. In response to the heavy critique it received, Google's senior management decided to not pursue a follow-up contract. But the controversy did not end there. Employees kept leaking information about the ways in which Google remained tied to the project through its venture capital arm. Meanwhile, members of the US government questioned Google's loyalty for its decision to not work with the US military. This led Google's executives to speak out publicly about Google's eagerness to be a proud military partner, setting a clear direction for the future.

In summary, this chapter has shown how Google's senior management engages with critique, especially when that critique comes from within, namely by keeping as much invisible as possible. This, however, results into a (in)visibility dynamic of push and pull, as Google needs to contend with critical employees who can leak important information to the press. Here we clearly see that Google is not a monolith, and its management cannot control it all. The chapter, however, also shows that despite the critique it received about its collaboration with the US military, Google's senior management remains committed to pursuing similar contracts. The commercial opportunities these contracts bring seem to outweigh the potential risks they bring to Google's reputation among its employees.

Finally, where chapters 3 and 4 shed light on Google's expansion into and navigation of a controversial space, chapter 5 explores how Google representatives are involved in internet and cybersecurity standardization, which is an important but overlooked way in which Google expands and navigates its position in security. It draws attention to a specific empirical case, namely the decision of the Dutch government to take a step back in how it provides its citizens with a secure online experience due to the dominance of Big Tech browsers in the Certification Authority Browser Forum, a cybersecurity standardization forum. Chapter 5 asked how browsers, especially Google-Chrome, exercise their infrastructural power in the CAB forum to shape the requirements for public web certificates.

On a general level, this chapter yields a detailed exploration of cybersecurity protocols and internet standardization practices: practices that have significant political impact on the possibilities for digital sovereignty but are rarely explored empirically by critical security studies scholars. In-depth background interviews with topic experts and practitioners over the course of November 2022 and July 2023 (see Appendix B), document research, and extensive email-list research showed how browsers like Google Chrome build on their infrastructural position to pro-actively shape the security requirements, police the community through setting conditions for who can(not) be trusted, and pressure the community towards automation. These findings showed that if governments want their online services to be accessible through Google Chrome, Apple Safari, Microsoft Edge or even the non-profit Mozilla Firefox, they have no other options than to follow the rules that these browsers set in this standardization forum. To be able to follow these rules, the Dutch government would need to invest in the automation of its digital infrastructure. Instead, the Dutch government decided to no longer be directly involved in providing its digital infrastructure providers with the certificates they need to be accessible through Big Tech browsers. Dutch digital infrastructure providers now need to rely on commercial vendors for these certificates. In summary, the final empirical chapter of this PhD thesis illustrated the ways in which Google Chrome can shape internet and cybersecurity standardization and showed why states need to abide by these rules if they want to make use of Google's browser infrastructure.

Taken together, these four chapters reveal that Google is no longer ambiguous when it comes to its involvement in security. It needs to manage its public image, but that does not stop Google from expanding into the security

domain throughout its ecosystem of platforms. It also indicates that Google's relationships with governments vary based on context. In situations where it needs to take actions that challenge its platform position, Google tends to distance itself from the government involved. When a Google platform provides services that have reached an infrastructural scale, then Google does not hesitate to treat governments just like any other user of its platform that needs to agree with the terms and conditions. However, when there is potential for long-term commercial benefit, Google may align itself with government interests, as seen in its collaboration with the U.S. government on defense projects.

Contributions to the literature

This PhD thesis argues that the ways in which Google builds on its digital dominance to navigate and expand its position in security can be best understood through three concepts. First, there is platformization, which is "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" (Helmond, 2015, p. 5). Second, there is infrastructural expansion, which in the case of Google refers to the process of entangling its platforms and services deeper and wider with digital society to the extent that it provides the foundation for many online services and can set de facto standards for others to follow (building on Helmond et al., 2019). Third, I deploy the concept of (in)visibility politics, with which I refer to how (in)visibility, despite being inherently relational, can be used strategically to pursue certain goals (building on Brighenti, 2007). In the following, I explain how a focus on these concepts allowed me to contribute to the study of Big Tech, algorithmic security, and commercial security actors.

Platformization

Together, the chapters offer novel empirical insights into how Google approaches security through its platforms and how its platform logic becomes entangled with (in)security. The chapters have also shown how Google's platforms enable national security actors such as the US military to develop new security practices and how Google leverages its most dominant platforms such as the browser Google Chrome to shape cybersecurity standards. Building on these empirical insights, the first argument of the PhD thesis draws attention to how Google builds on its digital dominance to expand

and navigate its position in the security domain through platformization. The PhD thesis shows how Google has been developing a broad range of new platform extensions that are aimed at keeping its users safe. Doing so locks more people into its ecosystem and pushes the platformization of security. Building on Anne Helmond's conceptualization of platformization, I argue that this reinforces Google's ecosystem overall: the platformization of any practice leads to a centralization of data and a decentralization of platform features (Helmond, 2015; Nieborg & Helmond, 2019). This dual logic strengthens Google's large-scale data analysis practices and increases how much of our lives is subject to surveillance. By approaching security responsibilities (whether these are given to Google by state actors of adopted voluntarily) through the logic of the platform, Google puts itself in the position to define a broad selection of security threats – threats that fit the (AI powered) platform solutions that Google can offer. I contribute to new media studies by arguing that spreading the platform logic feeds the broader development of platformization even if it means that data does not find itself back to Google. The platform logic leads actors such as the US military to reimagine and reshape their practices to fit the platform model, which includes the centralization of its data sources and the decentralization of machine learning applications to the battlefield. As this thesis has shown, the platformization of military practices informs how the US military relates to Big Tech and start-up companies, how they approach algorithmic security and, in the end, how war is being fought. With the platformization of security, security practices can become (even) more invisible. This is partly because platforms run on AI, which is inherently invisible, but also because these platforms are owned by Big Tech like Google of which a significant number of practices are opaque to the broader public.

By bringing in the notion of platformization, I broaden the conceptual toolkit of critical security studies. I have illustrated the importance of looking at platformization when trying to understand the actions and politics of Google and other Big Tech. Additionally, I argue that engaging with notions and practices of platformization helps students of critical security studies to explore the proliferation of algorithmic security and warfare. Platformization informs and reinforces certain ways of doing and thinking about security, and foregrounds the use of AI. As critical security studies researchers with a focus on algorithmic security have already raised concerns about, the use of AI de-politicizes security issues whilst having significant political consequences (Amoore & Raley, 2017; Bellanova et al., 2021; Bode et al., 2024; Hoijtink,

2022). This is because, despite increasing concerns about the sweeping possibilities of so-called "general AI" (Gebru & Torres, 2024), AI is still treated as a powerful technical solution that makes the practices of security actors more objective. This way of doing security has problematic implications for how security is achieved, and insecurity is defined. I contribute to research on algorithmic security by foregrounding a focus on the workings and impact of platformization. Without platforms, AI is difficult to make actionable. It needs the infrastructure of the platform to be developed and put into practice. The conceptual lens of platformization thus helps us understand the conditions of possibility of algorithmic security, as well as unpack specific implications that the turn to AI holds for security practices.

Infrastructural expansion

The chapters have also shown how Google is expanding into new sectors through its appropriation of security. Google shares its AI and cybersecurity expertise and offers its platforms for others to use for their own security objectives. Google is also pro-actively shaping internet governance by taking part in cybersecurity standardization. Based on these insights, the second argument of this thesis states that Google navigates and expands its position in the security domain through the infrastructural positions of the platforms that give Google its digital dominance. This development goes in both directions. Google shapes security understandings and standards to fit its commercial objectives through infrastructural expansion. At the same time, Google is becoming more infrastructural because it can further diversify its activities through its security work (Plantin & Punathambekar, 2019; van Dijck, 2021). As such, both Google's expertise and infrastructural platforms are increasingly laying the foundations for others to build on. I argue that this puts Google on the path to strengthen its position in society as seemingly inevitable and becoming infrastructural to online and algorithmic security.

My argument about the infrastructural expansion of Google into the domain of security brings insights from internet governance studies which examines the politics of internet standardization extensively (DeNardis, 2014; DeNardis et al., 2020; Musiani, 2015, 2015, 2020) to new media studies' exploration of the infrastructuralization of platforms (Helmond et al., 2019; Plantin & Punathambekar, 2019). New media studies literature locates Big Tech's infrastructural power in the vertical integration of their ecosystems, their ability to reuse platforms to expand into other domains, and how they repackage complex AI systems into relatively simple frameworks that others

can use (see Luitse, 2024). In line with this literature, I posit that Google expands infrastructurally by entangling its platforms with security and becoming the foundation for others to use to achieve their security objectives. More specifically, by examining how Google expands the digital dominance of its machine learning platform TensorFlow, I stress the role of open-source platforms in the infrastructuralization of Big Tech. Doing so brings into view how Google's infrastructuralization builds on the free labor provided by the open-source community that adds to TensorFlow's code base and reinforces the infrastructural status of the platform (see also Fukami & Shimizu, 2021; Widder et al., 2023). Additionally, I argue that Google's involvement in internet standardization forums enables it to expand infrastructurally (see also DeNardis & Hackl, 2015; ten Oever, 2021). Here, I understand the relation between standardization and infrastructuralization as a continuous process; the infrastructural position of Google Chrome allows it to set standards that in turn reinforce its infrastructure position.

Google navigates critique about its security position by presenting its infrastructural expansion as purely technical. But as critical security studies literature has extensively argued: there is no such thing as neutral technology (for an overview see Hoijtink & Leese, 2019). Conceptual attention to the productive and political nature of infrastructure thus builds on a growing body of literature that sits at the intersection of critical security studies and Science and Technology Studies (STS) that has drawn attention to the political nature and relevance of infrastructures (Aradau, 2010; Bellanova & de Goede, 2022b; de Goede, 2020; de Goede & Westermeier, 2022). This PhD thesis contributes to this literature by drawing attention to digital infrastructures, open-source platforms, and the standardization forums that allow digital infrastructures to function. Furthermore, I contribute to International Relations' (IR) institutional perspective on standardization (for an overview see Zúñiga et al., 2024) by exploring the relation between infrastructure and standardization. My research has illustrated how such a focus can shed light on the consequences that Big Tech infrastructure holds for the digital sovereignty of states. As governments from countries like the United States and The Netherlands have become more dependent on certain Google infrastructure and expertise for their security practices, this is an important conceptual focus for critical security studies and IR to consider.

Lastly, I contribute methodologically by demonstrating how unpacking technology down to the foundational level of protocols can yield important

theoretical and empirical insights (see also Campbell-Verduyn & Hütten, 2023). I call this approach "decoding the technobabble". While an increasing amount of STS inspired critical security studies engage with complex technology, I argue that is important to dive even deeper as a significant part of the politics of Big Tech takes place on this level. This thesis has shown that you do not necessarily need access to the specific technology, which is often proprietary (building on Aradau & Blanke, 2017). Often these technologies are developed in accordance with general principles that can be unpacked and understood. When it comes to Google's technology, this thesis has demonstrated that such a detailed technical exploration enabled new insights and raised new questions.

(In)visibility politics

Finally, the chapters show that Google is pro-actively spreading its ideas on how technology should be developed and for which security purposes by creating hypervisibility around its expertise. But the chapters also shed light on how Google is putting a stamp on (in)security through many unassuming projects and services, obfuscated collaborations with the US government, and through quite transparent but publicly largely unknown standardization negotiations. These empirical insights inform the third argument of this PhD thesis which is that Google navigates its position in the security domain by deploying (in)visibility politics.

Building on and contributing to literatures in critical security studies that foreground (in)visibility as an important knowledge practice (Brighenti, 2007, 2010a; Tazzioli, 2020; Uldam, 2016; Van Veeren, 2018), I was able to capture *how* Google aims to control the narrative about itself through hypervisibility and invisibility and all that lies in between. It is a key characteristic of how Google expands and especially navigates its position, how it marries seemingly opposing goals together, how it boosts its perceived leadership in AI, and how it keeps regulation at bay through the obfuscation of its overall ecosystem. Google aims to steer public attention away from its political involvements and towards seemingly neutral technical solutions, in particular AI, using hypervisibility. As we know from critical perspectives on transparency, such hypervisibility does not necessarily lead to meaning full understanding. Rather, it often it obfuscates important details in a sea of information (Ananny & Crawford, 2018; Stohl et al., 2016). Google's security involvements are thus fragmented, obfuscated, or simply unknown. Whether this is intentional - as argued by Maha Rafi Atal (2021) - or not, it becomes

challenging to create an overview of Google's security involvements. These (in)visibility politics complicate efforts to examine and regulate Google. But I argue that understanding these (in)visibility politics as a defining feature of Google's involvement with security can help us analyze the actions it takes in this domain. This argument contributes to new media studies literature, which often stresses the invisibility of Big Tech practices but draws less attention to how partial visibility and even hypervisibility is supportive of Big Tech power.

A more complex, relational understanding of how (in)visibility relates to power enables us to make sense of the seemingly contradicting hypervisibility and invisibility that surrounds the practices of Google. It has also shown that Google is not as all powerful as it is sometimes portrayed. Google's senior management deploys these politics to navigate critique and pushback from governments and employees. Google is susceptible to the public eye because its stakeholders need Google to have a profitable reputation. Google's senior management must therefore relate to these critiques and that influences their choices. That said, this thesis has illustrated that Google is in a position that allows it to shape security into what fits well with its objectives. In many ways Google impacts what future (AI-driven) security technology will look like and positions itself in a way that its ecosystem is and remains the most convenient option. This power, I argue, comes from the many and varied ways in which Google is involved in security through platformization and expanding infrastructurally. Google is becoming a powerful player in security, despite starting off ambiguously when it was tasked with content moderation responsibilities by the EU.

Implications for regulation and future research

At the start of this chapter, I argued that in the time of writing this PhD thesis, Big Tech's involvement in security has only become more prominent. Where Google first seemed to be ambiguous, or at least hesitant to take on responsibilities that put limits on its commercial opportunities, through platformization, infrastructural expansion and (in)visibility politics Google is now pro-actively trying to shape security practices. Before I raise the questions that require attention in future research, I draw out the wider implications of my research for Big Tech regulation.

Authors concerned with the power position of Big Tech have suggested various ways of regulating Big Tech (Cristofari, 2023; Gorwa, 2019; Hendrikse et al., 2022; Monsees et al., 2023; Rieder & Hofmann, 2020; van Dijck, 2020; van Dijck et al., 2019). Hendrikse et al. make various suggestions to counter the "Big Technification of everything" (2022). From countering the logics of surveillance capitalism and stopping the seemingly endless flow of data that is shared with Google and other Big Tech through platformization, to moving to open-source solutions and making the infrastructural core of Big Tech public. Others have pointed out that it might be ideal to govern platforms with a variety of stakeholders but warn that this might not be enough or realistic given the neoliberal politics that are intensified through Big Tech platforms (Thomas Poell in Cristofari, 2023, p. 29). Connecting these suggestions is the argument that Big Tech gain power as a collective as their data-driven practices are connected by a common logic and thus support each other (Dijck et al., 2019). While this thesis has argued that it is important to unpack Big Tech as a category, they do at times join forces, especially when faced with regulation. We can see this reflected in their initiative to develop joint cybersecurity standards for AI, or as shown in chapter 5 how Google and Apple push in tandem for new requirements in the Certificate Authority Browser Forum. That means that to a certain extent my research on Google holds lessons for the regulation of Big Tech more broadly.

As this thesis has illustrated throughout, the (in)visibility politics of Google complicate attempts of getting a full picture of Google's security involvements and its specific impact on the fields and topics it engages in. This is exacerbated by the fact that as Google expands into new markets (such as the defense sector), Google is diversifying even further. Its security involvements thus strengthen Google's position and maintain its fragmented reputation (see Atal, 2021). To be able to regulate Google, I argue it is essential to understand Google as a complex ecosystem of platforms that gains power by cross-subsidizing but in the end is still one company. Or to use the metaphor suggested by Anne Helmond (as cited in Cristofari, 2023, p. 110) Google is one octopus with many arms with even more suckers that lock-in markets as well as users. The lack of transparency of Google's security involvements throughout its ecosystem complicates attempts of regulation because it limits our ability to understand "how it works as a system" (Ananny & Crawford, 2018, p. 983). Some have therefore considered whether we should focus

regulation on the impact of Big Tech's output instead of achieving meaningful transparency (Balázs Bodó and Gianmarco Cristofari in Cristofari, 2023, p. 52). However, it is not just when Google makes so-called mistakes that its security involvements are potentially problematic and worthy of attention. This thesis has shown that understanding *how* Google expands and navigates its position in the security domain matters. It enabled this thesis to shed light on specific ways in which security is made to fit Google's commercial objectives, and how these are marked by the turn to AI. In the final three subsections, I explain how these insights lead to three avenues for future research: Google's epistemic politics, knowledge production within Google, and Big Tech climate politics.

Epistemic politics

This PhD thesis showed how Google makes use of the open-source community that uses its TensorFlow platform to further develop AI, how it builds on the infrastructural position of its browser Chrome to steer cybersecurity protocols, how Google appropriates security through its many dominant platforms and projects, and how it attempts to discredit critical AI voices from within. All these findings can be seen as ways in which Google develops epistemic authority in AI. Epistemic authority "is akin to the notion of source credibility (encompassing a combination of perceived expertise and trustworthiness)" (Kruglanski et al., 2009, p. 175). This "liquid" form of authority (Bode & Huelss, 2023) is socially constructed and therefore "always in flux, more or less embattled, and in need of constant reproduction"(Danielsson, 2020, p. 117; see also Riaz et al., 2016) In chapter 5, I also drew attention to the fact that Google's expertise in AI rarely gets questioned. When its involvement in Project Maven was criticized, the public debate revolved mostly around how Google capitalizes on this expertise. If we pair these insights with reports about how Google invests in AI research (van der Vlist et al., 2024; Williams, 2019) and how Big Tech-funded AI researchers end up in for instance the EU's High-level Expert Group on Artificial Intelligence (Bode & Huelss, 2023), important questions arise regarding Google's epistemic politics, which I loosely understand as the strategic use and expansion of epistemic authority.

In 2020, José van Dijck warned us that:

> If public interests become virtually dependent on private infrastructures while state or civil representatives have little sway over the conditions of its architecture, affordances, and

> functionalities, the information ecosystem gradually assumes a monocratic status. (Van Dijck, 2020, p. 12)

What are then the implications now that Google's expertise and infrastructure have become things that researchers, companies, and governments increasingly depend on? Which AI imaginaries become translated into (security) policies and applications? These questions are important to address, especially in light of the EU's wish to become more technologically independent (Csernatoni, 2022; Monsees & Lambach, 2022; Mügge, 2024), which includes both the ambition to have "sovereignty over the digital" and "sovereignty through the digital" (Bellanova et al., 2022, p. 338). Researchers have illustrated that the EU's dependence on Big Tech infrastructure and expertise has impact on its cybersecurity policy (Farrand & Carrapico, 2022) and military AI initiatives (Bode & Huelss, 2023). In line with Ingvild Bode and Hendrik Huells, who have examined "new forms of hybrid and liquid state-private epistemic authority, in which the institutional power of governmental actors, such as the EU, relies on private authority and expertise" (2023, p. 1236; building on Krisch, 2017), I propose a focus on Google's/Big Tech's epistemic politics within and beyond the European Union as an avenue for future research. As I explain in the following subsection, this suggestion goes hand in hand with unpacking how expertise is created within Google.

Knowledge production within Google

The PhD thesis has shown that a group of employees are critical of how Google's senior management steers the company's AI development. They question whose perspectives are included in the development of AI, for which purposes AI applications are made, and which harms these applications could produce. These employees protest, leak information to the press, or even resign. Others are fired. For example, Google's leading AI ethicists Timnit Gebru and Margaret Mitchell, both known for their work on algorithmic bias and how they promote diversity in the field of AI (Buolamwini & Gebru, 2018), were fired by Google in late 2020 and 2021 (Schiffer, 2020; Tarantola, 2021; Vincent, 2021). Gebru was fired for raising awareness about the potential negative effects that large-scale AI systems hold for minority groups in a research paper. Google's senior management maintained that she quit and that the paper in question was halted from publication as it did not live up to Google's publishing standards (Dean, 2020). Shortly after, Mitchell was fired after publicly speaking out about how Gebru's firing instead reflected Google's alienation of Black women (Fried, 2021). While much more can be

said about this example, relevant for this conclusion is how together with the findings of this PhD thesis it draws much needed attention to the internal politics and practices of Google.

Drawing inspiration from a rich literature at the intersection of science and technology studies (STS) and critical security studies that illustrates the relevance of mundane daily security practices in shaping (in)security understandings (Amicelle & Jacobsen, 2016; de Goede, 2018; Huysmans, 2011; Salter & Mutlu, 2013a), I suggest a focus on how (AI) knowledge is produced and steered within Google as an avenue for future research. How do employees build machine learning models? How do they navigate and give meaning to questions of responsibility and accountability? How does their work build on and contribute to knowledge produced by other Google platforms and subsidiaries? How do employees relate to the AI imaginaries of their senior management and which imaginaries are then translated into the algorithms/platforms they build? How do they navigate moments of controversy and friction within the company about how AI? Such questions would enable us to unpack Google even further and trace how security/AI imaginaries travel through the company and are translated into concrete applications. Furthermore, such research would help us contextualize why and how critique develops internally and leads to public protest. Lastly, a focus on the practices at Google and other Big Tech would facilitate a dialogue between STS informed critical security studies and recent new media studies literature on platform labor (Kelkar, 2018; Meisner et al., 2024; Shestakofsky & Kelkar, 2020; van Doorn, 2017).

Accessing Google for participant observation can prove to be difficult. Furthermore, Rikke Frank Jørgensen has shown that during his research in 2015-2017 most of his interviewees at Google and Facebook held on to the company narrative (2020). However, the amount of protests by both low-paid tech workers and more senior staff such as Timnit Gebru and Margaret Mitchell has been on the rise (Tiku, 2018). While these protests do not reflect daily practices, it is not unlikely that the (former) employees present at these protests would be more willing to divert from the company line.

Big Tech climate politics

Finally, throughout this PhD thesis, it has become clear that Google turns to AI as its main “solution” to the security threats it identifies. Google’s machine learning platform TensorFlow provided the backbone to Project Maven,

which still sits at the center of the United States approach to algorithmic war. Simultaneously, with the rise of AI large language models such as Microsoft and OpenAI's ChatGPT and Google's Gemini, so-called "generative" AI is becoming more publicly accessible (Ossip, 2024). In response to the "AI boom", climate scientists have started to examine the environmental impact of AI, which requires resource-intensive computing power and large-scale data centers that use a lot of electricity as well as water for cooling. Some weigh the potential benefits of using AI to find climate solutions against the impact it has on the climate (Cowls et al., 2023). Others say that this equation is more complex, pointing to how:

> increasing the environmental and financial costs of these models doubly punishes marginalized communities that are least likely to benefit from the progress achieved by large LMs [language models] and most likely to be harmed by negative environmental consequences of its resource consumption. (Bender et al., 2021, p. 610).

In light of this research on AI's climate impact, the final avenue for research that I like to put forward is a focus on Big Tech's climate politics.

Exploring how Big Tech are involved in climate politics enables us to expand the infrastructural perspective that I adopted in this PhD thesis. Such an infrastructural perspective brings into focus several recent infrastrucural expansions of Google and other Big Tech. For example, a focus on climate politics would enable us to examine the political stakes of Google's recent investment in nuclear power to run its AI infrastructure (Terrell, 2024) and how Big Tech become energy suppliers by using the waste heat of their data centers for central heating (Velkova, 2016). It would also draw attention to Big Tech's power intensive data centers and the impact those have on the communities they are placed in. With this focus comes the opportunity to explore how communities resist the building of these data centers out of climate concerns. A valuable example of this is the recent work by Tonia Sutherland and Gailyn Bopp, who have explored how the development of subsea data centers impact on local indigenous communities living on the Pacific Islands, in particular Hawai'i (2023). Doing so allowed them to draw attention to how:

> technology based corporate interests in the Pacific islands too often fail to consider the long-standing effects of colonialism and the reluctance of local ocean stewards to welcome new technology projects into local—and often sovereign—waters that provide spiritual and physical nourishment and return, as well as direct ties to the past and ancestral worlds. (Sutherland & Bopp, 2023, p. 358)

Additionally, focusing on Big Tech's climate politics makes room for exploring how across the world local communities resist Big Tech plans, such as in Zeewolde in The Netherlands (Hamilton, 2022), Northern Virginia (Woollacott, 2024) and Mesa Arizona in the United States (Solon, 2021) and Canelones in Uruguay (Butler, 2023). Such a focus can shed light on how the asymmetrical power relation between Big Tech and citizens can shift. For example, Anna Zenz and Julia Powles traced how a community in Canberra Australia successfully stopped the rollout of delivery drones by resisting the technological inevitability narrative of Google and the local government (Zenz & Powles, 2024).

Focusing on Google's – and Big Tech's – epistemic politics, daily knowledge practices, and climate politics gives us concrete ways to shed more light on their political impact on security and other sectors. While calls for breaking up Google are made in the US (Simpson, 2024) and billion dollar fines are handed out in Europe (Edwards & Leggett, 2024; Gerken, 2024), Big Tech's entanglement with digital societies is both wide and deep while their accountability remains low. With the security domain becoming a part of their business, Big Tech only seem to gain in power.