Assembling Publics: Microsoft, Cybersecurity, and Public-Private Relations

Liebetrau, Tobias; Monsees, Linda

cogitatio

Politics and Governance (ISSN: 2183–2463)
2023, Volume 11, Issue 3, Pages 157–167
https://doi.org/10.17645/pag.v11i3.6771

Article

Assembling Publics: Microsoft, Cybersecurity, and Public-Private Relations

Tobias Liebetrau [1,*] and Linda Monsees [2]

[1] Centre for Military Studies, University of Copenhagen, Denmark
[2] Center for Governance of Emerging Technologies, Institute of International Relations Prague, Czech Republic

* Corresponding author (tl@ifs.ku.dk)

Submitted: 31 January 2023 | Accepted: 3 May 2023 | Published: 31 August 2023

Abstract
In this article, we advance the literature on publics in international politics by exploring the nexus between publicness and big tech companies. This nexus finds a significant expression in the increasing impact of big tech companies to mediate disputes over societal problems, deliver social goods and rearticulate public-private relationships. We develop an analytical framework by combining recent scholarship on assemblage theory and publics, allowing us to understand publicness as enacted in practices which revolve around issues and rearticulate relations of authority and legitimacy. To demonstrate the value of the framework, we show how Microsoft is involved in assembling publicness around cybersecurity. Microsoft does so by problematising and countering state-led cybersecurity activities, questioning the state as a protector of its citizens and proposing governance measures to establish the tech sector as authoritative, and legitimate "first responders." With this rearticulating of public-private relations, we see the emergence of a political subject for whom security is not solely the right of a citizen secured by the state but also a customer service provided as a service agreement. The study hence offers important insights into the connection between publicness and cybersecurity, state and big tech relations, and the formation of authority and legitimacy in international politics.

Keywords
assemblage; big tech; citizen-user; cybersecurity; global governance; international politics; Microsoft; public

Issue
This article is part of the issue "Publics in Global Politics" edited by Janne Mende (Max Planck Institute for Comparative Public Law and International Law) and Thomas Müller (Bielefeld University).

1. Introduction

In this article, we advance the literature on publics in international politics by exploring how big tech companies assemble distinct forms of publicness, arguing that it marks important transformations in contemporary global governance. To do so, we develop an analytical framework uniting recent scholarship on assemblage theory and public theory. In line with the goal of the thematic issue (Mende & Müller, 2023), we do not ask if a global public exists but investigate the various manifestations of publics. Mende and Müller (2023, p. 92) identify four manifestations of global publics, and we contribute primarily to the understanding of the second manifestation: Publics are groups of actors that form communicative spaces....What makes the group of actors hang together is that its members react and refer to each other's arguments about the issue. In this article, we specifically focus on how private companies can create these issues and how thereby, a public is assembled. More specifically, we examine how Microsoft assembles publicness around cybersecurity and thereby rearticulates relations of authority and legitimacy between big tech companies, citizens, and the state.

Research on the international political role of private companies has produced valuable knowledge about present forms of global governance (Hofferberth, 2019; Mende, 2023), security practices (Berling & Bueger, 2015; Leander, 2005), and the corporate power of big tech (Beaumier et al., 2020; Monsees et al., 2023; Srivastava, 2021). This article draws on but also extends insights from this literature to examine the nexus between publics and private companies in international politics. This nexus, we argue, finds a significant expression in the increasing impact of big tech companies, elsewhere captured in concepts such as "surveillance capitalism" (Zuboff, 2019), "internet-industry complex" (Flyverbom et al., 2019), or "data capitalism" (West, 2019). However, what is at stake here is not just a simple transfer of public functions from the state to the private sector. What we tease out is the ambivalence of the rearticulation of public and private. While private companies help in making issues relevant to public problems (such as privacy and cybersecurity), they also claim capability, legitimacy, and authority by providing social goods. In the case of cybersecurity, we observe a tension in which citizens become users in need of the protection provided by big tech companies. This is an expression of a broader trend in which relations of authority and legitimacy between both states and companies as well as companies and individuals are being rearticulated through extensive commercialization and corporate regulation of cybersecurity (Beaumeir, 2020; Christensen & Petersen, 2017; Liebetrau & Monsees, 2022).

In order to demonstrate how this plays out and captures the assembling of publicness, we develop an analytical framework combining works on assemblage theory and publics in global governance (Best & Gheciu, 2014; Bueger, 2018; Walters & D'Aoust, 2015), critical security studies (Abrahamsen & Williams, 2009; Monsees, 2019; Stevens, 2016), and sociology (Marres, 2012). Building on these diverse approaches, we treat assembling publicness as a research strategy for empirically grounded analysis of the process of composition (Buchanan, 2020, p. 458) rather than a unified theory or approach (Bueger & Liebetrau, 2023, p. 240), enabling us to examine publicness as enacted in practices, which revolve around issues and rearticulating relations of authority and legitimacy.

While existing literature has shown how developments in communication technology, the internet, and social media demand a rethink of the public sphere (Baum & Potter, 2019; Dahlgren, 2005; Papacharissi, 2002; Pond & Lewis, 2019), we focus on big tech companies given their unique role in mediating disputes over public problems, delivering societal goods, and rearticulating public-private relationships (Culpepper & Thelen, 2020; Oyedemi, 2020). Concretely, we explore Microsoft's involvement in cybersecurity. Cybersecurity is an issue that has emerged with the development of information communication technologies in everyday life (Dunn Cavelty & Wenger, 2020). Appearing as a new kind of public good over which states and commercial actors are negotiating the boundaries for their respective roles, cybersecurity is a paradigmatic case for understanding how private companies can assemble publics.

In the remainder of this article, we first develop the analytical framework of assembling publicness. In the main part of the research, we show how Microsoft is involved in assembling publicness around the issue of cybersecurity. This section illustrates how the assembling of publics achieves political force by rearticulating public-private relations and the formation of authority and legitimacy in cybersecurity governance. In the conclusion, we suggest three ways as for further research to unpack the assembling of publicness in international politics on the one hand, and problematize big tech practices and their political implications on the other.

2. Assembling Publicness in International Politics

Developing an analytical approach which draws on assemblage theory, critical security studies, sociology, and sciences and technology studies, this section lays the foundation for the following analysis, which examines Microsoft's efforts to assemble publicness around cybersecurity. The section consists of two parts. The first situates the article in relation to the existing literature on IR and the thematic issue. The second outlines the assemblage approach and how it allows us to capture the formation of publics through three central features, namely, practices, issues, and power relations.

2.1. Manifestations of Publicness

This article speaks to two major changes to international politics observed in IR in the past decades. The first concerns the shift from government to governance invoked by the global governance literature (Rosenau, 1995; Rosenau & Czempiel, 1992). As stressed by Mende and Müller (2023, p. 91), global governance is "characterised by a complex and constantly evolving constellation of actors—among them states, international organisations, non-governmental organisations and firms—that perform governance tasks and assume governance authority" (Avant et al., 2010; Stone, 2020; Zürn, 2018, as cited in Mende & Müller, 2023). Zooming in on privatization and commercialization of security, scholars have shown how public and private are not two pre-existing realms but emergent spheres in which relations of legitimacy, authority, and responsibility are distributed, negotiated, and contested (Abrahamsen & Williams, 2009; Avant, 2005; Krahmann, 2008; Leander, 2005; Leander & van Munster, 2007). However, as Walters and D'Aoust (2015, p. 47) observe, publics "remain undertheorised and underproblematised in critical security studies." We thus build on previous work that highlighted how publics manifest through practices but expand on it with a distinct focus on big tech companies and security governance, rather than centering on privatization, commercialization, or neoliberalism as it is usually the case in the literature (Walters & D'Aoust, 2015, p. 48).

Alongside this development, scholars have explored the existence, possibility, and importance of global publics. They have analysed how the proliferation of transnational issues (e.g., trade, finance, and environment), actors (e.g., IOs and NGOs), and governance arrangements demands us to pay attention to publicness at a global and transnational level (Best & Gheciu, 2014; Brem-Wilson, 2017; Eckersley, 2007; Mitzen, 2005; Norman, 2019; Ruggie, 2004; Volkmer, 2014). According to the introduction to the thematic issue, this literature has been preoccupied with analysing and debating whether a global public exists or not. Here, we rather follow the editors' suggestion to embrace and "investigate various manifestations of publics that exist in, and co-evolve with, global politics" (Mende & Müller, 2023, p. 92). Taking that as our starting point, we explore how big tech companies assemble forms of publicness, arguing that it marks important transformations in contemporary global governance.

In doing so, we understand publics as plural, situated, and dynamic. Their existence and boundaries are due to constant (trans)formation, negotiation, and contestation (Dean, 1999; Dewey, 1999; Fraser, 1990; Marres, 2007). We hence need an analytical perspective that can grasp emergent and multiple empirical manifestations of publics as well as their effects on claims to legitimacy and authority. To capture this formation, we construct an analytical strategy that introduces the manifestation of publics through three central features and presuppositions: practices, issues, and power relations.

2.2. Assembling Publicness as an Analytical Strategy

Our research strategy allows us to examine how publics "are assembled and actor constellations produced, without relying on an a priori definition on the identity, position or interest of actors" (Bueger & Liebetrau, 2023, p. 240), while emphasising that the assembling of publics is provisional, processual, and dynamic (Stevens, 2016, pp. 32–36). This research strategy thereby directs the study away from answering essentialist questions, such as what a global or international public is or where it is located, towards an empirically grounded analysis of how publicness emerges, stabilises, and decays. The framework does not exclude the possibility that publics reach a form in which they are organised by a dominating logic, are institutionalised, or are hierarchically structured. However, rather than presume a priori how publics are ordered and structured, it leaves this question open to empirical analysis.

Our research strategy thus assumes that publicness is specific to certain times. This means that publics are distinct from the logics, criteria, or definitions that are assumed to be stable across time and space. This could mean, for example, assuming that there a "public" or "private" realm exists as a fixed sphere unaltered by its agents' behaviour. Following on from this, our approach is reflexive. The analyst does not have a God's eye view from which to construct objective and ahistorical definitions and concepts (Haraway, 1988). One result of thinking in these terms is that "every time we make reality claims in science we are helping to make some social reality more or less real" (Law & Urry, 2004, p. 396). Consequently, the analytical framework contains a double move. It aims to identify and describe situated publicness in context and to problematize it further for critical purposes (Aradau & Huysmans, 2014).

First, both assemblage theory and sociological concepts of publics emphasize the importance of practice (Acuto & Curtis, 2014; Bueger, 2018; Marres & Lezaun, 2011; Monsees, 2019). Shifting the analytical perspective towards assembling publicness through practice is a crucial step. IR scholars have demonstrated how the enactment of publics plays out in practice. For instance, Walters and D'Aoust (2015) demonstrate how publics are enacted through paintings and public demonstrations. Each public addresses itself in a particular way towards the state; it can either reify or challenge the previous (Walters & D'Aoust, 2015, p. 59). Best and Gheciu (2014) focus on the importance of practice and the performative aspects of public-making. We follow their understanding of public-making practices as practices:

> That seek to claim particular problems, actors, or processes *as* public—or of common concern—and in doing so, that effectively work to constitute those issues as public. In other words, public-making practices are performative: they seek to create the things that they describe. (Best & Gheciu, 2014, p. 32)

Linking this to assemblage thinking, we understand publicness as based on relations and practice "in the sense that it depends on assembling practices involving actors, objects, rules, or principles in a particular territorial space and time, which gives them meaning in relation to one another" (Kolmasova, 2022, pp. 1329–1230). Drawing on Bueger (2018, p. 619), we argue that the assembling of publicness requires "consistent practical work" and must "always remain unstable and open to tensions and contestation." This prompts research to engage empirically with public assembling practices.

Second, a critical function of the assemblage framework is that it brings to the fore "a specific historical, political, and economic conjuncture in which an issue becomes a problem" (Ong & Collier, 2005, p. 14). An assemblage framework emphasizes the ambivalence, contestation, and multiplicity of public-making practices (Bueger & Liebetrau, 2023, p. 238). This idea fits hand in glove with sociological conceptions of multiple publics emerging in relation to problems and issues (Callon et al., 2009; Marres, 2007). For example, Marres (2007, 2012) directs our attention to how publics emerge as a result of issue formation. The public is not a pre-constituted sphere in which issues are deliberated. Rather, issues are perceived as needing action, and a public emerges as a result. This also means that publics are not necessarily linked to state politics but can be found everywhere and assembled around a multiplicity of actor or things (Honig, 2017; Marres, 2012; Marres & Lezaun, 2011). We argue that when we pay attention to public-making practices, we need to seriously consider how certain issues become public issues without reading them back into a state-centred framework. The political power of how big tech assembles publics only becomes visible when we look at the state and big tech symmetrically. Consequently, the making of publics is far from a neutral undertaking but a highly political practice. Combining assemblage thinking and sociological conceptions of publics sensitises us to the ambiguity, contestation, and disagreement over the issues at stake, and, following on from that, rearticulations of public-private relations. This allows us to identify how the notion of a citizen-user becomes core to Microsoft's assembling of publicness around cybersecurity.

Lastly, assemblage thinking addresses questions relating to power, authority, and legitimacy (Abrahamsen & Williams, 2009, p. 3, 14). Primarily, it allows us to see how assemblages generate the capacity to act in particular ways, rendering some actors more powerful than others (Bueger & Liebetrau, 2023, p. 243). When studying relations and practices of assembling publicness, we study how capability, expertise, and knowledge might become authoritative and legitimate. Zooming in on the historical concept of the public, it refers to the emergence of a public in which an opinion is formed. This public was considered both the opposite of the private sphere and the opposition to the state's power (Habermas, 1962, p. 55). In a democracy, the role of the public is to legitimize the actions of the state (Habermas, 1962, p. 82, 97). From this perspective, legitimate policies are those which are formulated in the name of the public and mirror the public's interest (Eckersley, 2007, p. 334). Legitimacy then relies on recognition by subjects (citizens) (Gronau & Schmidtke, 2016). In line with the overall analytical perspective, legitimacy is thus not a legal or formal concept but a relational and performative concept (Kratochwil, 2006). If publicness does not only centre on the state, formations and relations of legitimacy are multiple. As we show below, this means that claims about legitimacy can hinge on relations between private companies and citizens. Claiming to act in the public's interests or to fulfil the public's needs endows one with legitimacy and authority to act. Assemblage theory allows us to scrutinize how publicness is assembled across actors and thus enacts relations of authority and legitimacy.

In sum, we see that who appears as a public actor or what issue is considered a public problem is the outcome of political processes. If we consider the public and the private as a result of political processes, the consequences of assigning something or someone as being public come into view. Claiming that an issue is a public problem or that someone acts in the public interest means simultaneously making claims about certain actors' authority and legitimacy (Dean, 1999). Deploying the assemblage framework hence enables us to examine processes of political ordering that are enmeshed with reconfiguring publicness. As we illustrate below, Microsoft assembles in assembling publicness around cybersecurity by challenging state behaviour in cyberspace and claiming authority and legitimacy for itself (and the tech sector) as a cybersecurity provider. These ordering processes unfold political power by influencing relations of legitimacy and authority.

3. Assembling Publicness: Microsoft, Cybersecurity, and Public-Private Relations

The following section presents an analysis of Microsoft's cybersecurity practices that demonstrates how the assemblage framework helps to think about publics in international politics. Microsoft has more than one billion customers in more than 140 markets. The company owns, operates, and leases data centres in more than 20 countries (Smith & Browne, 2019). Microsoft has promoted significant cybersecurity initiatives involving states, companies, and international organisations, such as the Digital Geneva Convention (Microsoft, 2017), the Cybersecurity Tech Accord (Smith, 2018a), and the Paris Call for Trust and Security in Cyberspace (81 states and more than 700 companies are supporting the call. As you can see in the following link: https://pariscall.international/en). Exploring the changing relationship between states, big tech, and citizens, recent scholarship has demonstrated how Microsoft positions itself as a dominant player in global cybersecurity governance, namely through practices of norm entrepreneurship and policy shaping (Fairbank, 2019; Gorwa & Peez, 2020; Hurel & Lobato, 2018). We add to this existing literature by examining how Microsoft also assembles publics around cybersecurity and thereby shifts notions of legitimacy and authority.

Put in methods terms, and following Flyvbjerg (2006, pp. 232–233), we consider the case of Microsoft a paradigmatic case as it highlights general characteristics and serves as an exemplar suitable for reinterpretation, contestation, and comparison by other scholars. We follow a qualitative-interpretative research design (Klotz & Prakash, 2008; Schwartz-Shea & Yanow, 2012). Examining the assembling of publicness around cybersecurity, we focus on sites of tensions and moments of controversy from the 2013 Snowden revelations to the present, analysing Microsoft's practices, accounts, and relations (Loughlan et al., 2015, pp. 38–39). In doing so, we rely on multiple empirical sources, including policy reports, white papers, speeches, blog posts, press releases, news sources covering Microsoft's actions, existing scholarship on Microsoft, as well as engagement in cybersecurity workshops, conferences, and debates featuring Microsoft practitioners. We analysed these documents collaboratively in several rounds, thereby following an iterative research strategy going back and forth between theoretical reflection and empirical analysis.

3.1. Problematising Cybersecurity: Destabilising State Authority and Legitimacy

A decade ago, Edward Snowden famously disclosed information about the extensive intelligence practices of the US National Security Agency and its partner services. The revelations surprised seasoned observers, questioned established understandings of the legitimacy of the institutions involved, and stimulated intense political controversy, confirming transformations in the relations between state security practices and democratic procedures, state and civil society, and state and corporate interests (Bauman et al., 2014, p. 122). The files revealed how intelligence services, particularly the US National Security Agency and Government Communication Headquarters (GCHQ), rely on voluntary or forced collaborations with private providers such as Microsoft, Google, Facebook, Verizon, and Vodafone. Despite their involvement in the collection of user data, the US tech industry publicly criticized the US government, called for intelligence reform, and pushed for stronger cyber security standards, rebuilding public and consumer trust (Roberts & Kiss, 2013).

Microsoft played a crucial role in this campaign. Brad Smith, then Microsoft's general counsel, compared the government surveillance to "sophisticated malware or cyber attacks" and emphasized that Microsoft "are taking steps to ensure governments use legal process rather than technological brute force to access customer data" (Arthur, 2013). Corporate Vice President Scott Charney (2013) noted that "industry creates and operates most of the infrastructure that enables cyberspace" and argued that global cyber security norm building would hence benefit from including private companies to ensure "that nation-state behaviour in cyberspace does not erode the fundamental trust and security mechanisms of the internet." The increasing awareness of mass surveillance highlights the ambiguous role of state agencies in protecting as well as targeting its citizens' private sphere (see Monsees, 2019). While Microsoft's primary focus was on creating international norms that rein in government behaviour in cyberspace, the company emphasized the need for a multistakeholder approach, portraying this as an "operational reality rather than an ideology," thereby underlining the central role of the private sector in defending cyberspace and its users (McKay et al., 2014, pp. 14–16). Similarly, McKay et al. (2014) emphasised that "military espionage and other surreptitious activity reminds us that governments often have other interests that conflict with their role as protectors." Microsoft compared the contradictory cybersecurity priorities of the government to an industry that "wants to protect the security and privacy of users, and support efforts to protect public safety and national security" (Microsoft, 2014). The company outlines a transnational public problem concerning the growing dependence on digital technology and the vulnerability of tech customers. Microsoft relates this problem to the contradictory role of governments as both protectors and perpetrators in cyberspace. This provides a first glimpse of Microsoft's central role in defining state activities in cyberspace as a global problem and assembling publicness around it. In doing so, Microsoft questions the state's historical role as the primary provider of security and puts forth a notion of a citizen-user—a subject that is in need of protection in cyberspace through state actions as well as that provided by companies. We thus observe an ambivalent dynamic in which the relation between companies and states is renegotiated and not a simple empowering of big tech at the cost of the state.

3.2. Proposing a Digital Geneva Convention: Assembling Publicness Around Cybersecurity

Still unsatisfied with government action in and discussion about cyberspace, Microsoft scaled up its efforts in 2017 by proposing a Digital Geneva Convention to strengthen global cybersecurity (Microsoft, 2017; Smith, 2017a). Microsoft reiterated its commitment to ensuring corporate protection of users from the state in cyberspace: "The world needs new international rules to protect the public from nation-state threats in cyberspace. In short, the world needs a Digital Geneva Convention" (Microsoft, 2017). In this context, Smith (2017b) clarified the changing relationship between states and companies:

> Let's face it; cyberspace is the new battlefield. The world of potential war has migrated from land to sea to air and now cyberspace....Cyberspace is owned and operated by the private sector. It is private property, whether it is submarine cables, datacenters, servers, laptops, or smartphones....it puts you in a different position, because when it comes to these attacks in cyberspace, we not only are the plane of battle, we are the world's first responders. Instead of nation-state attacks being met by responses from other nation-states, they are being met by us.

Smith (2017b) directs attention to the ways in which the cybersecurity practices of tech companies challenge the traditional security prerogative of the state. He contrasts a privately owned and operated cyberspace to conventional nation-state territory and national security responsibility. Smith thereby portrays the corporate tech sector as a global security actor in its own right, acting not just when mobilized by the state (Christensen & Liebetrau, 2019). This shows how Microsoft and the tech sector have "significant capacity to bolster or undermine government authority" and to increase "public demands for the companies to take action to protect users from governments" (Eichensehr, 2019, p. 668). This neither erodes state power nor is it automatically opposed to it, but it shows how relations of authority and legitimacy concerning cybersecurity between state and companies can become rearticulated.

According to Smith (2018b), the authority and legitimacy bestowed upon Microsoft and the tech sector stems not only from a lack of state capability but also from the fact that "nation-state hacking has evolved into attacks on civilians in times of peace." Consequently, private tech companies have "to help deter and respond to nation-state cyberattacks." They thereby increasingly "stand as competing power centers, challenging the primacy of governments." (Eichensehr, 2019, p. 668). Grounded in its supposed neutrality and expertise, Microsoft and the tech sector emerge as core actors in identifying cyber insecurity as a global problem and protecting against future security challenges. Microsoft thus not only defines what the problem is but also assembles publicness around it through its different initiatives (and the involvement of multiple global actors). As a result, the assembled public challenges the distribution of authority and legitimacy between states and private companies in relation to cybersecurity.

We see the contours of a vulnerable and de-territorialized public, or community of affected, as Dewey (1999) called it, being assembled around cyber insecurity, consisting of a user who has a right to security and is in need of protection from the state. As emphasized by Smith (2017b):

> We've pledged our support for defending every customer everywhere in the face of cyberattacks, regardless of their nationality. This weekend, whether it's in London, New York, Moscow, Delhi, Sao Paulo, or Beijing, we're putting this principle into action and working with customers around the world.

Microsoft calls upon digital citizens and endows them with a universal right to protection that is determined neither by territoriality nor nationality. Through such digital acts (Isin & Ruppert, 2017), Microsoft enacts a new political subject—a citizen-user—that co-exists in the privately owned and operated cyberspace and the territory of states. For this subject, security is not solely the right of a citizen secured by the state, but also a service stipulated in the terms of agreement between Microsoft and its customers. Microsoft thus assembles an issue public around cybersecurity. The result is, however, not only the creation of certain norms but a challenge to boundary drawing as to what counts as "private" and what as "public" authority and legitimacy. In the next subsection, we look at how the lines of public and private are redrawn in more detail.

3.3. Aiming to Sit at the Head of the Table: Rearticulating Public-Private Relations

While Microsoft's proposals for a Digital Geneva Convention received extensive attention across state entities and private companies, the initiative was also perceived as brazen and met with pushback (Gorwa & Peez, 2020, p. 265; Jeutner, 2019, p. 161). Hence, in April 2018, Microsoft initiated the Cybersecurity Tech Accord (CTA). The CTA toned down the language of the Digital Geneva Convention. It was launched by a group of 34 technology companies, including giants such as Microsoft and Facebook, and a diverse group of international telecoms, hardware manufacturers, open-source software providers, and cybersecurity threat intelligence companies. The CTA is a four-point reformulation of central features of the Digital Geneva Convention principles of responsible behaviour in cyberspace for the private sector. According to one of the four principles, the "no offense," accord signees "will not help governments launch cyberattacks against innocent citizens and enterprises, and will protect against tampering or exploitation of their products and services through every stage of technology development, design and distribution" (The Cybersecurity Tech Accord, 2017). While the "stronger defence" principle encompasses a commitment to "protect all customers globally regardless of the motivation for attacks online." (The Cybersecurity Tech Accord, 2017). As Gorwa and Peez (2020, p. 279) stress, the Tech Accord demonstrates a major departure from past norm-building efforts in the cyber realm since it is led by tech companies and not states.

Continuing these efforts, Microsoft initiated the Digital Peace Now campaign in 2018. It is a global policy effort urging world leaders and citizens to create digital world peace (O'Sullivan, 2018a). Announcing the start of the campaign, Microsoft states that "Digital Peace Now is going to be all about people—people banding together to tell their world leaders that the internet must be a peaceful, shared community" (O'Sullivan, 2018a). In line with this, the campaign promotes two general courses of action. The first one is to "demand government action" by signing the online "Digital Peace Petition" (Digital Peace Now, n.d.). The second one encourages citizens to join the campaign and consider cybersecurity concerns when voting (O'Sullivan, 2018b). Once more, we see how Microsoft calls upon digital citizens and endows them with a universal right to protection determined neither by territoriality nor by nationality, while still relying on the state by demanding changes in government action. A public is thus assembled in which Microsoft defines the problem and the object of protection. However, the demarcation of this public does not follow those of a nation-state nor traditional notions of public and private authority.

Microsoft continues to form new spaces of cybersecurity governance, in which companies and government actors contest and renegotiate their respective authority and legitimacy regarding cybersecurity and the protection of individuals. At the time of writing, this has culminated in Microsoft's (informal) co-authorship of the French government initiative of the Paris Call for Trust and Security in Cyberspace and its sponsorship of the recently founded Cyber Peace Institute (Broeders & van der Berg, 2020, p. 11). Fairbank (2019, p. 16) argues that "through the CTA and the Paris Call, Microsoft has helped bring together valuable actor groups within industry, civil society and global government that encourage the adoption of international cybersecurity norms." Gorwa and Peez (2020, p. 273) go one step further in arguing that "Microsoft has not only aimed for a seat at the table, but for the seat at the head of the table as the cyber-norms effort grows with initiatives such as the Paris Call." This underlines how Microsoft, through its continued efforts in cybersecurity governance, plays a key role in assembling publicness around cybersecurity and rearticulating governance relations of authority and legitimacy across public and private actors.

In sum, the analysis shows how Microsoft assembles publicness around the issue of cybersecurity, which contours it defines as a global problem, and claims is solvable only through the intervention of private companies on account of their neutrality, expertise, and extensive reach. The analysis highlights the ways in which relations of authority and legitimacy between both states and companies, as well as companies and individuals, are being rearticulated through extensive commercialization and corporate regulation of cybersecurity, relying on ownership of infrastructure, technical expertise, and global customer bases.

4. Conclusion

To explore the nexus between publicness and big tech companies, this article introduced an analytical framework for assembling publicness. By shifting the perspective from state-based territorial and institutional conditions of publicness to processes of public-making, the framework provided tools to defamiliarize and rethink relations between companies and states on the one hand, and companies and individuals on the other. Investigating these relations through Microsoft's assembling of publicness around cybersecurity, we saw how claims to authority and legitimacy rearticulated public-private relations. This demonstrates that paying further attention to the assembling of publicness, without automatically reading it back into strict spatial or functional frames, is of fundamental importance to our understanding of publicness in international politics, including how the practices of big tech companies question conventional politics and political ordering. In conclusion, we therefore suggest three ways forward as to how further research can unpack the assembling of publicness in international politics on the one hand and problematize big tech practices and their political implications on the other.

First, looking closer at the political and democratic implications of the analysis, we observe an ambiguous double movement: On the one hand, it shows how, through assembling publicness, new issues which cannot be sufficiently addressed by national politics, are put on the international political agenda. It opens possibilities for engagement in the processes of determining what cybersecurity is, can, and should be, as well as determining the political issues at stake and, not least, who has a legitimate stake in these issues and a right to security. On the other hand, the analysis demonstrates how assembling publicness by a private company alters subject positions and can lead to the creation of a citizen-user, where rights become services that customer need to pay for. From a democratic perspective, this is problematic since the erosion of the role of the state as the provider of security clashes with the right of the citizen to claim protection against outside threats. As critical security studies have shown, many of today's persistent security issues, such as climate change and migration, do not neatly align with the spatio-functional borders of the state and its institutional framework (Walker, 2010). Rather, they implicate a wide range of different actors, technologies, and governance measures, cutting across spatial and functional lines of demarcation. Rooted in various strands of IR research on the role of private companies in the constitution of international politics and public policy, future research could unpack this ambiguity and its political and normative consequences through the assembling of publicness.

Second, the analysis suggests there is further work to be done in examining how big tech practices rearticulate public-private relations by questioning state behaviour, providing social goods, and assembling publicness. A prime case here is the recent unprecedented support to Ukraine offered by Microsoft and other tech companies (Microsoft, 2022). It has been argued that a key reason Ukraine has not suffered a major cyber-blow is exactly because of this support. Microsoft moved Ukrainian digital data to its European cloud facilities, Google provided free licensing of its products, Palantir offered data analytics software, and Starlink satellites permitted Ukraine to keep its critical communication running. The involvement of big tech on the side of Ukraine shows that big tech companies now play a decisive role in war. This involvement could also be scrutinized in light of Microsoft's and other tech companies' activities in the past decades.

Investigating the extent to which big tech has "become supplemental sovereigns, governing individuals alongside states" (Eichensehr, 2019, p. 668), the research could also explore the role and political implications of these companies in providing other social goods such as health or mobility (Maghalaes & Couldry, 2021). This would allow us to grasp the manifold forms of authority and legitimacy that big tech companies can assume in global governance. Such studies could benefit from problematising how big tech practices of assembling publicness intersect with questions concerning the enduring legacies of state-centrism, Western bias, gender relations, and socio-economic status.

Third, the framework paves the way for an open-ended, empirically driven research agenda on assembling publicness in international politics and governance, allowing scholarship to examine the evolvement of public-private and state-company relations over time to grasp both continuity and change in the contemporary role of private companies in the constitution of publicness and relations of authority and legitimacy. Leveraging perspectives from international political economy, the history of international relations, and international political sociology dealing with the role of private companies, could support research on the assembling of publicness to spark alternative imaginaries and nurture novel futures of public-private relations in international politics.

Acknowledgments

This article has a history of five years and one pandemic behind it. We, thus, have many people, colloquia, and conferences to thank. While we cannot mention everybody who has helped by providing valuable comments and suggestions, we are particularly grateful to Rocco Bellanova, Christian Bueger, Daniel Lambach, Anna Leander, Rens van Munster, and Karen Lund Petersen, who all commented on this article outside of organized fora. We also thank the reviewers and the editors of this thematic issue for supporting this article and their editorial work.

Conflict of Interests

The authors declare no conflict of interests.

References

Abrahamsen, R., & Williams, M. C. (2009). Security beyond the state: Global security assemblages in international politics. *International Political Sociology*, *3*(1), 1–17.

Acuto, M., & Curtis, S. (Eds.). (2014). *Reassembling international theory*. Palgrave Macmillan.

Aradau, C., & Huysmans, J. (2014). Critical methods in international relations: The politics of techniques, devices and acts. *European Journal of International Relations*, *20*(3), 596–619.

Arthur, C. (2013, December 5). Microsoft likens government snooping to cyber attacks. *The Guardian*. https://www.theguardian.com/technology/2013/dec/05/microsoft-likens-government-snooping-cyber-attacks

Avant, D. D. (2005). Private security companies. *New Political Economy*, *10*(1), 121–131.

Baum, M. A., & Potter, P. B. K. (2019). Media, public opinion, and foreign policy in the age of social media. *The Journal of Politics*, *81*(2), 747–756.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology*, *8*(2), 121–144.

Beaumier, G., Kalomeni, K., Campbell-Verduyn, M., Lenglet, M., Natile, S., Papin, M., Rodima-Taylor, D., Silve, A., & Zhang, F. (2020). Global regulations for a digital economy: Between new and old challenges. *Global Policy*, *11*(4), 515–522.

Berling, T. V., & Bueger, C. (Eds.). (2015). *Security expertise: Practice, power and responsibility*. Routledge.

Best, J., & Gheciu, A. (2014). Theorizing the public as practices: Transformations of the public in historical context. In J. Best & A. Gheciu (Eds.), *The return of the public in global governance* (pp. 15–44). Cambridge University Press.

Brem-Wilson, J. (2017). La vía campesina and the UN Committee on world food security: Affected publics and institutional dynamics in the nascent transnational public sphere. *Review of International Studies*, *43*(2), 302–329.

Broeders, D., & van der Berg, B. (2020). Governing cyberspace behavior, power, and diplomacy. In D. Broeders & B. van den Berg (Eds.), *Governing cyberspace behavior, power, and diplomacy* (pp. 1–15). Rowman and Littefield.

Buchanan, I. (2020). Assemblage theory, or, the future of an illusion. *Deleuze Studies*, *11*(3), 457–474.

Bueger, C. (2018). Territory, authority, expertise: Global governance and the counter piracy assemblage. *European Journal of International Relations*, *24*(3), 614–637.

Bueger, C., & Liebetrau, T. (2023). Governing assemblages: Territory, technology and traps. In F. Gadinger & J. Aart Scholte (Eds.), *Polycentrism: How governing works today* (pp. 236–259). Oxford University Press.

Callon, M., Lascoumes, P., & Barthe, Y. (2009). *Acting in an uncertain world: An essay on technical democracy*. MIT Press.

Charney, S. (2013). *Challenges and opportunities in defining cybersecurity norms*. Microsoft.

Christensen, K. K., & Liebetrau, T. (2019). A new role for "the public"? Exploring cyber security controversies in the case of WannaCry. *Intelligence and National Security*, *34*(3), 395–408.

Christensen, K. K., & Lund Petersen, K. (2017). Public–private partnerships on cyber security: A practice of loyalty. *International Affairs*, *93*(6), 1435–1452.

Culpepper, P. D., & Thelen, K. (2020). Are we all Amazon primed? Consumers and the politics of platform power. *Comparative Political Studies*, *53*(2), 288–318.

Dahlgren, P. (2005). The internet, public spheres, and political communication: Dispersion and deliberation. *Political Communication*, *22*(2), 147–162.

Dean, J. (1999). Making (it) public. *Constellations*, *6*(2), 157–166.

Dewey, J. (1999). *The public and its problems*. Swallow Press.

Digital Peace Now. (n.d.). *Digital peace now* [Petition]. https://digitalpeacenow.org/take-action

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32.

Eckersley, R. (2007). A green public sphere in the WTO?: The amicus curiae interventions in the transatlantic biotech dispute. *European Journal of International Relations*, *13*(3), 329–356.

Eichensehr, K. E. (2019). Digital Switzerlands. *University of Pennsylvania Law Review*, *167*(3), 665–732.

Fairbank, N. A. (2019). The state of Microsoft?: The role of corporations in international norm creation. *Journal of Cyber Policy*, *4*(3), 380–403.

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative Inquiry*, *12*(2), 219–245.

Flyverbom, M., Deibert, R., & Matten, D. (2019). The governance of digital technology, big data, and the internet: New roles and responsibilities for business. *Business & Society*, *58*(1), 3–19.

Fraser, N. (1990). Rethinking the public sphere: A contribution to the critique of actually existing democracy. In C. Calhoun (Ed.), *Habermas and the public sphere* (pp. 109–142). MIT Press.

Gorwa, R., & Peez, A. (2020). Big tech hits the diplomatic circuit: Norm entrepreneurship, policy advocacy, and Microsoft's cybersecurity tech accord. In D. Broeders & B. Van Den Berg (Eds.), *Governing cyberspace: Behavior, power and diplomacy*. Rowman and Littlefield.

Gronau, J., & Schmidtke, H. (2016). The quest for legitimacy in world politics—International institutions' legitimation strategies. *Review of International Studies*, *42*(3), 535–557.

Habermas, J. (1962). *Strukturwandel der Öffentlichkeit: Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft; mit einem Vorwort zur Neuauflage 1990* [The structural transformation of the public sphere: An inquiry into a category of bourgeois society]. Suhrkamp.

Haraway, D. (1988). Situated knowledges: The science question in feminism and the privilege of partial perspective. *Feminist Studies*, *14*(3), 575–599.

Hofferberth, M. (Ed.). (2019). *Corporate actors in global governance: Business as usual or new deal?* Lynne Rienner Publishers.

Honig, B. (2017). *Public things: Democracy in disrepair*. Fordham University Press.

Hurel, L. M., & Lobato, L. C. (2018). Unpacking cyber norms: Private companies as norm entrepreneurs. *Journal of Cyber Policy*, *3*(1), 61–76.

Isin, E., & Ruppert, E. (2017). *Being digital citizens*. Rowman and Littefield.

Jeutner, V. (2019). The Digital Geneva Convention: A critical appraisal of Microsoft's proposal. *Journal of International Humanitarian Legal Studies*, *10*, 158–170.

Klotz, A., & Prakash, D. (2008). *Qualitative methods in international relations: A pluralist guide*. Palgrave Macmillan.

Kolmasova, S. (2022). Global assemblage of the responsibility to protect. *Globalizations*, *19*(8), 1328–1345.

Krahmann, E. (2008). Security: Collective good or commodity? *European Journal of International Relations*, *14*(3), 379–404.

Kratochwil, F. (2006). On legitimacy. *International Relations*, *20*(3), 302–308.

Law, J., & Urry, J. (2004). Enacting the social. *Economy and Society*, *33*(3), 390–410.

Leander, A. (2005). The power to construct international security: On the significance of private military companies. *Millennium*, *33*(3), 803–825.

Leander, A., & van Munster, R. (2007). Private security contractors in the debate about Darfur: Reflecting and reinforcing neo-liberal governmentality. *International Relations*, *21*(2), 201–216.

Liebetrau, T., & Monsees, L. (2022). Cybersecurity. In A. Ceron (Ed.), *Elgar encyclopedia of technology and politics* (pp. 9–14). Edward Elgar Publishing.

Loughlan, V., Olsson, C., & Schouten, P. (2015). Mapping. In C. Aradau, J. Huysmans, A. Neal, & N. Voelkner (Eds.), *Critical security methods: New frameworks for analysis* (pp. 23–56). Routledge.

Maghalaes, J. C., & Couldry, N. (2021). Giving by taking away: Big tech, data colonialism, and the reconfiguration of social good. *International Journal of Communication*, *15*, 343–362.

Marres, N. (2007). The issues deserve more credit: Pragmatist contributions to the study of public involvement in controversy. *Social Studies of Science*, *37*(5), 759–780.

Marres, N. (2012). *Material participation: Technology, the environment and everyday publics*. Palgrave Macmillan.

Marres, N., & Lezaun, J. (2011). Materials and devices of the public: An introduction. *Economy and Society*, *40*(4), 489–509.

McKay, A., Nicholas, P., Neutze, J., & Sullivan, K. (2014). *International cybersecurity norms: Reducing conflict in an internet-dependent world*. Microsoft.

Mende, J. (2023). Business authority in global governance: Companies beyond public and private roles. *Journal of International Political Theory*, *19*(2), 200–220.

Mende, J., & Müller, T. (2023). Publics in global politics: A framing paper. *Politics and Governance*, *11*(3), 91–97.

Microsoft. (2014). *Conundrums in cyberspace—Exploiting security in the name of, well, security*. https://blogs.microsoft.com/on-the-issues/2014/02/25/conundrums-in-cyberspace-exploiting-security-in-the-name-of-well-security

Microsoft. (2017). *A Digital Geneva Convention to protect cyberspace* (Microsoft Policy Papers). https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH

Microsoft. (2022). *Special report: Ukraine. An overview of Russia's cyberattack activity in Ukraine*. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

Mitzen, J. (2005). Reading Habermas in anarchy: Multilateral diplomacy and global public spheres. *The American Political Science Review*, *99*(3), 401–417.

Monsees, L. (2019). Public relations: Theorizing the contestation of security technology. *Security Dialogue*, *50*(6), 531–546.

Monsees, L., Liebetrau, T., Austin, J. L., Leander, A., & Srivastava, S. (2023). Transversal politics of big tech. *International Political Sociology*, *17*(1), 1–23.

Norman, D. J. (2019). Transnational civil society and informal public spheres in the nuclear non-proliferation regime. *European Journal of International Relations*, *25*(2), 486–510.

O'Sullivan, K. (2018a). *'Digital peace now' launches this weekend*. Microsoft. https://blogs.microsoft.com/on-the-issues/2018/09/28/digital-peace-now-launches-this-weekend

O'Sullivan, K. (2018b). *Continuing on the path toward digital peace*. Microsoft. https://blogs.microsoft.com/on-the-issues/2018/12/02/continuing-on-the-path-toward-digital-peace

Ong, A., & Collier, S. J. (2005). Global assemblages, anthropological problems. In A. Ong & S. J. Collier (Eds.), *Global assemblages. Technology, politics and ethics as anthropological problems* (pp. 3–21). Blackwell Publishing.

Oyedemi, T. D. (2020). Digital coloniality and "next billion users": The political economy of Google station in Nigeria. *Information, Communication & Society*, *24*(3), 329–343.

Papacharissi, Z. (2002). The virtual sphere: The internet as a public sphere. *New Media & Society*, *4*(1), 9–27.

Pond, P., & Lewis, J. (2019). Riots and Twitter: Connective politics, social media and framing discourses in the digital public sphere. *Information, Communication & Society*, *22*(2), 213–231.

Roberts, D., & Kiss, J. (2013, December 9). Twitter, Facebook and more demand sweeping changes to US surveillance. *The Guardian*. https://www.theguardian.com/world/2013/dec/09/nsa-surveillance-tech-companies-demand-sweeping-changes-to-us-laws

Rosenau, J. N. (1995). Governance in the twenty-first century. *Global Governance*, *1*(1), 13–43.

Rosenau, J. N., & Czempiel, E. O. (Eds.). (1992). *Governance without government*. Cambridge University Press.

Ruggie, J. G. (2004). Reconstituting the global public domain: Issues, actors, and practices. *European Journal of International Relations*, *10*(4), 499–531.

Schwartz-Shea, P., & Yanow, D. (2012). *Interpretive research design: Concepts and processes*. Routledge.

Smith, B. (2017a). *Transcript of keynote address at the RSA Conference 2017 "The Need for a Digital Geneva Convention"* [Speech transcript]. Microsoft. https://blogs.microsoft.com/uploads/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf

Smith, B. (2017b). *The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack*. Microsoft. https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack

Smith, B. (2018a). *34 companies stand up for cybersecurity with a tech-accord*. Microsoft. https://blogs.microsoft.com/on-the-issues/2018/04/17/34-companies-stand-up-for-cybersecurity-with-a-tech-accord

Smith, B. (2018b). *An important step toward peace and security in the digital world.* Microsoft. https://blogs.microsoft.com/on-the-issues/2018/11/12/an-important-step-toward-peace-and-security-in-the-digital-world

Smith, B., & Browne, C. A. (2019). *Tools and weapons: The promise and the peril of the digital age*. Hodder and Stoughton.

Srivastava, S. (2021). Algorithmic governance and the international politics of big tech. *Perspectives on Politics*. Advance online publication.

Stevens, T. (2016). *Cyber security and the politics of time*. Cambridge University Press.

The Cybersecurity Tech Accord, 2017, https://cybertechaccord.org/accord

Volkmer, I. (2014). *The global public sphere: Public communication in the age of reflective interdependence*. Polity Press.

Walker, R. B. J. (2010). Democratic theory and the present/absent international. *Ethics & Global Politics*, *3*(1), 21–36.

Walters, W., & D'Aoust, A. M. (2015). Bringing publics into critical security studies: Notes for a research strategy. *Millennium: Journal of International Studies*, *44*(1), 45–68.

West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society*, *58*(1), 20–41.

Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.

About the Authors

Tobias Liebetrau is a researcher at the Centre for Military Studies, Department of Political Science, University of Copenhagen. He studies theoretical, methodological, and political aspects of cybersecurity, digital technology, and infrastructure. His work has appeared in journals including *International Political Sociology*, *European Journal of International Security*, and *Contemporary Security Policy*.

Linda Monsees is a researcher at the Center for Governance of Emerging Technologies. Her expertise lies in the study of international security and how digital technologies impact security practices but also wider society. At the moment, she conducts research on the idea of digital sovereignty, the politics of semiconductors, and broader questions about the role of private companies in this field.