10. Private Authority and the Political Economy of Private Companies in Cybersecurity Crises and Conflicts

Louise Marie Hurel

<b>Introduction

On 28 February 2022, four days after the outbreak of the Russo-Ukrainian War, Brad Smith, President of Microsoft wrote: 'One of our principal and global responsibilities as a company is to help defend governments and countries from cyberattacks' (Smith, 2022). Indeed, the company has sought to 'walk the talk' prior to and throughout the course of the war. The day before Russia's invasion of Ukrainian territory, Microsoft had reported FoxBlade, a wiper malware that was used to target financial institutions and government ministries in Ukraine. Microsoft shared this intelligence with the White House, which later asked the company to share details of the malware with other European countries, especially the Baltics and Poland, over fears of replication of the malware beyond Ukrainian infrastructure (Sanger et al., 2022). Three months later, Microsoft published a report, 'Defending Ukraine: Early Lessons from the Cyber War' (Microsoft, 2022b). The report, aimed at a broader audience, highlighted the key trends of cyber operations and influence operations and outlined four pillars to counter Russian cyber threats: digital tactics, public-private cooperation, multilateralism, and free expression.

A couple of months later, Google published a 50-page report titled, 'Fog of War: How the Ukraine Conflict Transformed the Cyber Landscape' (Google, 2023). The title resonated with

many political scientists and International Relations scholars in its invocation of a concept strongly associated with Carl von Clausewitz's *On War* (Clausewitz, 1976). Clausewitz argued, among other things, that 'war is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty. A sensitive and discriminating judgement is called for; a skilled intelligence to scent out the truth' (Clausewitz, 1976, p. 101). Google's report did not seek to be a reflection on the philosophy of war, nor does it provide a direct and explicit reference to Clausewitz. As one scrolls through the pages, a different language is presented altogether: a detailed description of cyber and influence operations conducted by different Russian 'government-backed attackers'. The document outlines the phases of the operations, modalities of attacks and campaigns, tactics, and so on. Private companies using terms familiar from the canonical theory of war without explicitly referencing Clausewitz might seem a mere displacement of terminology in a report. However, the activities of Microsoft, Google and other firms in conflicts and crises are at the core of understanding the role of private authority in contemporary cybersecurity (geo)politics, in general, and cyber operations, in particular.

National crises and conflicts were once conceived primarily as the responsibility of governments – and, in the case of warfare, a prerogative of sovereign states – but in practice are rarely detached from private governance. Rather than being mere providers of infrastructure or ad hoc solutions to protect and mitigate risks, the involvement of companies such as Microsoft, Mandiant (part of Google), Slovakian threat intelligence company ESET, and many others in existing conflict, crises or following diplomatic éclats (see Microsoft, 2022) open up a number of relevant questions about the motivations, interests, legality and ultimately the power of private actors in geopolitical contestation. What is more, these companies have also increasingly

expanded their role in supporting defensive operations and activities (vulnerability reporting and management, incident response) to, at times, more controversial offensive-leaning activities to infiltrate, disrupt and destroy systems of 'adversaries,' raising additional questions of how deeply engaged they should be engaged in cybersecurity provision (Pattison, 2020).

To understand the expressions of private companies' roles in conflict and crises, I suggest two moves are required. First, it entails stepping back from the often-portrayed 'newness' of cybersecurity dynamics and revisiting existing literature on private-sector engagement in conflict, followed by positioning the space of action and influence of these actors in shaping cybersecurity politics. Second, it requires a closer investigation of the different levers (existing and emergent) and activities in which these companies are engaged in, how these activities contribute to the establishment of their authority in cybersecurity governance, and their particular expressions in cases of conflict and crises.

In practice, therefore, this chapter examines how private companies' practices and legitimacy-making strategies have been conceptualized by cybersecurity scholars. It then positions the discussion in a broader interdisciplinary field that has already sought to reflect on the politics of the private sector in security and provides examples of those practices of legitimacy-making from a market and policy perspective. Finally, it proposes pathways for future research agendas on this topic. This chapter, therefore, while concerned with cyberwarfare, also looks at these other dynamics in order to explore conflict-related private-sector activity.

This chapter should also be read with at least two qualifications in mind. First, that the terms 'private sector' and 'private companies' encompass a vast array of actors in cybersecurity and could include diverse legal, grey, and 'illegal' or unregulated companies that shape the field. This chapter cannot offer an exhaustive analysis of this extensive range of actors, concentrating

instead on the role of 'big tech' companies and threat intelligence firms. However, it is important to recognize the vast array of other private companies, such as highly defensive ones (private CERTs, incident response providers, 'bug bounty' platforms), or more offensive-leaning entities like 'grey hat' and 'black hat' hacker companies, defense contractors, state-sponsored hackers, and so-called 'cyber mercenaries' (McMurdo, 2016; Pattison, 2020).

Second, that the investigation of changing expressions of private authority and governance in cybersecurity (through the analysis of companies in this field) should not be seen as a reference to a distinct kind of influence that is portrayed as a binary: public 'or' private. States rely on these companies for their hardware and software infrastructure, security protocols and services, capacity to aggregate information and other assets, which creates an entanglement of public-private ownership and management over infrastructure, data and services. Moreover, as explored later in the chapter, many of these big companies are responsible for delivering services, technologies and training under strategic government-led capacity building or crisis response efforts. This further illustrates a continuum of public-private relations, some of which can be framed as the procurement of services from one government to another facilitated by private companies. That is also the case of nation-state proxies for cyber operations, where it is often challenging to distinguish between state and private actors such as cyber mercenaries (hackers-for-hire), patriotic hackers or self-organized groups (Schmoldt, Chapter 9, this volume). Additionally, this entangled influence also includes 'designing formal and informal rules for products, establishing sectoral regulation in tech, certifying professional competency and setting technical standards that impact society at large' (Hurel and Lobato, 2020, p. 288; Hall and Biersteker 2002; Rudder et al., 2016) These and other dimensions highlight that the investigation

of expressions of private authority in international cybersecurity politics are indissociable from the 'public' authority.

<b>Not a new story: emergence of private authority in cybersecurity

There are multiple ways of perceiving the emergence of private companies in cyber operations and crises. This section highlights at least three layers that have, concomitantly, laid the foundations for much of the contemporary dynamics of power and influence for these companies in this field: (i) states performing like markets through, among other things, ample push towards privatization; (ii) the expansion of the privatization of security; and (iii) more specifically and recently, market consolidation of a range of cybersecurity players. In 1991, Susan Strange noted that 'we shall never get to the bottom of other puzzles in international relations unless we put the study of international business at the centre, together with states, instead of the periphery' (Strange, 1991, p. 245). The problem, however, is that the story about conflict and crises have been increasingly told through a state-centric lens when, ultimately, the embeddedness of information and communications technologies across different societies and sectors – platforms (Gorwa, 2019), surveillance (Hayes, 2012), cloud services (Cubitt et al., 2011), applications (van Eeten, 2021) and others – has also meant that the governance of security, and cybersecurity specifically, is intimately entangled with private companies.

States, as the classic unit of analysis in International Relations and other fields, have derived their legitimacy from their territory, international recognition, and monopoly of violence/force (Weber, 1946; Hobbes, 2008). That does not mean they are comprise a stable, standardized or opaque unit of analysis. However, it does reflect the longstanding mantra of the Westphalian notion of sovereignty later codified in the United Nations Charter after World War II, which in itself has been a conceptual fountain for assuming the stability of the existence of the nation-

state. More interestingly is that, at the same time, and especially following the end of the Cold War and the push towards economic liberalization, 'the nature of the nation-state itself keeps evolving towards what has been called a market-state with increasing and systemic privatization' (Maurer, 2018, p. 3).

Following the 1990s, ceding power to supranational institutions (International Monetary Fund, World Trade Organization) and private companies (financial firms and/or credit rating agencies) became a precondition for states wishing to participate in the globalized economy (Sassen, 1999). Many scholars reflected on the shift from public to private authority given the need to cope with international information flows, jurisdictional challenges and transnational threats. However, rather than a 'shift', it exposed a key paradox of the role of the state in the twenty-first century, according to the liberal view whereby the state's own existence and reassertion is preconditioned on its capacity to become more market-like. That is the case of Philip Bobbitt's notion of the 'market-state', where he argues that rather than the end of the state, governments will seek to maximize for opportunity (rather than the welfare) of its people – depending on how much they can grasp the opportunities from engagement in a global economy (Bobbitt, 2003).

A second movement that merits equal attention is the privatization (and outsourcing) of security, which is far from new. In the fifteenth and sixteenth centuries, mercantile companies became a driving force in colonial expansion and exploration with English privateers at times joining the Royal Navy to fight against the Spanish Armada given their expertise and knowledge (see Egloff, 2017). Centuries later, post-Cold War military cuts meant that fewer resources were left for peacekeeping, leading to increased interest from governments in outsourcing security services, principally for reasons of cost efficiency. This left private companies to meet capacity shortfalls, perform training, develop security frameworks, and help with security responses

(Cilliers, 2002; Brooks and Laroia, 2005). Other cases such as the war in Iraq later exposed the role of private military companies like Blackwater as key providers of US military capacity (see Avant, 2005) and the ethical and legal challenges of that relationship (Leander, 2010), particularly following the 2007 Nisour Square shooting in Baghdad. What we have then is a 'marriage' between a global economy that encourages states to reaffirm their own stance as 'developed' and 'relevant' when delegating services to private actors and market forces on the one hand, and the evolving privatization of security and technological infrastructure on the other. As Kevin O'Brien (1998, p. 80) notes, 'by privatizing security and the use of violence, removing it from the domain of the state and giving it to private interests, the state in these instances is both being strengthened and disassembled.'

Outsourcing of security equally informs conflict, crises and peacetime activities in cybersecurity, albeit conveyed differently. During conflict, self-organised and state-affiliated groups have been one of the expressions of how private authority beyond the realm of private companies can be exerted. The formation of 'malicious' groups such as the Syrian Electronic Army, which operated as 'counter-revolutionary hackers' defending Bashar Al-Assad's regime and targeting Western governments (Harding and Arthur, 2013); or still-ambiguous formations (yet not deemed 'malicious') such as the Ukrainian IT Army of volunteers from within and outside Ukraine to help conduct denial-of-service attacks and other activities against Russia (Render-Katolik, 2023) reflect the porous nature of private authority formation in conflict, although in-depth analysis is beyond the scope of this chapter. A clearer example of private companies' involvement in conflict would include – as detailed later in this chapter – their provision of critical infrastructure and operating as vehicles for government assistance in both conflict and crisis response. An example of the former is Amazon Web Services supporting Ukraine's

transfer of government data to a server outside its territory; and of the latter, Microsoft's support in investigating Iranian attacks against the Albanian government in September 2022, which later led directly to the severing of diplomatic ties between those countries (Microsoft, 2022a).

However, given that most cyber operations are conducted below the threshold of armed conflict, many of these private companies operate at times in a grey zone. Companies such as Booz Allen Hamilton, for example, have provided a series of training and operational support to activities conducted by US Cyber Command (Booz Allen Hamilton, 2016; Brewster, 2021). In cases such as these, scholars have argued that 'private firms can justifiably launch some cybersecurity services – defensive measures [i.e., patching, antivirus software implementation, administrative controls] – but are not permitted to perform others – offensive measures [i.e., hacking back, supporting Active Cyber Defense]' (Pattison, 2020, p. 233). There are also peacetime activities in the hands of private companies that contribute to the consolidation and expansion of states' reliance on them in later conflict, such as risk compliance and cloud services.

Big Tech companies, threat intelligence companies, cloud solutions vendors, 'bug bounty' platforms, cyber insurance vendors, hackers-for-hire and even ransomware groups are all expressions of the complex market consolidation of a range of private actors in cybersecurity, a third shift supporting the emergence of private authority in cybersecurity. The rise of these and other players are rooted in an ongoing outsourcing of infrastructure (Dunn Cavelty and Suter, 2009), capacities (Collett and Barmpaliou, 2021), capabilities (Maurer, 2018) and security (Berntsson and Kinsey, 2016). None of these are new or unique to cybersecurity but they amplify and contribute to a specific topography of private-sector cybersecurity politics and practices. Moreover, many of these companies have taken intra- and extra-organisational measures (Hurel and Lobato, 2020) to engage in cyber diplomatic efforts at the UN with the purpose of informing

and shaping international norms guiding state behaviour in cyberspace (Hurel and Lobato, 2018). Additionally, some of them have also sought to create platforms for socializing norms within the private sector itself (Gorwa and Peez, 2020; Eggenschwiler, 2022). These and other examples (some of which will be further unpacked) highlight the dynamic and evolving role of private companies in shaping cybersecurity governance and international politics.

It might seem commonplace to make the case that private governance is tethered to public governance of cybersecurity, given their technological interdependencies and the ubiquity of security outsourcing. However, it is more challenging to locate the sources of their respective legitimacy. So far, we have primarily reflected on the space they have occupied in a state-based view of security. Scholars have suggested that a broad understanding of non-state actors' legitimacy means that 'they perform the role of authorship over some important issue or domain', are recognised in what they do by a broader audience, and conduct activities such as agenda-setting and the development of policies, practices, rules and norms (Hall and Biersteker, 2002, p. 4). I approach the influence of private companies in making and shaping cybersecurity through an overview of some of the instances (practices and discourses) and mechanisms (initiatives) that many of these players have devised more broadly, the layers of authority these represent, and how they relate to specific cases of conflict and crisis. Conceptually, it draws from the understanding that private authority refers to 'institutionalised forms or expressions of power' (Hall and Biersteker, 2002, p. 4). It is, therefore, set against the backdrop of a broader and much needed exercise of investigating the 'standard' and specific expressions of private-sector legitimacy-making in cybersecurity.

<b>Layers of authority

Governments usually look to the ICT industry to prevent, detect, respond to and recover from cyberattacks (Charney et al., 2016). When analysing the case of the US, Kristen Eichensehr (2017) noted that while the US has, in many instances, failed to strengthen public-private partnerships, a closer evaluation of the country's history of policies and measures shows the existing presence of public-private cybersecurity governance. She highlights four areas where that shared governance has worked previously in the context of responding to international cyber threats: (i) disrupting networks of infected computers used by transnational criminal groups; (ii) remediating software vulnerabilities; (iii) attributing cyber intrusions to state-linked or state-sponsored actors; and (iv) defending privately owned systems from sophisticated actors.

In this section I propose a closer look at the practices that make up private authority/corporate power in cybersecurity. While not seeking to be exhaustive, this section unpacks four dimensions of private authority in cybersecurity – that is, the levers used by private companies in legitimizing their presence and role in this field: market authority, infrastructural and platform power, normative influence, and knowledge and capacity influence (see Table 1). This analysis has applications beyond the specific contexts of cyber-related conflict and cyber operations, so I also provide examples of the wider implications of this framework for emerging conflict dynamics in other areas.

Table 1. A typology of private authority in cybersecurity.

Layers of authority	**Practices/Indicators**
Market authority	Market valuation Transnational presence

	Mergers and acquisitions
Infrastructural and platform power	Ownership over infrastructure (software and hardware) Widespread provision of and reliance from other parties on specific services (i.e., cloud) Provision of platform services
Normative influence	Lobbying Self-regulation/co-regulation Corporate Social Responsibility Devising internal teams to liaise with governments Engagement in multilateral negotiations Engagement in multistakeholder forums Ad-hoc creation or leadership in private sector, public-private or multistakeholder initiative
Knowledge and capacity influence	Publicly disseminate and display expert knowledge - Blog posts - Participation at events - Issue alerts/advisories - Publish special reports on specific operations - Conduct public attribution

	Privately disseminate and display expert knowledge - Brief governments and other parties of interest - Participate or organise private discussions Designation of the company's own threat actor taxonomy Training and framework development

<c>Market authority

Cybersecurity companies exert their influence through practices that seek to *establish their authority as market players*. More specifically, market authority refers to the consolidation and expansion of a company's market share, annual revenue, global footprint, number of staff, number of shareholders, acquisitions, Returns on Investments and other elements that are often indicators for determining and measuring the size and presence of a company in the economy (domestically or internationally).

Literature on private-sector influence in cybersecurity has focused on international norms, private governance and threat intelligence, often concentrating on the relationship between private companies and governments (Dunn-Cavelty and Suter, 2009; Carr, 2016; Christensen and Petersen, 2017). Scholarship exploring intra-organisational dynamics is uncommon (Hurel and Lobato, 2020; Harvey, 2023) and there are at least two reasons for this. One, that it is often challenging to access staff from different teams or divisions of the same company that are willing or able to be interviewed; non-disclosure agreements and organisational culture can be strong constraints on participation. Two, a relative lack of engagement with the business and management literature by scholars in International Relations and political science, although there

is growing interest from within International Political Economy. Leaving such gaps unaddressed may lead to a myopic view of the politics of private involvement in cybersecurity. Below I suggest two forms of legitimacy-making practices linked to market authority: market consolidation; and cybersecurity mergers and acquisitions.

Market authority and power have been widely debated in International Political Economy, where the emergence of neoliberal globalisation is posited as a challenge to state sovereignty and authority. Some scholars have argued that the concentration of technology development in the hands of private companies has left states with a choice between surrendering their own ownership and sovereignty over infrastructures and services and, if not abiding by those forces, dealing with marginalization (see Kobrin, 2002). While the trade-off might not be as clear as suggested by some, the consolidation of large-scale complex software and hardware supply chains, and their subsequent compromise by malicious cyber incidents has resurfaced the concern with how dependent states and societies are on the services and infrastructure provided and hosted by the private sector.

Such a dimension of legitimacy-making is not exclusive to cybersecurity and is the cornerstone of the value and influence of private companies in general. However, the emergence and establishment of cybersecurity as a global market is intimately connected with a history of more than 30 years of corporate battles for market consolidation in broader technology development. Investigating those historical and socio-political ties are fundamental to advancing research on the politics of private companies in cybersecurity. Since the 1980s, information technologies have been one of the epicentres of industrial growth and the structuring of a market rooted in a handful of companies (Akcigit et al., 2021). From the 1980s to the1990s, ICT development shifted from hardware to software development and interoperability, with Microsoft taking the

lead over the long-term market leader, IBM. Globalization of markets and supply chains in the 1990s and early 2000s also converged with the dot-com bubble, with a series of Internet giants seeking to carve out their space. For those companies that survived the burst of the dot-com bubble, the late 2000s and 2010s became a period of considerable market consolidation of technology companies, as some have called the 'Big Tech Bang' (Fernandez et al., 2020). Older tech giants such as Microsoft managed to remain and innovate, while then-newcomers Google, Facebook/Meta and others emerged, expanded and developed their businesses and platform models leading to subsequent cycles of the rise of platform services and strengthening of Chinese Big Tech. This was also a period where some cybersecurity companies started to emerge (Davies, 2021). The 1980s in particular were marked by the development of the commercial antivirus companies such as McAfee (1987), Symantec (1982) and Avast (1988). Similar yet earlier trends of consolidation were observed in the cybersecurity (then still largely antivirus) market when Symantec acquired Norton Security in 1999 and, more recently, Avast (2021). However, what followed since then is a diversification of specialized markets in cybersecurity focusing on compliance and vulnerability reporting, threat intelligence, bug bounty, pen-testing, and other markets such as cyber insurance.

As companies expand and consolidate, a closer look at their market value provides some indication of the place and space occupied by many of these tech and cybersecurity giants. According to Forbes' Global 2000 annual ranking of the world's largest companies (revenue, profits, assets, and stock market value) launched in 2023, 169 technology companies account for $4.2 trillion in combined revenue (past 12 months) (Ponciano, 2023). At the top of the ranking stands Alphabet – Google's parent company – followed by Microsoft and Apple. Beyond numbers, these figures also show that market concentration is not devoid from geographical

tendencies despite the transnational nature of their services and operations, with six out of ten based in the US, and all others based in east Asia. These and other elements illustrate a *layering of the politics of market authority* whereby companies manage to endure and innovate through cycles of financial and political crises.

Additionally, cybersecurity-related companies enhance their market legitimacy through mergers and acquisitions. Google's first security acquisition was in 2007; Microsoft – an older player in the market – had first acquired security software company XDegrees as early as 2002 (Sliwa, 2002). In 2022, Google generated headlines with the announcement of its $5.4 billion acquisition of threat intelligence giant Mandiant (Murphy et al., 2022). Prior to the acquisition, Google was known for its Threat Analysis Group, a specialized unit dedicated to cyber threat intelligence activities. Microsoft has not fallen short of its own moves to expand and consolidate cybersecurity through mergers and acquisitions. In 2022, Microsoft acquired Miburo, 'a cyber threat analysis and research company specializing on the detection of and response to foreign information operations' (Burt, 2022) and, earlier in 2021, RiskIQ, another threat intelligence and attack surface management company (Microsoft, 2021). In so doing, companies' acquisition processes can signal commitment and interest in scaling up its threat intelligence services – as was the case with Mandiant's multi-billion acquisition.

An investigation of Big Tech companies mergers and acquisitions can also illustrate which specific areas of investment have been prioritised in cybersecurity and what kinds of capacities are being integrated. Although Google's cybersecurity interest was highlighted by the acquisition of Mandiant, it was not the first time it had done so. A decade earlier, Google had acquired VirusTotal (Lardinois, 2012), an online malware-scanning platform, to enhance security across its products and services. In 2019, Chronicle, a cybersecurity company nested in Alphabet, was

then merged with Google Cloud. Chronicle offered, among other things, services for companies to upload, store and analyse internal security telemetry to investigate cyber threats (Gagliordi, 2019), as well as Security Operations Centre (SOC) services for cloud services – curating threat feeds, and providing management support for clients.

Finally, what these and other examples show is that Big Tech companies are particularly capable of conducting vertical integration while using it to also reassert themselves as effective actors in cybersecurity. That is the case with VirusTotal that, despite being acquired in 2012, was later incorporated within Chronicle and then into Google Cloud Platform as a result of the 2019 merger (Kurian, 2019). Even though the case highlights how big tech companies such as Google have used their mergers and acquisitions to enhance internal cybersecurity service provision, they also illustrate how companies may repurpose previous acquisitions depending on the circumstance (i.e., VirusTotal).

This section illustrates that the study of private sector market authority and legitimacy-making in cybersecurity is also historically linked to a sequencing of decisions taken by these companies (especially Big Tech) to invest in consolidating rather than primarily outsourcing security services. Companies do not simply take prominence in cybersecurity because they believe it is an area of interest, rather they have continuously sought to invest and acquire functionalities and services into their suite of products. Such a dimension of market authority often operates in the background of big private companies' engagement in conflict and crises, given that the perception of their legitimacy as 'desirable' and 'dependable' partners is linked to their capacity and market presence. However, when considering crisis responses, size is not always the sole or decisive factor. The decision of which company should provide licenses and other services to boost a 'victim' country often lies with the government that is seeking to act as a supporter. In

the case of Costa Rica – when the country was seeking to recover from a crippling ransomware incident perpetrated by the ransomware-as-a-service (RaaS) group Conti in 2021 – the United States 'sent over teams to assist, with donated software and expertise from Microsoft, IBM and Cisco' (Bufithis, 2022) and Spain donated 100,000 licenses of a nationally bred ransomware solution, MicroCLAUDIA (Gobierno, 2022).

<c>Infrastructural and platform power

Even though market share and other indicators are relevant to the consolidation of private authority in cybersecurity, firms' provision of software, hardware and services often mean that they exert an infrastructural influence on the governance of cybersecurity. Below I outline briefly the scholarly definitions of infrastructural and platform power and later in the section illustrate how they allow us to further unpack the modalities of private-sector cybersecurity influence within and beyond conflict.

Scholars across the social sciences have reflected on the multiple meanings of infrastructure. These range from material understandings of infrastructures as Large Technical Systems (LTS) like pipes, networks, electric grids and railways (Hughes, 1983), to phenomenological 'objects', that is, the understandings about our society and our work that become taken for granted (Star and Ruhleder, 1996). Most importantly, this literature has contributed to the investigation of politics in the making of those infrastructures, inviting scholars to interrogate their taken-for-grantedness and their 'unseen' power, be they material or knowledge infrastructures. As addressed previously, the governance of digital and broader sets of critical infrastructures are intimately associated with private companies.

The development of interconnected systems and infrastructures is indissociable from private authority and politics. Indeed, as DeNardis and Musiani (2016) have posited, the basic functional

elements of the Internet (protocols, domain names, routing, addressing) have become sites of political struggles between public and private entities. In the case of the mainstream history of the Internet (Murphy, 2002), while initially conceived as a government-funded and -led project in the United States, the subsequent development of the global infrastructure of material components and 'critical internet resources' (CIRs) like the Domain Name System (DNS), root servers and Internet transmission protocols, has increasingly been governed and influenced by private actors (DeNardis, 2009; Mueller, 2010). This is the case with Verisign, a US company founded in 1995 that operates as a global domain name registry and Internet infrastructure provider. It is the only company that administers two out of 13 root zone servers that are responsible for managing CIRs. Additionally, the majority of the root zone servers are administered by private entities (with some exceptions) and ten out of 13 are based in the US. Despite the multiple conceptualizations of infrastructure, *infrastructural and platform power* may refer to at least two expressions of private authority in cybersecurity: the perennial private governance or corporatization of critical infrastructures; and the increasing reliance of public-sector entities on private cybersecurity services (platforms and solutions).

One important example of how infrastructural power can be decisive in critical sectors is the case of Starlink's involvement in the Russo-Ukrainian War. Starlink is a division of Elon Musk's Space X company that provides Internet broadband through a constellation of low Earth orbit satellites. At the start of the war, Elon Musk had agreed to provide Starlink services to Ukraine after the country's Minister of Digital Transformation had briefly corresponded with him via Twitter/X (Borger, 2023). The objective was to prevent Ukraine from suffering from continuous Internet blackouts and also ensuring that their communication channels for operations could remain resilient and consistent despite Russian offensive kinetic and cyber operations. One year

into the war, in February 2023, SpaceX and the Ukrainian government came into slight disagreement. SpaceX's chief operating officer noted that even though they had known that Starlink had been used not just for internet but to support military communications, when they discovered that it was leveraged to operate drones, the chief operating officer noted that 'it was never meant to be weaponized' (Roulette, 2023). In addition to disagreements over the scope and purpose of use of a critical service provided between the company and the Ukrainian government, it was later discovered that Elon Musk had directly ordered the Starlink communications network to be shut off during a Ukrainian drone attack. According to Musk, he 'refused to comply with an emergency request from Ukrainian officials to enable Starlink connections to Sevastopol on the occupied Crimean peninsula' after having had 'conversations with a Russian official' (Kim, 2023).

In a situation as delicate and complex as an armed conflict, unilateral decisions such as the one taken by Musk without the Ukrainian government's knowledge or consent illustrates how infrastructural power can have real implications for the theatre of operations. It also raises a series of additional questions over the legal status of a company in a war, their own political alliances and interests, and the implications of their actions for critical service provision. Procurement and securing provision of resources during conflict and crises can often prove slow and/or fragile, not just because of the power of these companies over infrastructures but also because initial donations can often come to an end, requiring either the country or an ally to cover the financial costs, as the United States did in this case (Harper, 2023). Ukraine's dependence on a single commercial company for critical communication became more evident given that SpaceX's individualized leadership meant that Musk could 'call the shots' on what should or not be done (Jayanti, 2023).

Conflict and crises are also opportunities for expansion of infrastructural and platform power of a handful of companies. For small- and medium-sized companies, engaging in an armed conflict represents a remarkably elevated level of business risk. This is arguably the case for bigger companies too, but these situations can also present unprecedented opportunity to consolidate their presence in specific regions and strengthen their relationships with governments, as Amazon did at the beginning of Russia's war in Ukraine. Amazon worked with the Ukrainian government to transfer and develop cloud-based backups for essential government data which included but was not restricted to more than ten million gigabytes from dozens of Ukrainian ministries, schools, companies, and universities in the country (Amazon, 2022a). It is too early to assess the longer-term repercussions or political implications of such an unprecedented and abrupt transition of critical government assets to the hands of large corporate powers such as Amazon. However, it is clear that despite Amazon's $75 million top-level corporate investment in Ukraine (Amazon, 2022b), they have consolidated themselves as dependable and morally aligned partners of the Ukrainian government. This begs the question of the precedent this demonstration of infrastructure and platform power will have for other companies or even to Amazon's future involvement in conflict and crises. It also raises issues around the expectations national authorities may have of similar corporate rescue in times of crisis, and whether such assistance will in future be American, European or, perhaps, Chinese.

Altruism is rarely mentioned in descriptions of business incentives. While Microsoft, Amazon, SpaceX and others might have posed as moral supporters of Ukraine at the start by providing services, there is always the question of 'who pays the bill' at the end of the day. That is one of the constraints to the expansion or sustainability of infrastructure power in the particular context of crises and conflict situations. Six months after the start of the Russo-Ukrainian War, SpaceX

approached the US government to cover the costs of their Starlink operations in Ukraine – which they did (Jayanti, 2023).

Beyond the example of cloud as both a platform (interface, buildable and expandable) and an infrastructure (reliant on data centres, critical reliance on them from companies and governments), private companies also exert their influence and legitimacy through a host of platformized services. A deeper dive into the platform politics of cybersecurity companies is beyond the scope of this chapter (see Plantin and Hurel, forthcoming), but existing business models like 'bug bounty' platforms provide a clear example of how the private sector has sought to govern vulnerabilities by creating a two-sided market and moderate the relationship between governments, companies, and security researchers.

<c>Normative influence

Another way in which private companies seek to enhance their legitimacy in cybersecurity is by exerting *normative influence*, defined as a companies' active engagement in shaping standards, rules, regulations and norms for governing cybersecurity. Traditionally, the binary between public and private assumed that 'the public sphere' was the space where rules are defined by the state and the 'private sphere' is not only a reference to all other governance communities (civil society organisations, corporations, associations and individuals) but ultimately has been 'understood as subordinate to the state and subject to its regulation' (Backer, 2011, p. 752). Even though the artificial binary between public and private has been contested (Leander, 2009), its perpetuation has often obscured the investigation of private practices in making and shaping norms, especially considering the dominant 'imperative' of states' formal control over the use of force, which has also contributed to a state-centric view of security governance (Leander, 2010). This perspective persists in norms-making and norms entrepreneurship beyond the state,

especially in securitized areas such as cybersecurity where, despite private ownership of infrastructures and systems, states are still perceived as the ultimate generators and arbiters of norms (see Finnemore and Hollis, 2016).

Norms-shaping is enacted through practices such as diplomatic engagement, lobbying, self-regulation, co-regulation, public-private partnerships (PPPs) and ad hoc multistakeholder initiatives. The engagement of companies such as Microsoft in cyber diplomacy is one example of how private authority is articulated beyond the contractual business-to-business or PPP environment. Since the early to mid-2010s, Microsoft has engaged in cyber norms entrepreneurship through a series of activities which include but are not restricted to proposing a Digital Geneva Convention in 2017, engaging in UN cyber norms processes such as the Open-Ended Working Group (OEWG) since 2019, opening an office for UN engagement in 2020, working with delegations and non-governmental stakeholders to promote specific norms, and hiring the former Danish tech ambassador, Casper Klynge, to be the first Vice President for UN Affairs, followed by a former UK ambassador who later took the same position. When it comes to cyber norms development, it is not that other companies do not engage in these spaces – Hitachi (Japan) and Huawei (China) have previously participated in the OEWG sessions – rather that there is something particular to the way in which Microsoft assembles its internal teams, resources, expertise and existing international commercial presence with its ambition to become a quasi-diplomatic player (Hurel and Lobato, 2020). As suggested by Fairbank (2019), there are at least four objectives to the company's engagement in norms entrepreneurship: trust-building, software protection, balance of responsibility and socio-political influence. However, the company engages in this cyber norms entrepreneurship both at the diplomatic (Hurel and Lobato, 2019, 2020) and corporate levels (Gorwa and Peez, 2020). Cases such as this also illustrate how

internal changes can unlock different political engagements supporting the expansion of the services and footprint of the company internationally. Further research in this area could potentially show how intra-organisational measures associated with team building and restructuring supported or challenged the company's ambitions to situate itself as a major international cybersecurity player.

Scholarship on cyber norms entrepreneurship has expected that other companies would also seek to engage more actively in diplomatic circles. Since 2017, however, Microsoft still remains the outlier, although there are other expressions of normative influence concerning cyber diplomacy. Other coalitions of companies that have also sought to engage in such forums. That is the case of the International Chamber of Commerce (ICC) and the Cybersecurity Tech Accord. The latter, also an initiative spearheaded by Microsoft, has sought to provide a platform for entities across the private sector to advocate for certain norms and/or propose their own norms in contexts such as the Open-Ended Working Group. The ICC on the other hand, represents a much wider set of entities from the private sector and has also historically engaged in multilateral and bloc-type forums. It was founded in 1919 with the goal of providing a space for businesses to self-organise and develop their own standards and norms. As one of their blogs note, 'businesses need certainty and stability for success, and multilateralism is a key component of this' (Burge, 2023). In recent years, the ICC and other national offices such as the ICC London, have dedicated their agenda to conducting digital and cyber policy advocacy at the International Telecommunications Union, UN First Committee (OEWG), International Corporation for Assigned Names and Numbers, UN General Assembly and related processes, such as the Global Digital Compact (see ICC UK, n.d.).

<b>Knowledge and capacity influence

Another way in which Big Tech and cybersecurity companies reinforce their legitimacy is through posing as credible and reliable providers of cyber threat intelligence (CTI). Technology companies leverage the global presence of their software and hardware to position themselves as authoritative sources about the malicious activities and vulnerabilities they observe across their services. Cybersecurity companies also do so, often relying on the sensors, telemetry, customer base (geographic distribution) and services they provide to clients. Palo Alto Networks, for example, a cybersecurity solutions company established a specific threat intelligence team called Unit 42. Its self-appointed mission is twofold: protect the digital world from cyber attacks and collect and analyse threat intelligence to inform responses (Unit 42, n.d.). Like other firms in this field, Unit 42 organises itself internally to exert influence based on the credibility and objectiveness of 'knowing' the threat landscape and through the monitoring and identification of threats across their services through bespoke engagement with prospective and current clients.

Some of this work of knowledge and capacity-related legitimacy is expressed through the development teams dedicated to cybersecurity operating in and between technical and policy audiences. Google and Microsoft, despite not being principally branded as threat intelligence companies, have established groups with this function. Google has its Threat Analysis Group (TAG), responsible for tracking and countering government-backed hacking against Google and its users; Microsoft, on the other hand, also has teams linked to threat intelligence and law enforcement support, such as MSTIC, as its threat intelligence group was known until early 2023. Both sets of company teams reinforce Big Tech visibility by maintaining blogs and other public engagement channels which provide updates on technical attributions and investigations, and also brief governments on specific operations.

These teams, while important, gain more notoriety when the company engages in attribution of specific state-sponsored incidents, publish reports on the topic and, at times, establish their own taxonomy to name specific threat actors (see Lambert, 2023). Microsoft's and Google's reports on the war in Ukraine (Microsoft, 2022b; Google, 2023), mentioned at the start of this chapter, comprise a snapshot of the two most visible components of private-sector engagement in conflict that draws not only on the 'most powerful' companies but also on their attempts to showcase their expertise and knowledge in the context of the Russo-Ukrainian War. However, while there might be some novelty associated with the emphatic and public role of some Big Tech companies in Ukraine, as this chapter illustrates, private-sector engagement in conflict is far from new. The prominence of such actors in cybersecurity governance is articulated– through their market power, their embeddedness in countries' digital infrastructures, their investments and presence in national lobbying forums and among other areas.

Traditionally, war and conflict are scenarios permeated by uncertainty. However, it is precisely in the context of uncertainty that Google, Microsoft and other companies use the language of uncertainty to showcase their own epistemic certainty about cyber threat actors and their tactics, techniques and procedures. Reports, solutions and expert insight are commercialized or shared as the differential and yet crucial assets that governments as consumers require to properly address and mitigate emerging threats.

This section has outlined four types of expressions of private authority-making in cybersecurity: market authority, infrastructural power, normative influence, and knowledge and capacity influence. Rather than clearly separate, they should be seen as intimately imbricated, at times reinforcing and at other times potentially contradicting each other. The analyses of these expressions of private authority are not intended to be exhaustive but instead provide an

indicative picture of some of the underlying practices that express and articulate these diverse types of private authority.

<b>Beyond the cyber bubble: Tackling gaps in future research

This chapter focused on unpacking how companies engage in legitimacy-making strategies in cybersecurity; how these have been conceptualized in the scholarly literature; and highlighted the need for greater interrogation of the political-economic embeddedness of firms' actions. In proposing a typology for private authority, the chapter should be seen as a provisional intervention in the ongoing mapping of the evolving practices in the field. I outline some future areas of research below. Prior to that, however, we need to address two remaining dynamics that permeate the scholarly and policy reflections on the role of private companies in cybersecurity.

The first is the risk of losing sight of a broader field and literature that has long conceptualized and reflected on the politics of private companies in the realm of security. There are different private sector actors that merit further study and integration with the study of private authority, and this requires an interdisciplinary effort. This exercise includes more traditional defence contractors and the cybersecurity equivalent of private military companies working in the field conducting and supporting governments in either 'active defence' (i.e., honeypots or masquerading techniques to lure adversaries into one's own infrastructure) or offensive activities (i.e., hacking back) (see Pattison, 2020; Broeders, 2021). Other stakeholders, such as business associations and their role in lobbying for certain views and values in cybersecurity, as well as emerging market players like cyber insurers and bug bounty platforms (Bozzini, 2023), are equally important for understanding the political economy of private companies during peacetime and conflict. The second dynamic, linked to the first, is the risk of perceiving all cybersecurity politics as unique to this highly specialized field. As this chapter illustrates, while

there are indeed specific expressions of such politics in cybersecurity, closer reading of scholarly work across International Relations, management studies, business, sociology and others can provide a useful background for future interdisciplinary and more contextualized reflections on private authority and cybersecurity governance.

Future research should be attentive to the geographic entanglements of the companies being researched. In practice, this includes a couple of prospective scholarly exercises. First, it entails being sensitive to where these companies are based, especially transnational Big Tech. Are the values, justifications for action, and narratives global but perhaps speaking from a specific geographical standpoint? A second exercise is to go 'beyond Big Tech' and look at national and regional markets (Hurel, 2022). In so doing, new avenues of research could shed an important light on how these smaller – yet at times powerful – local or national cybersecurity providers also play a role in shaping cybersecurity beyond the 'international' realm, and how they interact with governments and with the Big Tech firms. In adopting such a line of enquiry, one delves into an understanding of cybersecurity politics and private authority that is expressed at a micro or domestic level. This might involve the application of other research methods such as more anthropological field work and use of transparency laws to access primary data regarding national contracts and so on. Such an exercise could also include non-English language fieldwork and a closer interrogation of the telemetry and data collection infrastructures of firms and their geographic preoccupations and priorities (see Fidler, 2023; Mumford and Shires, 2023).

Additionally, future research should seek to go beyond the external engagements of these companies and trace intra-organisational politics within international politics. This includes conducting more interviews with private companies, building rapport, and engaging in participant observation (as well as other ethnographic methods if possible). Longer term in-depth

research could significantly add to the investigation of the motivations and commitments of, for example, a cybersecurity company engaging in particular conflict or crises scenarios but not others. Another possibility is the investigation of smaller companies and local markets as expressions of sometimes less obvious – yet at times highly influential – connections between bespoke companies and political elites in specific countries. The latter could also be a fruitful avenue for linking local and global politics in cybersecurity.

Moreover, while private military security companies have been the object of great reflection in conflict studies, there are still important lessons and reflections to be drawn from those experiences. The deployment of these companies in conflict and/or peacekeeping operations have raised significant questions about the ethical and legal status of these companies in and adjacent to conflict theatres. Despite growing cybersecurity scholarship on the role of cyber mercenaries, hackers-for-hire, and whole organised crime business models such as RaaS, we are only starting to ask the key policy questions concerning their emergence and operation. Future research has the potential to continue exploring the evolving role of defence and specific cybersecurity contractors in filling the functional gaps of current cyber commands and whether, in cases such as these, it is possible – as ideally suggested by Pattison (2020) – to draw a line between private companies' involvement in defensive and offensive operations.

A key aspect of advancing research in cybersecurity and especially with private companies requires critical and purposeful thinking of how to deal with secrecy from different geographical standpoints (see LA/CS Net, 2023). Many researchers seeking to advance research in this field will face subjects that are bound by non-disclosure agreements and other corporate confidences. Future discussions on methods and secrecy should involve a cross-pollination between cybersecurity and other scholarly fields that face similar challenges such as surveillance studies,

conflict studies, financial crime and others (De Goede et al., 2020; see Gomez et al., Chapter 4, this volume).

Finally, as we enter into a new era of heightened global conflict and the increasing dependence of countries (especially developing ones) on outsourced infrastructure, there is a space for growing critical reflection over the nexus between crisis-conflict and cybersecurity. From a scholarly standpoint, part of this effort could include further intersections between conflict studies and cybersecurity studies, reflecting in particular on the learnings and particularities of private military companies and private-sector engagement in humanitarian or conflict situations and how that relates to or is unique for private-sector cybersecurity. An equally crucial point is to be able to interrogate the motivations, geographic focus, links with different governments, internal shifts, and narratives about what is 'right and wrong' emerging from these companies as they seek to legitimise or justify their involvement in or abstention from certain conflicts and crises scenarios.

<b>References

Akcigit, Ufuk, Wenjie Chen, Federico J. Diez et al. (2021) Rising Corporate Market Power: Emerging Policy Issues. *International Monetary Fund Staff Discussion Notes* 2021/001. https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2021/03/10/Rising-Corporate-Market-Power-Emerging-Policy-Issues-48619.

Aguerre, Carolina and Hernan Galperin (2015) Internet policy formation in Latin America: Understanding the links between the national, the regional, and the global. *GigaNet: Global Internet Governance Academic Network, Annual Symposium 2015*. https://dx.doi.org/10.2139/ssrn.2809883.

Amazon (2022a) Safeguarding Ukraine's data to preserve its present and build its future. 9 June. https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future.

Amazon (2022b) How Amazon is assisting in Ukraine. 21 June. https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine.

Backer, Larry Catá (2011) Private actors and public governance beyond the state: the multinational corporation, the Financial Stability Board, and the global governance order. *Indiana Journal of Global Legal Studies* 18(2): 751–802.

Berndtsson, Joakim and Christopher Kinsey (2016) *The Routledge Research Companion to Security Outsourcing*. London: Routledge.

Booz Allen Hamilton (2016) Booz Allen to help US Cyber Command boost cybersecurity. 13 July. https://www.boozallen.com/e/media/press-release/booz-allen-to-help-us-cyber-command-boost-cyber-security.html.

Borger, Julian (2023) Elon Musk ordered Starlink to be turned off during Ukraine offensive, book says. *The Guardian*. 7 September. https://www.theguardian.com/technology/2023/sep/07/elon-musk-ordered-starlink-turned-off-ukraine-offensive-biography.

Brewster, Thomas (2021) Pentagon cyber PR contractor admits dark web child sexual exploitation charges. *Forbes*. 6 December. https://www.forbes.com/sites/thomasbrewster/2021/12/06/booz-allen-cyber-command-pr-pleads-guilty-to-dark-web-child-pornography-charges/.

Broeders, Dennis (2016) The Public Core of the Internet: An International Agenda for Internet Governance. *WRR Report* 94. https://english.wrr.nl/publications/reports/2015/10/01/the-public-core-of-the-internet.

Broeders, Dennis (2021) Private active cyber defense and (international) cyber security: Pushing the line? *Journal of Cybersecurity* 7(1): tyab010.

Brooks, Doug and Gaurav Laroia (2005) Privatized peacekeeping. *The National Interest* 80: 121-125.

Bufithis, Gregory (2022) The Conti ransomware group, a crippled Costa Rica - and how things fall apart, even for our cyber tormentors. *Gregory Bufithis*. 11 July. https://www.gregorybufithis.com/2022/07/11/the-conti-ransomware-group-a-crippled-costa-rica-and-how-things-fall-apart/.

Burt, Tom (2022) Microsoft to acquire Miburo to boost threat intelligence research into new cyber threats. *Official Microsoft Blog*. 14 June. https://blogs.microsoft.com/blog/2022/06/14/microsoft-to-acquire-miburo/.

Carr, Madeline (2016) Public–private partnerships in national cyber-security strategies. *International Affairs* 92(1): 43–62.

Cezar, Asunur, Huseyin Cavusoglu and Srinivasan Raghunathan (2014) Outsourcing information security: Contracting issues and security implications. *Management Science* 60(3): 638–657.

Christensen, Kristoffer Kjærgaard and Karen Lund Petersen (2017) Public–private partnerships on cyber security: a practice of loyalty. *International Affairs* 93(6): 1435–1452.

Cilliers, Jakkie (2002) A role for private military companies in peacekeeping? *Conflict, Security & Development* 2(3): 145-151.

Clausewitz, Carl von (1976) *On War*. Eds. and trans. Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press.

Collett, Robert and Nayia Barmpaliou (2021) *International Cyber Capacity Building: Global Trends and Scenarios*. European Commission. https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf.

Costa Rica (2022) *Plan General de la Emergencia Ciberataques*. Comision Nacional de Prevencion de Riesgos y Atencion de Emergencias. https://www.cne.go.cr/recuperacion/declaratoria/planes/Plan%20General%20de%20la%20Emergencia%20por%20Ciberataques.pdf.

Cubitt, Sean, Robert Hassan and Ingrid Volkmer (2011) Does cloud computing have a silver lining? *Media, Culture & Society* 33(1): 149-158.

Davies, Vikki (2021) The history of cybersecurity. *Cyber Magazine*. 4 October. https://cybermagazine.com/cyber-security/history-cybersecurity.

De Goede, Marieke, Esmé Bosma and Polly Pallister-Wilkins, eds. (2020) *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*. London: Routledge.

DeNardis, Laura (2009) *Protocol Politics: The Globalization of Internet Governance*. Cambridge, MA: MIT Press.

DeNardis, Laura and Mark Raymond (2013) Thinking clearly about multistakeholder internet governance. *GigaNet: Global Internet Governance Academic Network, Annual Symposium 2013.* https://dx.doi.org/10.2139/ssrn.2354377.

DeNardis, Laura and Francesca Musiani (2016) Governance by infrastructure. In Francesca Musiani, Derrick L. Cogburn, Laura DeNardis and Nanette S. Levinson, eds. *The Turn to Infrastructure in Internet Governance.* New York: Palgrave Macmillan, 3-21.

Dunn Cavelty, Myriam and Manuel Suter (2009) Public-private partnerships are no silver bullet: an expanded governance model for critical infrastructure protection. *International Journal of Critical Infrastructure Protection* 2(4): 179-187.

Dunn Cavelty, Myriam and Andreas Wenger (2020) Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy* 41(1): 5-32.

Eggenschwiler, Jacqueline (2022) Big tech's push for norms to tackle uncertainty in cyberspace. In Myriam Dunn Cavelty and Andreas Wenger, eds. *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation.* London: Routledge, 186-204.

Fernandez, Rodrigo, Ilke Adriaans, Tobias J. Klinge and Reijer Hendrikse (2020) *The Financialisation of Big Tech.* Amsterdam: SOMO. https://www.somo.nl/nl/wp-content/uploads/sites/2/2020/12/Engineering_Financial-BigTech.pdf.

Fidler, Mailyn (2023) Infrastructure, law and cyber instability: an African case study. In Robert Chesney, James Shires and Max Smeets, ed. *Cyberspace and Instability*. London: Edinburgh University Press, 281-298.

Finnemore, Martha and Duncan Hollis (2016) Constructing norms for global cybersecurity. *American Journal of International Law* 110(3): 425-479.

Gagliordi, Natalie (2019) Alphabet's moonshot security firm Chronicle joins Google Cloud. *ZDNet*. 27 June. https://www.zdnet.com/article/alphabets-moonshot-security-firm-chronicle-joins-google-cloud/.

Google (2023) *Fog of War: How the Ukraine Conflict Transformed the Cyber Landscape*. https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf.

Gorwa, Robert (2019) What is platform governance? *Information, Communication & Society* 22(6): 854-871.

Gorwa, Robert and Anton Peez (2020) Big tech hits the diplomatic circuit: Norm entrepreneurship, policy advocacy, and Microsoft's cybersecurity tech accord. In Dennis Broeders and Bibi van der Berg, eds. *Governing Cyberspace: Behavior, Power, and Diplomacy*. Lanham, MD: Rowman and Littlefield, 263-284.

Harding, Luke and Charles Arthur (2013). Syrian Electronic Army: Assad's cyber warriors. *The Guardian*. 30 April. https://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background.

Jayanti, Amritha (2023) Starlink and the Russia-Ukraine War: a case of commercial technology for public purpose? *Belfer Center for Science and International Affairs*. 9 March. https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose.

Hayes, Ben (2012) The surveillance-industrial complex. In Kirstie Ball, Kevin Haggerty and David Lyon, eds. *Routledge Handbook of Surveillance Studies*. London: Routledge, 167-175.

Harper, Jon (2023) Pentagon contracting with SpaceX's Starlink to provide satellite communication capabilities to Ukraine. *DefenseScoop*. 1 June.

https://defensescoop.com/2023/06/01/pentagon-contracting-with-spacexs-starlink-to-provide-satellite-communication-capabilities-for-ukraine/.

Hurel, Louise Marie and Luisa Cruz Lobato (2018) Unpacking cyber norms: Private companies as norm entrepreneurs. *Journal of Cyber Policy* 3(1): 61–76.

Hurel, Louise Marie and Luisa Cruz Lobato (2020) Cyber-norms entrepreneurship? Understanding Microsoft's advocacy on cybersecurity. In Dennis Broeders and Bibi van der Berg, eds. *Governing Cyberspace: Behavior, Power, and Diplomacy*. Lanham, MD: Rowman and Littlefield, 285-314.

Hurel, Louise Marie (2022) Beyond the great powers: Challenges for understanding cyber operations in Latin America. *Global Security Review* 2(7): 21-31.

Hughes Thomas P. (1983) *Networks of Power: Electrification in Western Society, 1880-1930*. Baltimore, MD: Johns Hopkins University Press.

Hobbes, Thomas (2008) *Leviathan*. Ed. J.C.A. Gaskin. Oxford: Oxford University Press.

Eichensehr, Kristen E. (2017) Public-private cybersecurity. *Texas Law Review* 95(3): 467-538.

Kim, Victoria (2023). Elon Musk acknowledges withholding satellite service to thwart Ukrainian attack. *New York Times*. 8 September. https://www.nytimes.com/2023/09/08/world/europe/elon-musk-starlink-ukraine.html.

Kobrin, Stephen J. (2002) Economic governance in an electronically networked global economy. In Rodney Bruce Hall and Thomas J. Biersteker, eds. *The Emergence of Private Authority in Global Governance*. Cambridge: Cambridge University Press, 43-75.

Kshetri, Nir (2015) India's cybersecurity landscape: the roles of the private sector and public-private partnership. *IEEE Security & Privacy* 13(3): 16-23.

Kurian, Thomas (2019) Google Cloud + Chronicle: the security moonshot joins Google Cloud. *Google Cloud*. 28 June. https://cloud.google.com/blog/topics/inside-google-cloud/the-security-moonshot-joins-google-cloud.

LA/CS Net (2023) Latin American Cybersecurity Research Symposium: Questioning biases, building bridges. *Latin American Cybersecurity Research Network*. February. https://latamcyber.net/lacs-net-symposium-2022.

Lambert, John (2023) Microsoft shifts to a new threat actor naming taxonomy. *Microsoft Security*. 18 April. https://www.microsoft.com/en-us/security/blog/2023/04/18/microsoft-shifts-to-a-new-threat-actor-naming-taxonomy/.

Lardinois, Frederic (2012) Google acquires online virus, malware and URL scanner VirusTotal. *TechCrunch*. 7 September. https://techcrunch.com/2012/09/07/google-acquires-online-virus-malware-and-url-scanner-virustotal/.

Leander, Anna (2009) The privatization of international security. In Myriam Dunn Cavelty and Victor Mauer, eds. *The Routledge Handbook of Security Studies*. London: Routledge, 216-226.

Leander, Anna (2010) The paradoxical impunity of private military companies: Authority and the limits to legal accountability. *Security Dialogue* 41(5): 467–490.

Liebetrau, Tobias and Linda Monsees (2023) Assembling publics: Microsoft, cybersecurity, and public-private relations. *Politics and Governance* 11(3): 157-167.

Maurer, Tim (2018) *Cyber Mercenaries: The State, Hackers, and Power*. New York: Cambridge University Press, 3-28.

McMurdo, Jesse Jacob (2016) Cybersecurity firms – cyber mercenaries. *Homeland & National Security Law Review* 4(1): 35-78.

Microsoft (2021) Microsoft acquired RiskIQ to strengthen cybersecurity of digital transformation and hybrid work. 12 July. https://www.microsoft.com/en-us/security/blog/2021/07/12/microsoft-to-acquire-riskiq-to-strengthen-cybersecurity-of-digital-transformation-and-hybrid-work/.

Microsoft (2022a) Microsoft investigates Iranian attacks against the Albanian government. 8 September. https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/.

Microsoft (2022b) *Defending Ukraine: Early Lessons from the Cyber War*. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

Monsees, Linda, Tobias Liebetrau, Jonathan Luke Austin et al. (2023) Transversal politics of big tech. *International Political Sociology* 17(1), olac020.

Mueller, Milton L. (2010a) *Networks and States: The Global Politics of Internet Governance.* Cambridge, MA: MIT Press.

Mueller, Milton L. (2010b) Critical resource: An institutional economics of the Internet addressing-routing space. *Telecommunications Policy* 34(8): 405-416.

Murphy, Brian Martin (2002). A critical history of the Internet. In Greg Elmer, ed. *Critical Perspectives on the Internet*. Lanham, MD: Rowman & Littlefield, 27-45.

Murphy, Hannah, Richard Waters and Madhumita Murgia (2022) Google buys cyber security company Mandiant for $5.4bn. *Financial Times*. 8 March. https://www.ft.com/content/0eabf63d-29d6-49f0-bce8-1ef1d33467e2.

O'Brien, Kevin (1998) Military-advisory groups and African security: privatized peacekeeping? *International Peacekeeping* 5(3): 78-105.

Pattison, James (2020) From defence to offence: The ethics of private cybersecurity. *European Journal of International Security* 5(2): 233–254.

Plantin, Jean-Christophe, Carl Lagoze, Paul N. Edwards and Christian Sandvig (2018) Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society* 20(1): 293-310.

Ponciano, Jonathan (2013) The world's largest technology companies in 2023: a new leader emerges. *Forbes*. 8 June. https://www.forbes.com/sites/jonathanponciano/2023/06/08/the-worlds-largest-technology-companies-in-2023-a-new-leader-emerges/.

Render-Katolik, Aiden (2023) The IT Army of Ukraine. Center for Strategic & International Studies. 15 August. https://www.csis.org/blogs/strategic-technologies-blog/it-army-ukraine.

Roulette, Joey (2023) SpaceX curbed Ukraine's use of Starlink internet for drones – company president. *Reuters*. 9 February. https://www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet-drones-company-president-2023-02-09/.

Sanger, David E., Julian E. Barnes and Kate Conger (2022) As tanks rolled into Ukraine, so did malware. Then Microsoft entered the war. *New York Times*. 28 February. https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html

Sassen, Saskia (1999) Making the global economy run: the role of national states and private agents. *International Social Science Journal* 51(161): 409-416.

Sliwa, Carol (2002) Microsoft acquires maker of secure file access software. *ComputerWorld*. 11 September. https://www.computerworld.com/article/2578228/microsoft-acquires-maker-of-secure-file-access-software.html.

Smith, Brad (2022) Digital technology and the war in Ukraine. *Microsoft On the Issues*. 28 February. https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/.

Star, Susan Leigh and Karen Ruhleder (1996) Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information Systems Research* 7(1): 111–134.

Sweetman, Derek (2009) *Business, Conflict Resolution and Peacebuilding: Contributions from the Private Sector to Address Violent Conflict*. London: Routledge.

Unit 42 (n.d.) About. Palo Alto Networks. https://www.paloaltonetworks.com/unit42/about.

van Eeten, Michel (2017) Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity. *Digital Policy, Regulation & Governance* 19(6): 429-448.

Weber, Max (1946) Politics as a vocation. In *From Max Weber: Essays in Sociology*. Eds. and trans. H.H. Gerth and C. Wright Mills. New York: Oxford University Press, 77-128.