Department of Public Policy
CENTRAL EUROPEAN UNIVERSITY

TECH GIANTS AND THE UKRAINE WAR: RETHINKING POWER, SOVEREIGNTY, AND MODERN CONFLICT

By
AMANDA NARHAN PEREIRA

Submitted to
Central European University
Department of Public Policy

In partial fulfilment for the degree of MASTER OF ARTS IN INTERNATIONAL PUBLIC AFFAIRS

Supervisor: **DANIEL LARGE**

Vienna, Austria

2024

CEU eTD Collection

COPYRIGHT NOTICE

Copyright © Amanda Narhan Pereira, 2025. Tech Giants in the Ukraine War: Reshaping Modern Warfare and Geopolitics - This work is licensed under Creative Commons Attribution-NonCommercial-NoDerivatives (CC BY-NC-ND) 4.0 International license.

CEU eTD Collection

AUTHOR'S DECLARATION

I, the undersigned, **Amanda Narhan Pereira**, candidate for the MA degree in International Public Affairs declare herewith that the present thesis is exclusively my own work, based on my research and only such external information as properly credited in notes and bibliography. I declare that no unidentified and illegitimate use was made of the work of others, and no part of the thesis infringes on any person's or institution's copyright.

Vienna, 03 June 2025

Amanda Narhan Pereira

CEU eTD Collection

ABSTRACT

This thesis investigates a vitally important question: how are private technology companies reshaping war? It uses a qualitative case study methodology to examine the operational roles of three major technology firms—SpaceX, Microsoft, and Google—during the Ukraine war in particular. The study analyses their influence on military strategy, cyber defence, and information governance, drawing on primary and secondary sources including corporate actions, public statements, and conflict events. Key findings reveal that these companies are redefining their roles in the international system and performing sovereign-like functions by controlling critical digital infrastructure, shaping narratives, and influencing battlefield outcomes without formal state authority or democratic oversight. This dynamic challenges traditional International Relations theories centred on state sovereignty, suggesting a process where sovereignty becomes fragmented across digital platforms. The research also further highlights how Big Tech's growing geopolitical power blurs the lines between public and private domains. Ultimately, the thesis contributes to rethinking sovereignty and power in the digital age, emphasising the need to adapt IR traditional theories to account for non-state actors as central players in global politics.

Keywords: Big Tech; Power; Sovereignty; War and technology; Digital infrastructure; International Relations.

CEU eTD Collection

ACKNOWLEDGEMENTS

I would like to express my heartfelt thanks to my supervisor, Dr. Daniel Large, for his unwavering guidance and support throughout my time at CEU. I am deeply grateful to my parents, Nilma and Adenilson, who have been my pillar and have always incentivised me to pursue my dreams. Special thanks to my boyfriend, Matthew, for his love, laughter, and endless support, and to my dear friends—Elin, Federica, Veerle, Kincso and Raeshma—whose encouragement made this journey lighter.

I dedicate this thesis to my great-grandmother, Maria do Carmo Lima Santos, who passed away in February. I never imagined I would leave for Vienna and not see her again. Her strength and love continue to inspire me.

CEU eTD Collection

TABLE OF CONTENTS

Introduction 1

Chapter 1: Literature Review 4

1.1. Concepts of Power and Sovereignty in International Relations 4

1.2. Realism, Liberalism, and Constructivism in the Age of Big Tech 5

1.3. Big Tech's Role in Modern Warfare 7

1.4. Strategic Dependencies and the Erosion of Sovereignty 9

Chapter 2: Theoretical Framework & Methodology 12

2.1. Realism and Neorealism: The Enduring State-Centric Paradigm 12

2.2. Liberal Approaches: Cooperation and Interdependence 13

2.3. Constructivism: Socially Constructed Power and Technology 15

2.4. Methodology 16

Chapter 3: Constructivist Readings of Big Tech's Role in War 17

3.1. Microsoft 18

3.2. Google 20

3.3. Starlink (SpaceX) 21

Chapter 4: Big Tech's Challenge to the Nation-State 25

4.2.1. Starlink (SpaceX) 27

4.2.2. Microsoft & Google 28

Conclusion 31

Bibliography 33

CEU eTD Collection

CEU eTD Collection

LIST OF ABBREVIATIONS

AI — Artificial Intelligence

Big Tech — Technology Giants

C2ISR — Command, Control, Intelligence, Surveillance, and Reconnaissance

DoD — Department of Defense

EU — European Union

GCAT — Google Cybersecurity Action Team

GDP — Gross Domestic Product

Google — Google LLC (subsidiary of Alphabet Inc.)

ICRC — International Committee of the Red Cross

ICT— Information and Communication Technology

IPOs — Initial Public Offering

IR — International Relations

Microsoft — Microsoft Corporation

NGOs — Non-Governmental Organisations

Starlink — Satellite internet constellation operated by SpaceX

SpaceX — Space Exploration Technologies Corp.

SOS — Save Our Souls (emergency alert)

RT — Russia Today (Russian state media outlet)

TAG — Threat Analysis Group

UN — United Nations

UNICEF — United Nations International Children's Emergency Fund

U.S. – United States

CEU eTD Collection

INTRODUCTION

The growing influence of technology giants (commonly referred to as "Big Tech") in warfare suggests an underlying transformation in global power structures may be in progress. These corporations wield extraordinary societal reach, with platforms that permeate nearly every dimension of modern life, a tendency particularly evident in their expanding partnerships with states to provide essential and security services (George, 2023). Private sector involvement in warfare is not unprecedented—private military firms have been pivotal to post-Cold War conflicts, allowing governments to outsource military operations while bypassing democratic oversight (Saner et al., 2019). However, the current integration of tech firms into the machinery of modern conflict represents a novel and more systemic transformation.

This thesis explores these developments through via an interrogation of its central research question: *how are private technology companies reshaping war?* Two specific sub-questions guide the inquiry: (1) To what extent does Big Tech shape wartime political identities and meanings in the Ukraine conflict? (2) How do technology firms reshape traditional state functions and alter the contours of the international order? Focusing on the Ukraine war as a case study, this thesis analyses how Big Tech firms based in the United States— more specifically Google, Microsoft, and SpaceX (Starlink)— are not only supporting military operations but actively shaping geopolitical outcomes. Their expanding role in cyber defence, communications, and satellite intelligence during the conflict positions them as decisive actors and reflects a broader transformation in global power in power dynamics between states and non-state actors.

"Big Tech" refers to technological multinational corporations based in the United States (U.S.). These companies "are the defining institutions of our day, dominating our political economies,

CEU eTD Collection

societies, and polities as Big Oil or Big Banks did in their time" (Birch & Bronson, p. 1). A particularly important development has been the growing collaboration between the Pentagon and executives from major tech firms such as Google, Microsoft, and Starlink, reflecting a concerted effort to integrate AI and data-driven technologies into the Department of Defense (DoD). The partnership integrates Silicon Valley's "best practices" (Suchman, 2022) into the operations of the DoD.

This research situates Big Tech as both products and actors of structural change. As Kirshner (2013) contends, power transitions are increasingly shaped by factors like technological advancement and global interconnectedness. In the case of the Ukraine war specifically, the aforementioned companies have played central roles in military communications, cybersecurity, and infrastructure continuity. Their participation indicates a growing asymmetry: states are now increasingly dependent on private infrastructure that they do not control.

The theoretical framework deployed here combines elements of the major traditional theories of realism, neorealism, liberalism and constructivism to address this complex case. On top of this, Gilpin's (1981) theory of systemic change helps to understand the shifts of power driven by technological and economic forces. Nye's (2011) perspective on asymmetrical interdependence, non-state actors, and soft power, meanwhile, is utilised to explain these companies' influence. Lastly, Wendt (1999) usefully emphasises the social and ideational structures that give meaning to material resources, making technologies politically significant only within particular normative and institutional contexts.

Whilst the war in Ukraine is the immediate context for this analysis, the implications are global. The role of tech firms in shaping conflict, diplomacy, and international order requires us to reassess longstanding assumptions in International Relations (IR). Although scholars have

CEU eTD Collection

studied the political impact of multinational corporations since the 1970s (Uhlin, 1988), the integration of Big Tech into state functions and conflict dynamics remains underexplored, particularly by scholars within classical and constructivist theoretical paradigms. This thesis seeks to bridge that gap by examining how corporate technological advancements are reshaping sovereignty, power, and the international system itself. This thesis will show that (1) Big Tech firms are increasingly performing state-like roles in war, asserting authority over digital infrastructure, information flows, and security functions, and; (2) tech firms like SpaceX, Microsoft, and Google are reshaping the practice of sovereignty through their influence over warfare, infrastructure and public debate, giving rise to a need to rethink the concept.

The structure of the thesis is as follows: Chapter One introduces the key concepts and scholarly debates that frame this research. Chapter Two develops the theoretical framework and explains its relevance to the case study. Chapters Three and Four each address one of the sub-questions in detail, providing empirical analysis and theoretical interpretation drawn from the case-study of the Ukraine conflict. The thesis concludes with a final chapter that draws together the findings and reflects on their broader implications.

CEU eTD Collection

CHAPTER 1: LITERATURE REVIEW

This literature review situates the growing role of Big Tech in international security, state sovereignty, and warfare. It demonstrates the growing importance of tech companies in warfare and the implications of their partnership with governments for the international order. The section engages with a multidisciplinary scholarship, defines key concepts like power and sovereignty, and contextualizes Big Tech's rise and transformative impact."

1.1. Concepts of Power and Sovereignty in International Relations

Power is central to International Relations (IR), yet scholars have long debated its meaning. As Drezner (2020) notes, there is no single, agreed-upon definition. Barnett and Duvall (2005, p. 41), in one of the most cited articles on this topic, argue that "power works in various forms and has various expressions that cannot be captured by a single formulation cannot capture." Gilpin (1981) similarly finds power one of the most troublesome concepts in IR, and Guzzini (2000) calls it under-researched.

Attempts to clarify this complexity have produced a range of definitions and typologies. Nye, for instance, distinguishes between hard power and soft power (2004), smart power (2009), and sharp power (2018), while Wendt (1999, p. 8) highlights that power includes "the power to engage in organised violence". This idea ties power to sovereignty in a direct way: control over coercion and the ability to defend or assert territorial authority.

Sovereignty, meanwhile, is traditionally linked to the Peace of Westphalia (1648), marking a watershed moment in the rise of modern states with fixed borders and exclusive authority (Berg & Kuusk, 2010). Bull (1977) describes this as the emergence of an "international society,"

CEU eTD Collection

where states became the primary units endowed with legal and coercive power, emphasizing that no external authority governs a state without its consent.

Mainstream IR theories, particularly the English School, treat the sovereign state as the foundational actor in world politics, emphasising mutual recognition and shared legal identity (Bain, 2003; Biersteker & Weber, 1996). However, competing schools of thought define sovereignty differently. To Liberals, sovereignty refers to the state's capacity to regulate activities across borders amid globalisation, while Realists define it sovereignty by a state's ability to make ultimate decisions, especially in war (Thomson, 1995).

Yet the central debate today is not on sovereignty's definition, but its status: is sovereignty eroding? Liberal interdependence theorists (Cooper, 1972; Keohane & Nye, 1972, 1978; Rosecrance, 1986) argue that globalisation, technology, and non-state actors weaken sovereignty. Critics like Waltz (1979) and Gilpin (1987) disagree, saying sovereignty remains rooted in political will and coercive power, echoing realist views. Gilpin (1987) draws historical parallels, noting that political power—not innovation—sustained the Roman Empire's dominance. This last view has been strengthened after Covid-19 and the burgeoning U.S.-China rivalry.

1.2. Realism, Liberalism, and Constructivism in the Age of Big Tech

As this is a war case, the most logical theoretical perspective to adopt is Realism, focusing on power, conflict, and state behaviour. However, as global companies, civil society, and globalisation are involved, Liberalism is also applied, as it addresses these dynamics. Constructivism, in turn, offers a useful middle ground, focusing on identities, norms, and ideas

CEU eTD Collection

shaping behaviours. Together, these three theoretical lenses offer a more comprehensive framework.

Realists like Morgenthau (1948) and Edward Carr (1939) see States as rational political units in an anarchic system where power, especially military capacity, determines position. In this view, analyses of International Politics should focus on the dimension of State power, that is, on the military and material capacity that each State has.

Neorealism, particularly in the work of Kenneth Waltz (1979), further develops this idea by framing the international order as a structure defined by the distribution of power. Mearsheimer's offensive realism (1994) argues that states seek power maximisation. Yet, these theories overlook powerful non-state actors like tech firms (Leese & Hoijtink, 2019).

In contrast, Liberalism believes cooperation is possible even under anarchy. Thinkers like Nye and Keohane (1978) emphasise the roles of institutions, economic interdependence, and democracy. Technology is often perceived as a force for integration and transparency (Fukuyama, 1992; Castells, 2000). Keohane and Nye (1978) argue that power is multidimensional, and that interdependence creates both vulnerabilities and opportunities.

These concepts challenge the realist notion of power as purely military and suggest that actors who control structural dynamics, such as financial systems, trade networks, or communication infrastructure, hold significant influence. Keohane and Nye (1978) also emphasise the complexity of modern international politics. Non-state actors, alliances, and domestic-transnational linkages have blurred the lines between domestic and foreign policy, creating new governance challenges.

Constructivism, meanwhile, challenges both realism and liberalism, particularly after the Cold War's end—an event that schools failed to predict or explain. The fall of the Soviet Union

CEU eTD Collection

demonstrated that international politics could change not only through shifts in power distribution but also through transformations in ideas, identities, and norms (Wendt, 1992).

At its core, constructivism contends that the international system is not a fixed, objective structure, but a socially constructed realm shaped by the intersubjective meanings actors attach to it (Adler, 1999). Wendt (1987, 1999) highlights the mutual constitution of agents and structures. Constructivist scholars reconceptualise power to include symbolic, discursive, and normative dimensions.

Guzzini (2000) emphasises identity formation as central to international politics, as actors define themselves—and their interests—through shared meanings and social interaction. Norms and narratives play a key role in this identity construction. In this sense, constructivism is well-suited for analysing the rise of Big Tech firms. It helps explain not only how these firms act, but also how they define and legitimise their roles within the international system. Companies like Google, Microsoft, and SpaceX do not merely participate in geopolitics—they redefine themselves in the process, assuming quasi-state functions such as infrastructure provision, cybersecurity, and arbiters of the truth (Tréguer, 2019).

While each tradition offers valuable perspectives, none fully explains the rise of powerful tech firms. Their core assumptions are challenged by blurred lines between public and private authority, inviting a rethinking of international power and these companies' roles.

CEU eTD Collection

1.3. Big Tech's Role in Modern Warfare

The Ukraine war exemplifies how private technology firms shape warfare and redefine their identities. Described as a 'battlefield laboratory,' the conflict has seen companies play key roles alongside states, donating, supplying infrastructure, and delivering humanitarian aid (Chabert, 2023; Economist, 2023). Matania and Sommer (2023) describe the war in Ukraine as the first

major conventional land conflict in years involving broad international engagement, where the cyber domain—including social media, cloud services, search engines, and internet access—has become central to the war effort, especially due to the influential role of the companies that control these digital spaces.

This growing influence of these companies in warfare is the result of a historical process where states and corporations compete and collaborate over the control of communication infrastructure. In 1831, French entrepreneur Alexandre Ferrier proposed the first private optical telegraph between Calais and London, prompting state pushback over fears of losing information control (Flichy, 2009; Tréguer, 2019). Though initially rejected, the telegraph's rapid expansion by private actors set the precedent for the corporatisation of communication. By the late 19th century, firms operated global networks serving state and market interests (Beniger, 1986; Headrick, 2012). Today, neoliberal reforms have dismantled telecom monopolies, but the state-private dynamic persists—now recalibrated by Big Tech's unparalleled algorithmic, data, and infrastructural power (Galloway, 2004; Fuchs & Trottier, 2015).

As Scott (1998) observed, states increasingly depend on corporate data-processing systems to govern societies. Firms like Google, Microsoft, and Starlink have become virtually sovereign infrastructure providers, blurring public-private power lines (Leclercq-Vandelannoitte & Bertin, 2024). Big Tech firms are in fact increasingly redefining themselves as more than private companies, positioning themselves as key actors in global security and diplomacy (Leclercq-Vandelannoitte & Bertin, 2024).

A milestone was Denmark appointing a tech ambassador in 2017 to liaise with firms like Google, Facebook, Apple, and Microsoft (Hewitt, 2019; Sandbu, 2019). As the Danish Ministry of Foreign Affairs explained, these companies had grown so powerful that their economic

CEU eTD Collection

influence and societal reach surpassed that of many nation-states with which Denmark maintains traditional diplomatic relations (Ministry of Foreign Affairs of Denmark, 2017). This move formalised a new diplomatic category—what Sandre (2017) called "techplomacy"—reflecting the recognition of private corporations as legitimate and necessary interlocutors in international affairs.

Eric Schmidt's (2023) assertion that "war is the midwife of innovation" captures Big Tech's eagerness to redefine its role in global affairs. Through the development and deployment of dual-use technologies like facial recognition, these firms are increasingly embedded in state surveillance and security infrastructures (Coveri et al., 2024). In the Ukraine war, this shift became particularly visible: Starlink provided rapid battlefield communication and civilian internet access, aiding in infrastructure resilience (Bojor et al., 2024; Jayanti, 2023); Microsoft, now actively engaged at the UN level, pledged $100 million—surpassing the contributions of several states (Matania & Sommer, 2023; Kiel Institute, 2023); and Google not only contributed $55 million but also took a central role in combating disinformation (Kyiv Post, 2022). Such moves clearly demonstrate Big Tech's strategic repositioning.

1.4. Strategic Dependencies and the Erosion of Sovereignty

In relation to modern warfare, Kaldor (2007) argues that "new wars are 'globalised wars'" (p.154), which entail a "fragmentation and decentralisation of the state" (p.155). This aligns with Abels (2024) highlights about modern states' strategic vulnerability to Big Tech. Starlink's service limitation during Ukraine's 2023 counteroffensive, coinciding with Elon Musk's Russia-favourable peace plan, revealed tech firms' impact on military operations. Microsoft's suspension of Azure in Russia caused disruptions, showing corporate decisions affect military strategies without direct government control.

CEU eTD Collection

This dynamic is further intensified by the U.S.-China tech rivalry, where economic power translates into geopolitical influence (Coveri et al., 2024). The scale of corporate dominance is striking—U.S. tech giants like Google, Amazon, and Apple together exceed the GDP of countries like Japan, while Alibaba and Tencent hold comparable weight in China (Jia et al., 2018; Li & Qi, 2022). Their influence stems from control over key technologies, particularly AI, where a few firms dominate global patent ownership (Fanti et al., 2022; Calvino et al., 2023).

The blurring boundaries between corporate and state power further compound this influence. The "revolving door" phenomenon has reached unprecedented levels, exemplified by Elon Musk's appointment to a key government position in Trump's second term (Wen, 2024) and the symbolic presence of tech CEOs—Bezos (Amazon), Zuckerberg (Meta), Cook (Apple), and Pichai (Google)—in prominent seats during Trump's inauguration at St. John's Church (Sherman & Halpert, 2025). These manifestations of proximity showcase how Big Tech influences political decision-making at the highest level, challenging traditional distinctions between public and private authority.

Platform technologies now underpin defence procurement, cyber operations, and battlefield communication (Coveri et al., 2024). Meanwhile, firms like Microsoft routinely share cyber threat intelligence with states, assuming quasi-intelligence roles. Others, like Palantir, directly shape intelligence architectures (Zammit, 2003). Rikap & Lundvall (2021) further argue that Big Tech’s control over data, media ecosystems, and innovation pipelines grants them *de facto* sovereignty over critical domains, reinforced by their roles in AI, surveillance, and cloud computing (Ietto-Gillies, 2021). By providing essential infrastructure, these companies gain strategic leverage to influence political outcomes and warfare results.

CEU eTD Collection

The deepening state dependence on digital platforms is significant, as tech firms steer innovation by controlling knowledge flows within flexible, layered ecosystems, benefiting from decentralised innovation while maintaining technological dominance (Coveri et al., 2024; Gawer, 2022; Jacobides et al., 2024). Governments' weakened capacity to regulate cyberspace allows these firms near-unchecked control over cloud services, algorithm governance, and social media moderation. Moreover, Big Tech's aggressive corporate strategies—acquisitions, IPOs, and service diversification—have created integrated digital ecosystems that increasingly resemble state functions. Google, for example, offers a suite of interconnected services spanning search, communication, finance, and geolocation, fostering systemic dependency from local to global governance levels (Matania & Sommer, 2023). Despite regulatory efforts, such as in the European Union, these firms operate with considerable autonomy, often bypassing territorial constraints due to minimal physical infrastructure requirements (Politou et al., 2018; Hartman, 2007). This extraterritorial reach reshapes power balances between states and global tech actors (Matania & Sommer, 2023).

Drawing from the debates presented, this literature review emphasises the evolving nature of power and sovereignty in IR, highlighting how Big Tech firms are redefining traditional state roles and challenging classical IR assumptions. Liberalism and Constructivism offer useful lens to analyse this phenomenon, yet no single theory fully explains the growing influence of Big Tech firms in international affairs. The Ukraine war exemplifies how private tech companies have become key actors in warfare, providing critical infrastructure, funding, and technological innovation. The involvement of firms like Starlink, Microsoft, and Google signals a significant shift in global politics, blurring the boundaries between public and private spheres, while strategic dependencies deepen, and traditional notions of state sovereignty face potential erosion

CEU eTD Collection

CHAPTER 2: THEORETICAL FRAMEWORK & METHODOLOGY

This chapter applies the previous theoretical framework to the specific case of the Ukraine war, and the role of tech firms in modern warfare therein. The research question — *How are private technology companies reshaping war?* — requires moving beyond traditional state-centric models of international relations. Adopting a pragmatic, eclectic approach, the chapter draws on canonical authors from Realism, Neorealism, Liberalism and Constructivism. This allows for a more comprehensive understanding of the growing power of private actors, such as SpaceX, Microsoft, and Google, whose involvement in the war in Ukraine reveals how strategic capabilities are no longer exclusive to states. The chapter argues that traditional IR theories each offer valuable but incomplete insights into the evolving role of Big Tech firms in global politics and warfare and contends that understanding the geopolitical rise of these firms requires integrating perspectives on material power, interdependence, and socially constructed identities.

It is organised into the following sections: Realism and Neorealism; Liberal Approaches; Constructivism, followed by a brief methodology outline.

CEU eTD Collection

2.1. Realism and Neorealism: The Enduring State-Centric Paradigm

Applied to the Ukraine war, realism can partially explain why states rely on Big Tech firms like Microsoft, Google, and Starlink: they provide strategic assets (cyber defence, communications, intelligence) that enhance state capabilities in pursuit of security. However, realism fails to fully account for the extent to which these corporations are not just tools of state power but actors with geopolitical interests, shaping war outcomes and setting norms. For both, Kenneth Waltz

(1979) John Mearsheimer (1994), power is conceived largely in material terms—military strength and economic resources—while technology is seen as an external variable that modifies the balance of power but does not fundamentally alter the logic of the system (Leese & Hoijtink, 2019). In this lens, the power that Google, Microsoft and Starlink hold would be underestimated. As Buzan (1987) observed, realism rarely treats technology—or its corporate stewards—as independently transformative. Yet in the Ukraine war, Big Tech is not merely altering the balance of power; it is tangling the relationship between state and non-state actors, challenging realism's assumption that states are the sole relevant actors in global politics, as it demonstrates these companies current possess capabilities that rival or even surpass those of states. To address these gaps, liberal theories offer an alternative lens by emphasising interdependence, cooperation, and the political role of non-state actors.

2.2. Liberal Approaches: Cooperation and Interdependence

Liberal IR theories, while maintaining many rationalist assumptions, emphasise the possibility of cooperation under anarchy, facilitated by international institutions, economic interdependence, and the spread of democratic norms. Within this tradition, technology is framed as a driver of integration and transparency, potentially reducing the risks of conflict (Leese & Hoijtink, 2019). Fukuyama (1992), for instance, argued that technological advancement may encourage cooperation by equalising power disparities or creating shared vulnerabilities. Castells (2000) takes this further by suggesting that global power is increasingly structured through networks and information flows, where influence lies in control over data and communication infrastructures, not just territorial sovereignty. This framework helps explain how companies like SpaceX, Microsoft, and Google—by providing critical infrastructure, cybersecurity, and informational dominance—have emerged as influential actors.

CEU eTD Collection

This perspective aligns with Keohane and Nye's (1978) theory of complex interdependence, which challenges the realist focus on military power by emphasising the political significance of economic and technological ties. First, the politicisation of economic actions, such as platform restrictions or service withdrawal, illustrates how commercial decisions can function as foreign policy (Keohane & Nye, 1978, p. 158). Second, linkage strategies show how actors use interdependence as leverage, exemplified by Starlink's proposal of a peace plan (p. 160). Third, asymmetrical interdependence explains how less vulnerable actors—like Microsoft or Google—can exert disproportionate influence; without their defence against Russian cyberattacks, Ukraine might have suffered significant territorial losses – a very tangible result. Finally, their distinction between sensitivity (short-term disruption) and vulnerability (long-term dependence) is crucial for understanding states' growing reliance on corporate infrastructure (p. 160).

These insights help explain how private firms like Google, Microsoft, and SpaceX influence war not simply by providing digital infrastructure, but through their **g**atekeeping power. Their tools and platforms are embedded in state security, civilian resilience, and international legitimacy. For example, Google's suspension of services in Russia or its protection of Ukrainian websites against Distributed Denial-of-Service (DDoS) attacks are not just technical decisions—they shape political realities and affect the conduct and outcome of war.

At the same time, liberal approaches tend to assume that institutions and actors respond predictably to incentives. They often overlook how norms, identities, and symbolic capital shape global influence. While they provide a framework for understanding the structural conditions that enable tech firms to act, they fall short of explaining how these firms legitimate their authority, craft narratives, or embed themselves in moral discourses of war. These dimensions are better captured by constructivist approaches.

CEU eTD Collection

2.3. Constructivism: Socially Constructed Power and Technology

This thesis applies constructivism to understand how Big Tech companies not only participate in global politics but actively redefine their own identities in relation to it. Firms like Microsoft and Google do not merely respond to external expectations—they perform roles typically assigned to states, such as providing cybersecurity, managing digital infrastructure during wartime, and framing political narratives. Through public statements, diplomatic presence, and crisis response, these corporations are modifying their identities to become central geopolitical actors, invoking norms of sovereignty, responsibility, and humanitarianism.

Constructivism also reinterprets the role of technology. Rather than treating it as a neutral tool or exogenous force, constructivist scholars argue that technology's meaning and effects depend on the social context in which it is embedded. As Wendt (1995) asserts, material capabilities only matter insofar as they are interpreted through shared knowledge and expectations. A satellite system or cybersecurity tool, for instance, can be seen as a commercial product, a humanitarian lifeline, or a strategic weapon—depending on how relevant actors frame and understand it.

This interpretive flexibility makes constructivism especially well-suited for analysing the geopolitical rise of Big Tech. Leese and Hoijtink (2019) point out that the growing entanglement of commercial technologies in warfare defies traditional notions of sovereignty and state monopoly over strategic assets. Constructivism enables us to interrogate not only what these technologies do, but how they become legitimate tools of governance, and how tech firms legitimise themselves as state-like actors through discourse, behaviour, and institutional adaptation. Nevertheless, despite it strengthens, constructivism fails to adequately account for the behaviour of states of the important impacts of globalisation on the international political arena.

CEU eTD Collection

In summary, Realism, Liberalism, and Constructivism each illuminate distinct aspects of Big Tech's influence in global politics. While Realism highlights material power, it tends to underplay the central role technology now plays in warfare and geopolitics, especially as tech firms deliver strategic services critical for states to function and engage in conflict. Liberalism, meanwhile, exposes the role of interdependence and economic leverage, which helps to understand how these companies acquired so much relevance and have become key actors in international politics. Constructivism reveals the importance of identity and discourse in shaping Big Tech's geopolitical roles. Companies like Starlink, Microsoft, and Google have moved beyond profit-driven multinational corporations to assume roles that influence global politics. The next chapter will explore these themes further through key episodes involving these firms.

2.4. Methodology

This thesis's methods employ a case analysis focusing on the actions of selected American Big Tech companies in the Ukraine war, following Russia's full invasion on 24 February 2022. The study adopts a qualitative triangulation approach, including a comprehensive review of academic literature, official reports, policy documents, and journalistic investigations. Primary data sources include government publications, think tank reports, and reputable academic databases such as Google Scholar and Connected Papers. This qualitative approach enables a layered understanding of how Big Tech actors interact with state structures and the international system, particularly in the context of the Ukraine war.

CEU eTD Collection

CHAPTER 3: CONSTRUCTIVIST READINGS OF BIG TECH'S ROLE IN WAR

This chapter explores how Big Tech firms like Microsoft, Google, and SpaceX have become central actors in the social construction of war, political identity, and legitimacy during the Ukraine conflict. It addresses the sub-question: *To what extent does Big Tech shape wartime political identities and meanings in the Ukraine conflict?*

Drawing on Wendt's (1995) social constructivism, this chapter investigates how Big Tech actions in Ukraine not only reflect but also shape political identities and meanings. Wendt posits that "material resources only acquire meaning for human action through the structure of shared knowledge in which they are embedded" (p. 73), and that actors respond to objects and other actors based on the meanings those entities hold. For example, American military power means something different to Canada than to Cuba; similarly, Big Tech's involvement in Ukraine carries distinct symbolic and strategic meanings for different actors.

In the context of the war, digital infrastructure such as Starlink terminals and Azure cloud services takes on meanings beyond their technical function. For Ukraine, Microsoft's cybersecurity support strengthened its identity as a "digital frontliner." Conversely, Google's restrictions on Russian state media contributed to Russia's construction of itself as a "sanctioned adversary." SpaceX's provision of Starlink has been interpreted as a symbol of Ukrainian resilience by Kyiv, while being framed as subversive interference by Moscow.

Wendt's idea that "anarchy is what states make of it" (1992) is adapted here to the corporate domain. Tech firms are not merely economic actors but participants in the identity-making and meaning-construction processes of international politics. Their role identities, such as Microsoft

CEU eTD Collection

casting itself as a "guardian of cyberspace" or Google as an "arbiter of truth," are relational and performative, emerging through ongoing interactions with states and publics.

By tracing how Microsoft, Google, and SpaceX frame their actions, and how those actions are interpreted by states and publics, this chapter argues that Big Tech is not merely acting in war, but redefining their identities, moving beyond traditional corporate roles. This chapter is structured as follows: first, it analyses Microsoft's case building legitimacy through cybersecurity and diplomacy. Second, it showcases Google's example, positing itself as a content regulator, influencing the war narrative, and as a key actor for humanitarian and infrastructure efforts. Lastly, it investigates Starlink's involvement in providing crucial support to Ukraine.

3.1. Microsoft

Microsoft exemplifies the transformation of Big Tech from a conventional multinational to a geopolitical actor. In 2020, it established formal offices at the United Nations in New York and Geneva, appointing a UN affairs team and head to engage with multilateral diplomacy (Matania & Sommer, 2023). This institutionalisation marks a diplomatic posture typically reserved for sovereign states rather than private enterprises.

At the 75th UN General Assembly, Microsoft declared its commitment to addressing global challenges, including democracy, human rights, economic development, education, broadband access, environmental sustainability, and the digital empowerment of the UN (Microsoft, 2020). This alignment with international organisations signals Microsoft's pursuit not only of influence but also to seek recognition as a global political actor.

During the war in Ukraine, Microsoft deepened this transformation by assuming a state-like role both materially and symbolically. The company condemned Russian aggression, advocated

CEU eTD Collection

for Ukraine's sovereignty, and publicised its cyber defence and humanitarian contributions (Smith, 2022). It provided critical threat intelligence, helped repel cyberattacks, and fortified Ukrainian digital infrastructure in coordination with organisations such as the ICRC and UN agencies (Matania & Sommer, 2023). These interventions signal Microsoft's shift from corporate vendor to geopolitical actor engaged in national-scale security and diplomacy.

A key example of this transformation was Microsoft's early cybersecurity assistance to Ukraine. The company played a decisive role in defending critical infrastructure—finance, energy, emergency services—against Russian cyberattacks. It was the first to detect the FoxBlade malware just before Russia's February 2022 invasion, promptly alerting Ukrainian authorities and providing mitigation tools (Matania & Sommer, 2023). Microsoft also maintained secure communication channels with the Ukrainian government, including regular contact between President Zelenskyy and Microsoft President Brad Smith.

In a June 2022 blog post, President Smith outlined five critical lessons from the early stages of the conflict, including the importance of cross-border digital infrastructure, modern cybersecurity tools, and coordinated international responses to Russian cyber campaigns. Notably, this type of strategic assessment—traditionally the domain of national defence agencies—was now being delivered by a private tech company. Despite reaffirming that Microsoft is a private corporation and not a government, Smith has often adopted rhetoric more typical of state leaders. For instance, he has underscored the company's global responsibility to help defend nations against cyberattacks and called on other tech firms, governments, academia, and civil society to join in a coordinated response (Matania & Sommer, 2023; Smith, 2022). This language signals a performative identity in line with Wendt's theory—Microsoft positions itself not merely as a vendor but as a geopolitical actor with sovereign-like responsibilities.

CEU eTD Collection

Microsoft's actions toward Russia also resembled those of a geopolitical opponent rather than a neutral corporation. Following a series of Russian cyberattacks—some of which exploited Microsoft tools—the company suspended all product sales in Russia in March 2022, effectively aligning itself with broader international sanctions (Smith, 2022).

3.2. Google

Google's involvement in the Ukraine conflict similarly transcended traditional commercial roles. By May 2022, it had committed over $55 million in humanitarian and informational support to Ukraine (Kyiv Post, 2022). This included $35 million for humanitarian aid, funded through employee donations and grants, and $20 million directed at countering misinformation and assisting refugees, with $10 million focused on Poland's refugee efforts. This scale of aid placed Google alongside state donors such as Austria, Luxembourg, and Switzerland, but also highlighted the unprecedented level of involvement by a private corporation in a major international conflict.

Google's Threat Analysis Group (TAG) has helped expose and block Russian cyber campaigns, asserting a normative stance in the information war. Its YouTube platform demonetised and delisted Russian state media, removing more than 8,000 channels and 60,000 videos for violating policies, such as spreading misinformation, promoting hate speech, or showing graphic violence related to the war. These actions demonstrate a clear political stance, beyond mere commercial interest (Matania & Sommer, 2023). Through such actions, Google becomes more than a company providing service: it performs a role in curating political realities and regulating public knowledge, therefore, shaping war narratives, like a state would do. Additionally, the firm also restricted the visibility of Russian-backed outlets in Search, removed RT and Sputnik apps from Google Play in Europe, and ensured their content was excluded from Search results in line with EU regulations (Walker, 2022).

CEU eTD Collection

Their digital support to Ukraine was also outstanding and essential. Google disabled live traffic features on Google Maps to protect civilian movements and adapted its earthquake warning technology to deliver Android-based air raid alerts (Culliford, 2022). They launched SOS alerts, highlighted refugee-aid services on Search and Maps, and partnered closely with the Ukrainian government to disseminate reliable safety information (Matania & Sommer, 2023). As Google expanded access to services such as Google Translate, Fi, and Cloud, it demonstrated its unparalleled ability to deliver large-scale digital humanitarian assistance. These actions positioned Google as a humanitarian infrastructure provider—a role traditionally fulfilled by international agencies or states—thereby reinforcing its emerging state-like functions in crisis governance.

Finally, Google has also played a defensive role in the cyber domain. It blocked phishing campaigns by Russian-linked groups like Fancy Bear, Ghostwriter, and Mustang Panda, alerted Ukrainian Gmail users, and protected over 200 government and civil society websites through Project Shield. Its Advanced Protection Program further secured high-risk users. The scale and precision of these efforts rival those of national cybersecurity agencies (Matania & Sommer, 2023).

3.3. Starlink (SpaceX)

SpaceX completes this triad of Big Tech firms assuming geopolitical roles, particularly through its Starlink satellite internet system. Starlink's role in maintaining Ukraine's internet connectivity, especially in war zones, rendered it both a symbolic and strategic asset. Its deployment was framed by Ukrainian officials as a lifeline for sovereignty and communication. Starlink's role in the Ukraine conflict was initiated shortly before Russia launched its full-scale invasion on February 24, 2022. At that time, a Russian cyberattack had disrupted Viasat systems, severely affecting Ukraine’s communications infrastructure (Isaacson, 2023). In

CEU eTD Collection

response, Ukrainian Deputy Prime Minister Mykhailo Fedorov publicly reached out to Elon Musk on Twitter, which led to the rapid shipment of 500 Starlink terminals within 48 hours (Isaacson, 2023).

Over the course of 2022, Starlink proved essential for maintaining communications on the front lines, supporting civilian access to the internet, and aiding in the restoration of damaged infrastructure. By May, it was reported that more than 150,000 users were relying on the system each day (Bojor et al., 2024; Jayanti, 2023). Starlink sustained vital connectivity for Ukrainian troops at moments when traditional telecommunications networks had collapsed (Trofimov et al, 2022). In addition, comprehensive kits—including field-ready solar panels and batteries—were supplied to ensure uninterrupted service (Isaacson, 2023). Ukraine's Minister Mykhailo Fedorov described Starlink as "crucial support for Ukraine's infrastructure and the restoration of destroyed territories" (Jayanti, 2023). Starlink's terminals enabled:

1. **Command, Control, Intelligence, Surveillance, and Reconnaissance (C2ISR):** Starlink provided vital satellite communication for Ukrainian forces, notably enabling trapped troops in Mariupol's Azovstal plant to share live updates, boosting morale (Schwirtz, 2022).

2. **Civilian Communication & Emergency Support:** Starlink restored civilian communication in war-affected regions, enabling emergency services and timely alerts that enhanced survival and coordination (Dalmia & Mittal, 2024).

3. **Support for Drone Warfare:** It enabled real-time drone operations, including missions that destroyed major Russian assets like the Moskva and Ivanovets (Sutton, 2022; Romaniuk, 2022).

CEU eTD Collection

4. **Propaganda and Strategic Communication:** Starlink facilitated global dissemination of frontline footage, strengthening Ukrainian morale and international backing through strategic messaging (Bojor & Cârdei, 2023).

5. **Social Resilience & Family Connectivity:** By maintaining family contact, Starlink supported troop morale and emotional resilience (Kwok et al., 2016; Kostenko et al., 2024).

6. **National and International Mobilisation:** Starlink broadcasts of civil defiance inspired national unity and global solidarity with Ukraine, intensifying resistance narratives and pressure on Russia (Bojor & Cârdei, 2023).

Moreover, SpaceX's role extended beyond this already extensive technological provision. Its decision to geofence Starlink access—specifically restricting service in Crimea to avoid escalating tensions—reflects a strategic calculus more characteristic of statecraft than corporate policy. This call carried significant geopolitical implications, influencing battlefield communications and contributing to broader diplomatic negotiations. By managing a critical layer of military-relevant infrastructure and exercising strategic restraint, SpaceX demonstrates how private firms can influence conflict dynamics and assert quasi-sovereign authority in contested spaces.

This chapter has shown how Big Tech's engagement in the Ukraine war extends beyond logistical or commercial support; it is deeply enmeshed in the construction of new geopolitical identities, performing roles traditionally associated with states. Drawing on Wendt's constructivism, we see that these firms are embedded in structures of shared meaning and are helping to reshape them. By positioning themselves as protectors of cyberspace, curators of truth, and providers of critical infrastructure, they are asserting forms of symbolic and strategic authority that blur the boundary between corporate and sovereign state.

CEU eTD Collection

Traditional IR theories conceptualise the state through Weberian attributes: monopoly on legitimate violence, defined territory, bureaucratic organisation, and claim to sovereignty. While Big Tech lacks territorial claims or coercive force, it increasingly exercises functional sovereignty, controlling infrastructure, shaping public narratives, and influencing war outcomes. Google's information governance, Microsoft's cyber defence capabilities, and SpaceX's military-relevant infrastructure provision illustrate their growing power and reliance by states and societies. These firms operate beyond the jurisdiction of any single government, affecting almost every aspect of the Ukraine conflict, yet they continue to be inappropriately treated as merely peripheral actors in the mainstream IR literature. This chapter has shown that this needs to change.

CEU eTD Collection

CHAPTER 4: BIG TECH'S CHALLENGE TO THE NATION-STATE

This chapter demonstrates how tech firms not only affect war but challenge the very structures that have traditionally governed it. Building on the previous analysis of Big Tech's operational roles in the Ukraine conflict, this chapter examines how these firms are eroding the monopoly of the nation-state over key war-making and governance functions. Through control of strategic infrastructure, narrative framing, and cyber capabilities, firms like SpaceX, Microsoft, and Google have begun to operate as sovereign-like actors, exerting influence without state authority or democratic oversight. This phenomenon addresses the central research question by focusing on a second, broader sub-question: *How do technology firms reshape traditional state functions and alter the contours of the international order?* The chapter is structured around specific studies of SpaceX, Microsoft, and Google, examining how each firm exerts sovereign-like influence during the Ukraine war. Through these examples, the chapter unveils the evolving roles of tech oligarchies in shaping military operations, cyber defence, and information governance.

As mentioned in the last chapter, tech firms are not merely economic players but increasingly powerful geopolitical actors, wielding influence once reserved for states. As our analyses has showcased, their control over digital infrastructure, communication systems, and dual-use technologies enables them to shape global outcomes independently of formal state authority.

A notable example is SpaceX's restriction of Starlink service during Ukraine's 2023 counteroffensive. This decision, made by Elon Musk without governmental directive, directly affected battlefield operations and was motivated by his stated desire to avoid escalation with Russia (Abels, 2024). This episode highlights how private actors such as Musk, through Starlink, now possess the capacity to unilaterally alter the course of military conflict, without

CEU eTD Collection

democratic oversight or institutional accountability. Gilpin (1981) anticipated such disruptions, arguing that although states have historically been the dominant actors in international politics, their supremacy is neither fixed nor immune to challenge. As economic, technological, and political shifts occur, non-state actors can reshape the global order, especially when they command strategic capabilities traditionally associated with sovereign power. This evolving reality also reflects a shift in the nature of power itself.

Nye's (2011) concept of soft power helps interpret this shift. In contrast to hard power, which refers to tangible resources like military force, economic leverage, and population, soft power is the ability to influence others by shaping their preferences, norms, and desires. It rests on intangible resources: culture, ideologies, international institutions, and agenda-setting capacity. According to Nye, the most enduring and sustainable power is not coercive but persuasive: it makes others want what you want. In this light, Musk's actions—framing infrastructure decisions as moral or geopolitical necessities—represent a form of technical and narrative influence that reconfigures the diplomatic field without direct confrontation.

Meanwhile, realism, with its emphasis on state monopoly over force and strategic resources, struggles to account for such influence. Its focus on formal authority overlooks how control over communication systems or platforms can translate into strategic leverage. As Kirshner (2013) notes, in today's digital age, power increasingly flows from command over information systems—domains where corporations often surpass states. Kaldor's "new wars" thesis (2007) further frames such dynamics, highlighting how modern conflicts increasingly blur the lines between state and non-state actors, public and private sectors, and combatants and civilians. In Ukraine, this ambiguity is exemplified by Microsoft's $100 million aid package and its proactive cyber defence of critical infrastructure. Similarly, Google censored Russian disinformation and engaged in active attribution of cyber operations, assuming roles traditionally held by intelligence services.

CEU eTD Collection

These developments support Wendt's (1992, 1995) constructivist view that sovereignty itself is not fixed, but shaped through social meaning and mutual recognition. Tech firms increasingly assert *de facto* sovereign functions—not by formal claim, but through control over critical infrastructure, communications, and legitimacy. As Gu (2023) and Srivastava (2021) note, sovereignty is increasingly divided between state regulatory efforts and Big Tech's borderless governance frameworks. This reflects a deeper structural entanglement, as theorised by political economists like Keohane and Nye (1978). Their concept of *asymmetrical interdependence* is especially relevant: states are often more dependent on private tech infrastructures than these companies are on state policy. As Pang (2022) and Fuchs (2015) argue, this leads to fragmented sovereignty and oligarchic influence, where firms operate not just within states but above them, shaping rules, narratives, and outcomes.

As Drezner (2019) suggests, these firms are not simply lobbyists or interest groups but active rule-makers in domains ranging from cybersecurity to data governance. Their power lies not only in market dominance but in their ability to set standards, mediate conflicts, and shape global norms—functions once reserved for sovereign states.

4.2.1. Starlink (SpaceX)

As mentioned before, in September 2022, during a critical Ukrainian operation targeting Russian naval forces near Crimea, SpaceX abruptly shut down Starlink satellite service in the area. Elon Musk later admitted this was a deliberate action motivated by fears of provoking a Russian nuclear response. This unilateral move exemplifies how a private firm, originally created for civilian internet provision, gained the ability to influence military outcomes directly. At the same time, Musk finalised his acquisition of Twitter and entered discussions with U.S. and European allies regarding funding Starlink's military and civilian operations in Ukraine (The Guardian, 2023; Srivastava & Schwartz, 2023). Although Musk denied reports of direct

CEU eTD Collection

communication with President Putin on peace proposals, leaked accounts suggest he proposed referendums in contested territories and sought international recognition of Crimea as Russian territory—a controversial stance diverging sharply from official U.S. policies at that time (Pendleton, 2022; Isaacson, 2023).

Concurrently, Musk moved to disable Starlink coverage in Russian-controlled areas of southern and eastern Ukraine, reflecting a dual strategy that balanced engagement with Ukrainian forces and attempts to de-escalate broader conflict risks. This episode highlights two key points: first, the extraordinary influence wielded by a private company over the conduct of war; second, the deep military and political reliance on SpaceX's technologies, which may explain the relative accommodation of Musk's broader ambitions—including his Twitter acquisition—by U.S. authorities (Coveri et al., 2024).

4.2.2. Microsoft & Google

Microsoft has played a prominent role in Ukraine through both humanitarian and cyber defence support, going beyond traditional boundaries between corporate philanthropy and state diplomacy. The firm partnered with humanitarian organisations such as the ICRC, UN agencies, and local NGOs, providing technology and logistical support for aid efforts. Moreover, their Employee Giving Program also mobilised resources for organisations like UNICEF and Polish Humanitarian Action (Matania & Sommer, 2023).

In the cyber domain, Microsoft's Threat Intelligence Center was pivotal in detecting and neutralising WhisperGate malware deployed by Russian actors in January 2022 to disrupt Ukrainian government systems. Brad Smith (2022), Microsoft's former president, framed cyber defence as a "global responsibility," positioning the firm as a sovereign-like actor with an obligation to uphold digital security and resilience. This diplomatic language signals

CEU eTD Collection

Microsoft’s self-perception as a global stakeholder in security governance, wielding influence once reserved for states.

Likewise, Google’s involvement in the Ukraine conflict demonstrates how digital platforms are not only key players in information warfare but also increasingly perform governance functions traditionally associated with sovereign states and international organisations. While earlier analysis highlighted Google's role in content moderation and counter-disinformation, functions reminiscent of state intelligence services, its broader activities extend much further into humanitarian, institutional, and normative domains.

In addition to curbing Russian disinformation and publicly attributing cyber threats to state-sponsored actors, Google has launched comprehensive efforts to promote democratic resilience across Eastern Europe. These include initiatives that support civil society, such as the "Protect Your Democracy Toolkit"—a package of training, cybersecurity tools, and informational resources designed for NGOs, journalists, and political activists in frontline states like Poland, Czechia, Lithuania, and Latvia (Kroeber-Riel, 2022). These efforts mirror the roles traditionally filled by state-funded development agencies or international NGOs, effectively situating Google as a parallel provider of democratic infrastructure.

Google’s impact has not gone unnoticed. President Volodymyr Zelenskyy awarded the company the Peace Prize for its contributions to Ukraine’s defence and digital resilience. This symbolic recognition elevates Google’s status to that of a valued geopolitical ally. At the same time, the company’s Google Cybersecurity Action Team (GCAT) worked alongside national governments and critical infrastructure providers to modernise IT systems, defend cloud environments, and strengthen software supply chains—responsibilities normally handled by state cyber command units (Matania & Sommer, 2023).

CEU eTD Collection

Furthermore, Google is actively shaping the ideological contours of the international order. As Nye (2011) describes, *soft power* involves the ability to set agendas, shape preferences, and establish legitimacy without coercion. Google's public advocacy for democracy, as exemplified by Kent Walker's keynote at the Copenhagen Democracy Summit and the company's support for the U.S.-led Declaration for the Future of the Internet, exemplifies this normative power. By promoting a human rights-centred vision for digital governance, Google is not merely reacting to state policy but actively crafting it, positioning itself as a global steward of democratic values (Matania & Sommer, 2023).

These actions illustrate a complex ramification of sovereignty: on one hand, states seek to preserve territorial and regulatory control over digital space; on the other, companies like Google carve out transnational zones of influence grounded in technological infrastructure, ideological leadership, and institutional legitimacy (Gu, 2023; Srivastava, 2021). This dualism produces a fragmented global order where tech corporations increasingly resemble sovereign entities, armed not with soldiers or tariffs, but with platforms and discourses.

This chapter has shown how Big Tech firms, particularly SpaceX, Microsoft, and Google, are no longer peripheral actors in wartime politics. Through their infrastructural, informational, and normative interventions in the Ukraine conflict, these companies have come to perform state-like functions. Their influence on military strategy, cybersecurity, and public discourse not only shapes the conduct of war but also redefines the very contours of sovereignty, underscoring a fundamental shift in global power structures

CEU eTD Collection

CONCLUSION

This thesis has sought to provide a much-needed analysis of the role of Big Techs in transforming the architecture of contemporary international politics, challenging foundational assumptions of sovereignty and power in the field of International Relations (IR). Anchored in the central research question—*How are private technology companies affecting war?*—the analysis focused on the roles of Microsoft, Google, and SpaceX during the Ukraine conflict. It has argued that these firms are not peripheral actors but, in fact, central geopolitical agents, performing fundamentally sovereign-like functions, often with greater agility and influence than states.

Across the empirical chapters, we saw how these companies intervened directly in warfare and geopolitics through digital infrastructure, cyber defence, and information governance. These interventions reveal a shift in global power structures, whereby Big Tech firms exercise what can be described as *functional sovereignty*—operating critical infrastructure, shaping narratives, and influencing military outcomes without democratic oversight or institutional accountability. Their actions blur the lines between public and private, civilian and military, national and transnational, and challenge neo-realist theorists about the centrality of the state.

In other words, this thesis finds that Big Tech firms—particularly Microsoft, Google, and SpaceX—are increasingly performing roles traditionally reserved for sovereign states, especially in the context of the Ukraine war. These companies have exercised strategic influence over battlefield communications, cybersecurity, and information control, often operating with more speed and autonomy than state actors. Their interventions have had tangible geopolitical effects, such as SpaceX's geofencing decisions impacting military operations or Microsoft defending Ukraine's digital infrastructure. Through these actions, they

CEU eTD Collection

have assumed symbolic roles—Microsoft as a cyber defender, Google as a curator of truth, and Starlink as a critical lifeline—thereby constructing new identities in global politics. The thesis also shows that traditional IR theories like Realism and Neorealism fall short in explaining these dynamics, while Liberal and Constructivism perspectives offer more effective analytical tools. Ultimately, the research reveals that sovereignty is becoming increasingly fragmented and exercised through digital infrastructures, with power now shared—and contested—between states and corporate actors.

This study's implications are significant. For IR scholarship, it suggests the need to reconceptualise the discipline's fundamental ideas of sovereignty and power in light of modern digital politics. For practice, it highlights a regulatory and security dilemma: states are dependent on actors they cannot fully control, while these actors face few binding obligations. The Ukraine war is an ongoing and evolving case, and the findings presented here reflect a specific temporal and geopolitical context.

A key limitation of this study is its Western-centric focus. By concentrating on U.S.-based firms and a single conflict, it does not capture the full global diversity of global corporate-state dynamics. Future research should broaden this scope by examining how Chinese and Russian tech companies, such as Huawei, Tencent or Sber, navigate geopolitical conflicts and state alignment. Finally, while this thesis has focused on Big Tech's role in Ukraine, the dynamics identified here extend far beyond one conflict. Sovereignty increasingly operates through platforms, networks, and algorithms, rather than just borders and institutions, and IR theory must evolve accordingly. The next step is to explore how these shifts unfold in other regions, such as the Indo-Pacific, Africa, or Latin America, and how a multipolar digital order is emerging from the interplay of state and corporate power.

CEU eTD Collection

BIBLIOGRAPHY

Abels, J. (2024). Private infrastructure in geopolitical conflicts: The case of Starlink and the war in Ukraine. *European Journal of International Relations,* 30(4), 842-866.

Adler, E. (1999). Constructivism in world politics. *Lua Nova: Revista de Cultura e Política, (47),* 163–200.

Barnett M and Duvall R (2005) Power in international politics. *International Organization* 59(1): 39–75.

Bain, W. (2003). The political theory of trusteeship and the twilight of international equality. *International Relations*, 17(1), 59–77.

Beniger, James R. 1986. *The Control Revolution: Technological and Economic Origins of the Information Society*. Harvard University Press.

Berg, E., & Kuusk, E. (2010). What makes sovereignty a relative concept? Empirical approaches to international society. *Geopolitics, 15*(4), 700–715.

Biersteker, T., & Weber, C. (1996). The social construction of state sovereignty. In T. Biersteker, & C. Weber (Eds.), *State sovereignty as social construct* (pp. 1–21). Cambridge: Cambridge University Press, 167.

Birch, K., & Bronson, K. (2022). "Big tech." *Science as Culture*, 31(1), 1–14.

Bojor, L., Petrache, T., & Cristescu, C. (2024). The impact of Starlink in the Russia–Ukraine war. *Land Forces Academy Review*, *29*(2[114])

Bull, H. (1977). *The anarchical society: A study of order in world politics*. NY: Columbia University Press. p. 13.

Buzan B (1987) *An Introduction to Strategic Studies: Military Technology and International Relations*. Basingstoke/London: Macmillan Press.

CEU eTD Collection

Calvino, F., Criscuolo, C., Dernis, H., & Samek, L. (2023). What technologies are at the core of AI? An exploration based on patent data. *OECD Artificial Intelligence Papers*, No. 6. OECD Publishing.

Carr, E. H. (1939). *The twenty years' crisis 1919-1939: An introduction to the study of international relations*. London: Macmillan

Castells M (2000) *The Information Age: Economy, Society and Culture, Part 1: The Rise of the Network Society*. Malden/Oxford/Chichester: Wiley-Blackwell.

Chabert, V. (2023). The outer-space dimension of the Ukraine conflict. *Journal of International Affairs, 75*(2), 145–156.

Cooper, R. (1972) Economic Interdependence and Foreign Policy in the Seventies. *World Politics* 24:159-181.

Coveri, A., Cozza, C., & Guarascio, D. (2024). Blurring boundaries: An analysis of the digital platforms-military nexus. *Review of Political Economy*.

Culliford, E. (2022, February 28). *Google temporarily disables Google Maps live traffic data in Ukraine*. Reuters. https://www.reuters.com/technology/google-temporarily-disables-google-maps-live-traffic-data-ukraine-2022-02-28/

Dalmia, N., & Mittal, S. (2024, February 15). How is Starlink Ukraine's strategic tool in the face of Russian invasion. *The Economic Times*. Available at: https://economictimes.indiatimes.com/news/defence/how-is-starlink-ukraines-strategic-tool-in-the-face-of-russian- invasion/articleshow/107710900.cms.

Drezner, D. W. (2021). Power and international relations: A temporal view. *European Journal of International Relations, 27*(1), 29–52.

Drezner, D. W. 2019. Technological Change and International Relations. *International Relations* 33 (2): 286–303.

CEU eTD Collection

Economist (2023). *How Elon Musk's satellites have saved Ukraine and changed warfare.* Available at: www.economist.com/briefing/

Fanti, L., Guarascio, D., & Moggi, M. (2022). From Heron of Alexandria to Amazon's Alexa: A stylized history of AI and its impact on business models, organization and work. *Journal of Industrial and Business Economics*, 49(3), 409-440.

Flichy, P. (2009). *Dynamics of modern communication: The shaping and impact of new communication technologies*. SAGE.

Fuchs, C., & Trottier, D. (2015). Towards a theoretical model of social media surveillance in contemporary society. *Communications – European Journal of Communication Research, 40*(1), 113–135.

Fuchs, C. (2015). The digital labour theory of value and Karl Marx in the age of Facebook, YouTube, Twitter, and Weibo. In E. Fisher & C. Fuchs (Eds.), *Reconsidering value and labour in the digital age* (Dynamics of Virtual Work Series, pp. 26–41). Palgrave Macmillan.

Fukuyama, F. (1992). *The end of history and the last man*. Penguin Books.

Gawer, A. (2022). *Digital platforms and ecosystems: Remarks on the dominant organizational forms of the digital age. Innovation, 24*(1), 110–124.

Gilpin, R. (2002). *War and change in world politics*. Cambridge University Press. (Original work published 1981)

Gilpin, R. (1987) *The Political Economy of International Relations.* Princeton, NJ: Princeton University Press.

Guo, X., Chmutova, I., Kryvobok, K., Lozova, T., & Kramskyi, S. (2024). The race for global leadership and its risks for world instability: Technologies of controlling and mitigation. *Research Journal in Advanced Humanities, 5*(1).

CEU eTD Collection

Galloway, Alexander R. (2004). *Protocol: How Control Exists after Decentralization*. MIT Press.

George, A. S. (2023). *Silicon Valley rising: How Big Tech may eclipse nation-states*. *Partners Universal Innovative Research Publication* (PUIRP), *1*(1), 102.

Guzzini S (2000) The use and misuse of power analysis in international theory. In: Palan R (ed.), *Global Political Economy: Contemporary Theories*. London: Routledge.

Hartman, L. P., Rubin, R. S., & Dhanda, K. K. (2007). The communication of corporate social responsibility: United States and European Union multinational corporations. *Journal of Business Ethics*, *74*(4), 373–389.

Headrick, Daniel R. (2012). *The Invisible Weapon: Telecommunications and International Politics, 1851–1945*. Reprint. Oxford University Press, USA.

Hewitt, H. (2019, June 6). *To regulate 'Big Tech,' we need prudence, not politics. The Washington Post.* https://www.washingtonpost.com/opinions/2019/06/06/regulate-bigtech-we-need-prudence-not-politics/?noredirect=on&utm_term=.163aed8fbe74

Hymer, S. H. (1972). *The internationalization of capital. Journal of Economic Issues*, *6*(1), 91–111.

Ietto-Gillies, G. (2002). *Transnational corporations: Fragmentation amidst integration*. Routledge.

Isaacson, W. (2023, September 7). *'How am I in this war?': The untold story of Elon Musk's support for Ukraine*. The Washington Post. https://www.washingtonpost.com/technology/2023/09/07/elon-musk-ukraine-starlink-walter-isaacson/

Jacobides, M. G., Cennamo, C., & Gawer, A. (2024). Externalities and complementarities in platforms and ecosystems: From structural solutions to endogenous failures. *Research Policy*, *53*(1), 104906.

CEU eTD Collection

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

Jia, K., Kenney, M., & Zysman, J. (2018). Global competitors? Mapping the internationalization strategies of Chinese digital platform firms. In R. van Tulder, A. Verbeke, & L. Piscitello (Eds.), *International business in the information and digital age.* Emerald Publishing Ltd.

Kaldor, M. (2007). *New and old wars: Organized violence in a global era* (2nd ed.). Stanford University Press.

Keohane R and Nye J (1978) *Power and Interdependence*. Boston: Longman.

Keohane, R., and J. Nye, (1972) Transnational Relations and World Politics. Cambridge, MA: Harvard University Press.

Kiel Institute for the World Economy. (2023, September 7). *Ukraine support tracker – A database of military, financial and humanitarian aid to Ukraine*. https://www.ifw-kiel.de/topics/war-against-ukraine/ukraine-support-tracker/

Kirshner, J. (2013). *Globalization and national security*. Routledge.

Kostenko, A., et al. (2024). Resilience and vulnerability of Ukrainians: The role of family during the war. *Problems and Perspectives in Management, Vol. 22, Issue 1*, 432-445.

Kroeber-Riel, A. (2022, June 3). *Advancing security across Central and Eastern Europe*. The Keyword. https://blog.google/technology/safety-security/advancing-security-across-central-and-eastern-europe/

CEU eTD Collection

Kwok, A.H., Doyle, E.E.H., Becker, J., Johnston, D., & Paton, D. (2016). What is 'social resilience'? Perspectives of disaster researchers, emergency management practitioners, and policymakers in New Zealand. *International Journal of Disaster Risk Reduction, Vol. 19,* 197-211.

Kyiv Post. (2022, May 6). *Google reports donating $55 million for humanitarian needs of Ukraine*. https://www.kyivpost.com/post/7877

Leclercq-Vandelannoitte, A., & Bertin, E. (2024). How to deal with Big Tech power? The "Big Tech Raj", a new form of biopower in the digital age. *Technological Forecasting and Social Change, 208*, 123732.

Leese, M., & Hoijtink, M. (2019). How (not) to talk about technology. In M. Leese & M. Hoijtink (Eds.), *Technology and agency in international relations* (pp. 1–23). Routledge.

Li, Z., & Qi, H. (2022). Platform power: Monopolisation and financialisation in the era of big tech. *Cambridge Journal of Economics,* 46(6), 1289-1314.

Mearsheimer J (1994/95) The false promise of international institutions. *International Security* 19(3): 5–49.

Matania, E., & Sommer, U. (2023). Tech titans, cyber commons, and the war in Ukraine: An incipient shift in international relations. *International Relations, 1–26*.

Microsoft. (2022). *What is Azure?* Microsoft. https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-azure/

Microsoft. (2020, October 5). *Why does Microsoft have an office at the UN? A Q&A with the company's UN lead*. https://news.microsoft.com/on-the-issues/2020/10/05/un-affairs-lead-john-frank-unga/

Ministry of Foreign Affairs of Denmark. (2017, January 27). *Anders Samuelsen announces digitisation ambassador*. [Press release].

CEU eTD Collection

http://um.dk/en/news/NewsDisplayPage/?newsID=FA99C286-F87C-4259-9A35-E4ED2315C3E2

Morgenthau, H. J. (1948). *Politics among nations: The struggle for power and peace*. Alfred A. Knopf.

Musk E (2022a) [@elonmusk], 26 February. https://twitter.com/elonmusk/status/1497701484003213317 (accessed 20 March 2024).

Nye, J. S., Jr. (2018, January 4). *China's soft and sharp power*. Project Syndicate. https://www.project-syndicate.org/commentary/china-soft-and-sharp-power-by-joseph-s--nye-2018-01

Nye, J. S. (2011, January 31). *The Future of Power*. Press Release. Harvard Kennedy School, Belfer Center for Science and International Affairs.

Nye J (2004) *Soft Power: The Means to Success in World Politics*. New York: PublicAffairs.

Pang, Jinyou. 2022. Logic and Influence for Power Rise of Contemporary Digital Giants in Europe and US. *People's Tribune* 742 (15): 80–85.

Pendleton, D. (2022, October 11). *Elon Musk denies report he spoke with Vladimir Putin before tweeting about 'peace' between Russia and Ukraine*. Fortune. https://fortune.com/2022/10/11/elon-musk-ian-bremmer-putin-russia-ukraine/

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR. *Journal of Cybersecurity*, *4*(1),

Rikap, C. & Lundvall, B.-Å (2022). China's catching-up in artificial intelligence seen as a co-evolution of corporate and national innovation systems. *Research Policy, 51*(1), 104395.

CEU eTD Collection

Romaniuk, R. (2022). Sinking the Moskva: Previously undisclosed details. How the Ukrainian Neptune destroyed the flagship of the Russian fleet. *Ukrainska Pravda*. https://www.pravda.com.ua/eng/articles/2022/12/13/7380452/.

Rosecrance, R. (1986) The Rise of the Trading State. New York: Basic Books

Sandbu, M. (2019). *The economics of big tech.* FT Collections. https://www.ft.com/economics-of-big-tech

Sandre, A. (2017, November 24). *Welcome to the era of tech diplomacy*. Medium. https://medium.com/digital-diplomacy/welcome-to-the-era-of-tech-diplomacy2e174446d25

Saner, R., Uchegbu, A., & Yiu, L. (2019). Private military and security companies: Legal and political ambiguities impacting the global governance of warfare in public arenas. *Asia Pacific Journal of Public Administration, 41*(2), 63–71.

Schmidt, E. (2023, February 28). Innovation power: Why technology will define the future of geopolitics. *Foreign Affairs.* Retrieved from https://www.foreignaffairs.com/unitedstates/eric-schmidt-innovation-power-technology-geopolitics.

Scott, James C. 1998. *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. Yale University Press.

Sherman, N., & Halpert, M. (2025, January 20). Bezos, Zuckerberg, Pichai attend Trump's inauguration. *BBC News*. https://www.bbc.com/news/articles/cvgpqeq82rvo

Smith, B. (2022, June 22). *Defending Ukraine: Early lessons from the cyber war*. Microsoft. https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

CEU eTD Collection

Smith, B. (2022, March 4). *Microsoft suspends new sales in Russia*. Microsoft. https://blogs.microsoft.com/on-the-issues/2022/03/04/microsoft-suspends-russia-sales-ukraine-conflict/

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

Srivastava, M., & Schwartz, F. (2023, June 1). *Elon Musk's SpaceX wins Pentagon contract for satellite in Ukraine. Financial Times*. https://www.ft.com/content/8503ed5a-5ca2-4d34-8c69-66ae92fa80dd

Srivastava, Swati. 2021. Algorithmic Governance and the International Politics of Big Tech. *Perspectives on Politics* 1–12.

Suchman, L. (2022). *Imaginaries of omniscience: Automating intelligence in the US Department of Defense. Social Studies of Science.*

Sutton, H.I. (2022). *Ukraine's Maritime Drones (USV) What You Need to Know. Covert Shores. Available* at: http://www.hisutton.com/Ukraine-Maritime-Drones.html.

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

Thomson, J. E. (1995). State sovereignty in international relations: Bridging the gap between theory and empirical research. *International Studies Quarterly, 39*(2), 213–233. https://www.jstor.org/stable/2600847

Tréguer, F. (2019). Seeing like Big Tech: Security assemblages, technology, and the future of state bureaucracy. In D. Bigo, E. F. Isin, & E. S. Ruppert (Eds.), *Data politics: Worlds, subjects, rights* (pp. 145–164). Routledge.

CEU eTD Collection

Trofimov, Y., Maidenberg, M., & FitzGerald, D. (2022, July 16). Ukraine leans on Elon Musk's Starlink in fight against Russia: SpaceX's satellite internet service has kept front-line troops connected where regular cell networks failed, officials say. *The Wall Street Journal*. https://www.wsj.com/articles/ukraine-leans-on-elon-musks-starlink-in-fight-against-russia-11657963804

Walker, K. (2022, June 10). *Google at the Copenhagen Democracy Summit*. The Keyword. https://blog.google/outreach-initiatives/public-policy/google-at-the-copenhagen-democracy-summit/

Waltz K (1979) *Theory of International Politics*. Reading: Addison-Wesley.

Walker, K. (2022, March 4). *Helping Ukraine*. The Keyword. https://blog.google/inside-google/company-announcements/helping-ukraine

Wen, P., & Agencies. (2024, November 13). Trump selects Elon Musk to lead government efficiency department. *The Guardian*. https://www.theguardian.com/us-news/2024/nov/13/trump-selects-elon-musk-to-lead-government-efficiency-department

Wendt A (2003) *Social Theory of International Politics*. Cambridge, UK: Cambridge University Press.

Wendt A (1995) *Constructing International Politics. International Security* 20(1): 71–81.

Wendt A (1992) Anarchy Is What States Make of It: The Social Construction of Power Politics. *International Organization* 46(2): 391–425.

Wendt A (1987) The Agent-Structure Problem in International Relations Theory. *International Organization* 41(3): 335–370.

Zammit, A. (2003). *Development at Risk: Rethinking UN-Business Partnerships.* Geneva: The South Centre and UNRISD.

CEU eTD Collection

CEU eTD Collection