CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Department of Political Science

Master's Thesis

2024 **Tim Lennart Dalhöfer**

CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Department of Political Science

Deploying the Silicon Web – The Role of ICT Companies in the Russian Invasion of Ukraine

Master's thesis

Author: Tim Lennart Dalhöfer

Study programme: Geopolitical Studies

Supervisor: Mgr. Bohumil Doboš, Ph.D.

Year of the defence: 2024

Declaration

1. I hereby declare that I have compiled this thesis using the listed literature and resources only.
2. I hereby declare that my thesis has not been used to gain any other academic title.
3. I fully agree to my work being used for study and scientific purposes.

In Prague on 31 July 2024 Tim Lennart Dalhöfer

References

Dalhöfer, Tim L. *Deploying the Silicon Web – The Role of ICT Companies in the Russian Invasion of Ukraine.* Praha, 2024. 59 pages. Master's thesis (Mgr.). Charles University, Faculty of Social Sciences, Institute of Political Studies. Department of Political Science. Supervisor Mgr. Bohumil Doboš, Ph.D.

Length of the thesis: 99.786 characters (116.705 characters including footnotes)

Abstract

With the start of the Russian full-scale invasion of Ukraine in February 2022, Western Information and Communication Technology (ICT) companies have found themselves in a strange position. Providing Ukraine's military resistance with critical capabilites and resources, these companies seem to have become geopolitical actors in their own right. Due to its novelty, academic research has so far been lacking theory-driven approaches for the implications that accompany this phenomenon. To help fill this research gap, this thesis offers a new perspective on the actions of ICT companies in interstate war by utilizing Slaughter's theoretical framework focused on connections and networks in geopolitics. It conducted a qualitative comparative analysis of these company action's and their impact on both sides of the war to determine how they shape the conflict and to which degree they provide a strategic advantage to their beneficiaries. The analysis of indivdual within-cases yields support to the notion that ICT companies can enhance the resilience of a country under military attack, while also constituting an important factor for the aggressor. Both findings highlight the critical role ICT companies can play in military conflict. At the same time, the thesis finds that ‚webcraft' alone yields only limited or diminishing returns unless underlined by traditional state-centric instruments of war.

Abstrakt

Po zahájení ruské invaze na Ukrajinu v únoru 2022 se západní společnosti v oblasti informačních a komunikačních technologií (ICT) ocitly ve zvláštní situaci. Zdá se, že tyto společnosti, které poskytují ukrajinskému vojenskému odporu kritické kapacity a zdroje, se samy staly geopolitickými aktéry. Vzhledem k novosti tohoto jevu zatím akademický výzkum postrádal teoreticky podložené přístupy k důsledkům, které tento jev provázejí. Aby pomohla zaplnit tuto výzkumnou mezeru, nabízí tato práce nový pohled na působení ICT

společností v mezistátní válce s využitím Slaughterova teoretického rámce zaměřeného na vazby a sítě v geopolitice. Provedla kvalitativní komparativní analýzu těchto akcí společností a jejich dopadu na obě strany války s cílem určit, jakým způsobem utvářejí konflikt a do jaké míry poskytují strategickou výhodu svým příjemcům. Analýza jednotlivých případů v rámci konfliktu přináší podporu pro názor, že ICT společnosti mohou zvýšit odolnost země, která je pod vojenským útokem, a zároveň představují důležitý faktor pro agresora. Obě zjištění zdůrazňují zásadní roli, kterou mohou ICT společnosti hrát ve vojenském konfliktu. Práce zároveň zjišťuje, že samotné „webcraft“ přináší pouze omezené nebo klesající výnosy, pokud nejsou podpořeny tradičními státními válečnými nástroji.

Keywords

Companies, Geopolitics, Networks, Resilience, Russia, Technology, Ukraine

Klíčová slova

Firmy, Geopolitika, Sítě, Odolnost, Rusko, Technologie, Ukrajina

Title

Deploying the Silicon Web – The Role of ICT Companies in the Russian Invasion of Ukraine

Název práce

Nasazení křemíkového webu - role ICT společností v ruské invazi na Ukrajinu

Table of Contents

Introduction

The Russian invasion of Ukraine on 24th February 2022 saw a massive collective response by Western governments in aiding Ukraine and condemning and sanctioning the actions of the Russian Federation. Western governments opened the gates of their arsenals to supply Ukraine with military hardware, and soon the deliveries of weapon systems like Javelin Anti-Tank Guided Missiles became symbols of the support to Ukraine's resistance. But it was not only Western governments that came to the aid of Ukraine. A public request on Twitter made by Ukraine's Minister for Digital Transformation shortly after the beginning of the invasion was answered by a U.S. tech billionaire over social media platform *X* (formerly *Twitter*) within hours.[1] The subject of the request: That US commercial aerospace company SpaceX should provide its fast, low-latency satellite-based Starlink internet to the Ukrainian people and government. The response tweet by SpaceX's CEO Elon Musk took only twelve hours and declared: "Starlink service is now active in Ukraine.".[2]

The provision of Starlink's services to Ukraine became one of the most visible and famous cases of support for the state by a commercial technology actor, but it was far from the only one. Over the coming weeks and months, dual-use technologies provided by other Information and Communication Technology (ICT) firms rose to prominence. Individuals from around the world could follow the actions on the ground via satellite imagery provided by Maxar Technologies Inc. or observe Russian tank columns streaming into Ukraine via Google Maps. Civilian drones available for purchase in ordinary supermarkets were turned into artillery observers and kamikaze weapons. In short, the Russian invasion of Ukraine[3]

[1] Jayanti, "Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?"
[2] Jayanti.
[3] The term 'Russian invasion of Ukraine' is used in this thesis to describe the events unfolding from 24th February 2022 onwards as part of the wider conflict of the Russo-Ukrainian War. This terminology was chosen to reflect the focus on this particular timeframe, excluding events that didn't take place immediately

became a staging ground for the military employment of dual-use technologies, often provided by private companies without explicit government sanction and yielding battlefield effects on a scale not seen before.

The provision of these services became highly visible on the Ukrainian side, often supported by Western media coverage.[4] Private companies it seemed, were becoming active and even independent stakeholders in an armed interstate conflict. This has already sparked a debate in Western media and policymaking circles about the power of these companies.[5]

Visibility of big tech support was much lower on the Russian side and the Russian armed forces were primarily reported to conduct a much more traditional offensive military campaign, which especially during 2022 yielded only meagre results and even the loss of previously conquered territory. These observations suggests that the involvement of these companies might have had a significant impact on the course of the war and has been relied upon to different degrees by the two sides of the conflict, giving rise to two research problems this thesis addresses:

First, *"How does the involvement of big ICT companies shape the Russian invasion of Ukraine?"*. And second, *"Do countries which obtain the support of big ICT companies have a strategic advantage in armed conflicts over the countries which cannot count on their support?"*.

---

before 24th February 2022 or afterwards, and to emphasize the character of the ongoing events as the result of a war of aggression initiated by the Russian Federation.

[4] Timmermans, "Satellite Imagery Companies in Support of Ukraine"; Horton, "Microsoft Creating a Front Line to Help Ukrainian Government"; Beaty and The Associated Press, "Microsoft Tops the List of Largest Private Donors to Ukraine with $430 Million—but Google Also Made the Cut."

[5] Ero, "Tech Companies Are Fighting for Ukraine. But Will They Help Save Lives in Other Global Conflicts?"; Giles, "Tech Giants Hold Huge Sway in Matters of War, Life and Death. That Should Concern Us All"; Sánchez and Torreblanca, "Ukraine One Year on: When Tech Companies Go to War."

Both these questions are highly relevant for the field of geopolitics which often considers states as the primary actors in international relations and especially when it comes to armed conflict. To answer the research questions, the thesis employed Anne-Marie Slaughter's theory of strategic interconnectivity laid out in her book *The Chessboard & the Web*. Challenging the traditional chessboard view of geopolitics, Slaughter puts forth a theory which requires modern policymakers to also take into account a different perspective of international affairs, the web view, marked by the growing interconnectivity of modern societies and decentralization of power.[6] Answering these questions has far-reaching implications that extend beyond the limits of the ongoing war in Ukraine: At their core lies a discussion of the role, impact and power of civilian companies in armed conflict, and whether technology is shaping societies in ways which challenge traditional notions of geopolitics.

The thesis will begin by providing an overview of the existing literature on the general topic of private companies in foreign policy and war, and in Ukraine specifically. Following this, Slaughter's theory will be introduced to provide a sound theoretical basis for assessing the role of 'Big Tech' in the Russian invasion of Ukraine. Afterwards, the methodological approach is laid out, including the definition of the main research subjects, ICT companies. The main body of the thesis deals with selected case studies of the involvement of these companies in the war, looking into the Ukrainian side and then comparing it with the Russian side. The findings from this analysis will then form the foundation for a discussion around the strategic significance of the support provided by these companies, embedded into Slaughter's theoretical framework. The thesis will conclude with a condensed summary of

[6] Slaughter, *The Chessboard and the Web*, 2017, 72.

the empirical and discussion findings and set them into a broader context while also providing an outlook on future developments associated with the topic.

The Russian invasion of Ukraine stands at the core of an unfolding geopolitical paradigm shift, which is not confined to Europe. Since the end of the Cold War, Western states have reduced their military expenditures and implemented liberal policies which saw the emergence of large technology conglomerates such as Microsoft and Alphabet, which increased the wealth and interconnectivity of their societies. At the same time, these countries became increasingly estranged from the traditional hard power concepts often associated with the chessboard view of geopolitics. Russia's invasion of Ukraine has challenged these perceptions. As European countries see themselves forced to ramp up defense industrial outputs and expand their militaries' capabilities in the face of a Russian threat, the reliance of modern societies on ICT means that these companies can potentially provide conflict parties with critical capabilities. But can the support and reliance on ICT companies really substitute for a lack of conventional military capabilities? By investigating the actions of these companies in the Russian invasion of Ukraine, this thesis will offer a new perspective on the impact their involvement can have in conventional interstate war and how it relates to traditional, state-centric conceptions of warfare.

1. Literature Review

Private Military Companies (PMCs) have received extensive scholarly attention in recent years, especially since their pervasive employment by the U.S. government during the wars in Iraq and Afghanistan. The involvement of private companies in war primarily focused on producing civilian goods on the other hand presents a much more scarcely researched

phenomenon. With the dawn of modern, industrialized wars, civilian industries gained a prominent role, shifting their production from civilian to military goods and thereby forming the material backbone of a country's war effort. These cases mostly include companies being ordered by the government to do so. But notable exceptions exist, like the Ford Motor Company during WWII, which shifted to producing military vehicles and components for the Allies voluntarily already in 1940.[7] This was two years before the second Wars Powers Act came into force in 1942, which compelled U.S. businesses to primarily service government contracts for the war effort.[8] Other cases of voluntary support by civilian companies include various American airlines and logistics companies voluntarily providing cargo and passenger planes to Operations Desert Shield and Desert Storm in 1990/91, prior to their formal activation as part of the U.S. Civilian Reserve Air Fleet.[9]

None of these actions however reflect the form of widespread, voluntary involvement witnessed from ICT companies since the Russian invasion of Ukraine in February 2022. Subsequently, scholarly attention to this phenomenon has only emerged since then and has been dominated by descriptive journalistic and think tank publications. For example, Lilly et al. (2023)[10] compiled a comprehensive list of specific ICT companies and the services provided by them to Ukraine since the onset of the invasion. They divide the support by these companies into three categories – hardware, software, and cyber services. From a limited historical analysis of this support, the authors derive a range of risks and opportunities facing companies when defending a state party to an armed interstate conflict,

[7] Quigley, "Detroit Defied Reality to Help Win World War II."
[8] Quigley; Lawson and Rhee, "Usage of the Defense Production Act throughout History and to Combat COVID-19."
[9] Matthews and Holt, *So Many, So Much, So Far, So Fast: United States Transportation Command and Strategic Deployment for Operation Desert Shield/Desert Storm*, 42.
[10] Lilly et al., "Business@War."

as well as a list of lessons learned for how companies and countries can handle similar cases in the future.

Fox and Probasco (2023)[11] from the Center for Security and Emerging Technology (CSET) conducted a workshop with relevant business leaders, former U.S. government officials, and representatives from the UK's Ministry of Defense to collect qualitative data on how the support for Ukraine by these companies was generated and the challenges faced in establishing and maintaining it. Despite not following strict qualitative methodology and being held under Chatham House rule, their work offers valuable first-hand insight into how ICT companies engaged with the Ukrainian government, and how similar public-private partnerships could be leveraged in the future.

Van Benthem (2023)[12] contributed to a crucial aspect of ICT company support in armed conflicts by analyzing the legal implications resulting from the direct or indirect involvement of Western ICT companies in acts of war in Ukraine under international humanitarian law. By arguing that these companies and their employees potentially expose themselves to military reprisals under international law, she raises to attention to a facet of this support that is often overlooked in the public debate.

Regarding cyber warfare, Mueller et al. (2023)[13] use a mix of empirical analysis and alternative scenario projection based on the Clausewitzian concept of war to assess the events in the cyber theatre of operations during the Russian invasion of Ukraine so far. They arrive at a range of conclusions related to cyber warfare: They find that the employment of offensive cyber tools has confirmed academic skepticism around the nature of 'cyber war',

[11] Fox and Probasco, "Volunteer Force."
[12] Van Benthem, "Privatized Frontlines."
[13] Mueller et al., "Cyber Operations during the Russo-Ukrainian War."

with the coercive impact of these measures during the war remaining limited. Due to the difficulties associated with predicting the effects and outcomes of cyber operations, the authors argue that they have had a greater impact on the strategic than on the tactical level of conflict, with malware being much easier to defend against than disinformation. With much of Ukraine's cyber security capabilities being provided or supported by Western ICT companies, Mueller et al.'s findings suggest that the support that these companies offer Ukraine has played an important role in this.

On the critical side, Öztemel (2022)[14] employs a theoretical Gramscian approach to analyze the involvement of ICT companies in Ukraine, including social media companies, through the lens of the concept of hegemony. She finds that the actions observed by these companies in Ukraine constitute a weaponization of public goods such as internet services, to further states' interests. This in turn would herald a new relationship between governments and businesses, turning the latter into state resources employed at will and not necessarily in line with the interests of the public. Many Western technology companies however stated that they offered their services to Ukraine on a voluntary basis,[15] casting doubt on the direct relationship between these companies and their exploitation by governments as tools of foreign policy.

In addition to the general lack of scholarly research, academic literature that exists at the time of the research for this thesis is falling short in theory-based approaches that recognize ICT companies as foreign policy actors in their own right. Such research can help to challenge existing understanding of the role of these companies in wars, as well as inform considerations about potential future conflicts and the role of these companies in them. At

[14] Öztemel, "Digital Hegemony and the Russia-Ukraine War."
[15] Fox and Probasco, "Volunteer Force," 3.

the same time, the focus of the existing literature is overwhelmingly on Ukraine, with Russia's employment or lack of employment of private sector support being largely ignored. As a consequence, this thesis is intended as a contribution to filling the existing gap in the literature and place the phenomenon of ICT company involvement in wars into a wider theoretical context.

2. Theoretical Framework

Anne-Marie Slaughter's network theory of international politics served as the theoretical foundation for this thesis. The theory derives from the assumption of two existing views of international politics, the traditional view of a chess game, and the new and increasingly important view of a web of connections. According to the theory, both views are valid and exist in parallel, influencing each other.[16] But while there exist grand strategies to underpin the traditional statecraft of the chessboard view, no such strategies exist for application in the realm of what Slaughter calls 'webcraft'.[17]

At its core, Slaughter's theory attempts to fuse two traditions of international relations theory, namely the realist and liberal paradigms. *Statecraft* here is closely related to realist understandings of everything from human nature, the international system, actors, foreign policy goals and means of how to achieve them. *Webcraft* on the other hand builds on classic ideas of liberal international relations theory, namely complex interdependence by Robert Keohane and Joseph Nye (1977) and evolutions of liberal institutionalism.[18]

[16] Slaughter, *The Chessboard and the Web*, 2017, 24.
[17] Slaughter, 73–74.
[18] Slaughter, 29–34.

But in her book, Slaughter goes deeper and develops her own theory by integrating ideas from networks theory into existing liberal concepts. The most fundamental rift between the chessboard and the web lies in what they understand as actors: While the chessboard view only recognizes states as the main actors, the web view looks at actors other than states, including everything from non-governmental civil society organizations to companies, social movements, terrorist organizations, organized crimes syndicates and private individuals, and perceives them as foreign policy actors *in their own right*.[19] Slaughter bases this definition of actors on a phenomenon she calls "disaggregation of the state",[20] which points to the importance of private connections in global governance outside of formal state hierarchies. When these different actors are taken into account, the view on international politics changes from one of separation defined by state borders, to one of connections, constituted by networks of actors.[21] This emphasis on actors also separates the web view from the chessboard view, which – borrowing from neorealist literature – traditionally focuses on the structure of the international system as the defining factor that shapes the actions of states and therefore international politics.[22]

Slaughter sees this shift not as an interesting intellectual tweak, but a necessity borne out of a changing foreign policy landscape. Due to globalization and advances in technology, the world and the people living in it are becoming increasingly connected socially, economically, politically and in many other dimensions.[23] Borrowing from chaos theory, Slaughter therefore adapts the notion of international politics as a "complex adaptive system",[24] being made up of a vast number individual parts which stand in constant

[19] Slaughter, 23, 37.
[20] Slaughter, 37.
[21] Slaughter, 7.
[22] See for example Donnelly, *Realism and International Relations*, 82–85.
[23] Slaughter, *The Chessboard and the Web*, 2017, 5.
[24] Slaughter, 39.

interaction with each other.[25] In complex adaptive systems, the components of the system interact with and adapt to each other as a whole, to create results that are not predictable from focusing only on the actions of individual components.[26] If international politics is a complex adaptive system and is made up of actors, then understanding international politics starts to mean understanding how different networked actors interact with and adapt to each other.[27]

While Slaughter's ontological bases are not novel and rather present different names for existing concepts and schools of thought in international relations literature, the implications she draws from them for applied foreign policy are innovative. The intellectual added value from her theory becomes visible when networks become seen as tools of foreign policy, which can be "designed, activated and managed to achieve specific policy goals".[28] In order to achieve this, Slaughter leverages existing ideas, concepts, and insights from the discipline of network study to provide a range of strategies on how networks can be leveraged to achieve foreign policy objectives.

2.1. Resilience Problems & Network Structures

Slaughter defines three broad categories of foreign policy problems currently facing policymakers: resilience problems, execution problems and scale problems.[29] According to her, "resilience problems involve avoiding and responding to crises, whether man-made, natural, or both, ranging from a direct military attack to an earthquake to a famine".[30]

[25] Slaughter, 38.
[26] Slaughter, 40.
[27] Slaughter, 40.
[28] Slaughter, 41.
[29] Slaughter, 77.
[30] Slaughter, 77.

Execution problems on the other hand concern how specific actions are implemented by a defined range of actors to achieve a specific policy goal, while scale problems occur when policy solutions fail to address a challenge on a macro scale.[31] While Slaughter emphasizes that most contemporary foreign policy problems are made up of a mix of these three categories, she argues that for each of these three dimensions specific types of networks can be designed and managed to address problems within the dimensions.[32] Using Slaughter's typology, the Russian invasion of Ukraine can accurately be described as a resilience problem for the Ukrainian state, making this the most relevant foreign policy problem dimension to investigate. In order to know what qualities a network addressing resilience problems must have, it is necessary to first define the term 'resilience' more closely.

Slaughter uses definitions by Levin & Lubchenco (2008) as well as Zolli & Healy (2014) to define resilience in foreign policy as the capacity of both individuals, collectives and systems to withstand external pressure and recover from it.[33] Drawing from resilience studies, Slaughter states that natural systems exhibit the qualities of diversity, modularity, and redundancy, and are more likely to be resilient to external pressures.[34] The core components of resilience are primarily found in networks rather than hierarchies, raising attention to the importance of how networks are structured to be as resilient as possible.[35] Slaughter finds that distributed mesh network structures are generally the most resilient, based on a study by Baran (1964).[36] However, mesh networks are more exposed to attacks because they cannot be sealed off, while also lacking the ability to form strong clusters that act as critical nodes

[31] Slaughter, 77–78.
[32] Slaughter, 78.
[33] Slaughter, 80–81.
[34] Slaughter, *The Chessboard and the Web*, 2017.
[35] Slaughter, 81.
[36] Baran, "On Distributed Communications: I. Introduction to Distributed Communications Networks," 34; in Slaughter, *The Chessboard and the Web*, 2017, 82–83.

for de-centralized (star) networks.[37] With these qualities in mind, it is now possible to look at Slaughter's resilience networks strategy that is most relevant for the investigation of the research topic of this thesis: defense networks.

2.2. Defense Networks

As Slaughter notes, war is usually associated with the realist chessboard view of international politics.[38] States are generally seen as the principal actors in war, pitting highly hierarchically organized armies against each other on the battlefield. The prime objective in this traditional conception of war is to conquer territory, especially central hubs of the adversary such as the strategically important chokepoints or the capital city.[39] Slaughter challenges this conception by pointing out the increasingly networked character of conflict, especially when non-state actors are partaking in the conflict.[40] She sees hybrid modes of warfare as focusing on structurally weakening the adversary instead of aiming for territorial conquest in the context of open military hostilities.[41]

It is at this point where Slaughter's theory requires adaptation: Even when non-state actors are completely ignored, with the full outbreak of military hostilities on 22nd February 2022, the Russian invasion has shown that conquest of the capital is not the only mode of warfare in this conflict: It has become an integral element of the Russian military campaign to degrade Ukrainian military and civil infrastructure alike, including the destruction of transmission stations, dams, and power plants.[42] Long-range precision-guided munitions

[37] Slaughter, *The Chessboard and the Web*, 2017, 83.
[38] Slaughter, 84.
[39] Slaughter, 86.
[40] Slaughter, 84.
[41] Slaughter, 86.
[42] See for example: United Nations Security Council, "Escalating Attacks on Ukraine's Civilian, Energy Infrastructure Making Humanitarian Aid Delivery Even More Dangerous, Relief Chief Tells Security Council"; Hurska, "Russian Attacks on Ukrainian Critical Infrastructure Become Hybrid Threat to Europe."

make all infrastructure in the country potentially vulnerable. In Slaughter's view, defending against hybrid threats is essentially an issue of strategic infrastructure dispersion to deny the adversary the capturing of critical hubs.[43]

It is crucial to note that nowadays the term infrastructure has evolved to not only encompass facilities that provide public goods like water and electricity or military goods like materiel and ammunition, but countries have recognized that due to the heavy reliance on information and communication technologies (ICT), digital infrastructure such as server farms, telecommunication antenna and data centers have become equally essential to modern societies.[44] The same is true for military applications which increasingly rely on ICT for everything from communication and targeting to payload delivery. Maintaining and protecting these infrastructures is also not a sole physical challenge but also a digital one, as connected infrastructures are also vulnerable to cyberattacks. Therefore, for this thesis, Slaughter's concept of infrastructure and what it means to protect it is extended to capture these technologies.

To determine the optimal network structure to minimize infrastructure vulnerability, Slaughter compares *random networks* - which contain an even distribution of connections between all nodes of the network – with *scale-free networks*, where major hubs exist that connect to many nodes at once, while other nodes have only a few interconnections.[45] While scale-free networks exhibit greater resilience vis-à-vis random failure, they are more vulnerable against deliberate attacks against the major hubs, as the network heavily depends

[43] Slaughter, *The Chessboard and the Web*, 2017, 86.
[44] European Parliament and The Council of the European Union, Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, (5), (20); European Commission, "White Paper - How to Master Europe's Digital Infrastructure Needs?," 3–5.
[45] Slaughter, *The Chessboard and the Web*, 2017, 84.

on their connections.[46] Thus, Slaughter argues that infrastructure needs to be organized in a random, distributed mesh network for the case of defense against deliberate external attacks.[47]

As the name suggests, Slaughter's concept of defense networks is first and foremost a concern for the defending side in an armed conflict. It would follow from this that an attacker would not need to pay attention to establishing these networks of web actors as they do not pursue resilience, understood as the capacity to resist change and recover from it.[48] The attacker would instead focus on a traditional chessboard-view of war, relying primarily on the capabilities of the state. But the literature review above has shown that even countries conducting offenses such as the United States during the 1991 Gulf War have relied on a network of private actors in the past to provide capabilities that the state either didn't have or wasn't as effective in. Also, it is important to point out that the roles of the offense and defense often change during a war, forcing the sides to adapt their posture. Even an initial attacker might therefore want to look at obtaining support from 'the web' to supplement their capabilities.

3. Methodology

The purpose of this thesis was to investigate how the involvement of ICT companies is shaping the Russian invasion of Ukraine and the implications of this support for strategic success, by using Anne-Marie Slaughter's theory of the chessboard and the web. This was achieved by investigating each side of the conflict's use of ICT company support, with cases

[46] Slaughter, 85–86.
[47] Slaughter, 86.
[48] Slaughter, 80–81.

of specific company support constituting within-cases. The author employed a comparative case study research design to illustrate the different roles the support of ICT companies plays for both the defender and the attacker in the ongoing war. The unique involvement of these companies in an armed interstate conflict presents what Gerring & Christenson (2017) term a 'pathway case', which serves to illustrate a theory and demonstrate the plausibility of its application to future cases.[49]

Slaughter's theory informed this thesis in the following ways: It determined non-state actors and more closely, significant private ICT companies as the principal actors whose actions were investigated. ICT herein presents an umbrella term that according to Rouse (2023) is defined as "computing and telecommunication technologies, systems and tools to facilitate the way information is created, collected, processed, transmitted and stored.".[50] The term includes both hardware and software components that are involved in the handling of information, including artificial intelligence applications and satellite communication infrastructure.[51] It also follows that the mode of interactions that were investigated were between companies and governments, often going through informal channels. This in turn determined the research basis for the thesis, which drew on qualitative data from company statements, existing research reports, news reports and government sources. Furthermore, the theory narrowed down the kind of support that was investigated. As Slaughter conceptualizes defense networks primarily in terms of infrastructure, the thesis focused on the (digital) infrastructure support extended to parties of the war by ICT companies. These actions constitute the independent variable whose influence on the strategic balance in the ongoing invasion was scrutinized.

[49] Gerring and Christenson, *Applied Social Science Methodology: An Introductory Guide*, 191.
[50] Rouse, "Information and Communication Technology (ICT)."
[51] Rouse.

The second research question regarding whether countries which obtain the support of ICT companies receive a strategic advantage over those countries who don't, was used to test Slaughter's theoretical framework. To answer the research question, two hypotheses derived from the theory were tested:

H1: The involvement of big ICT companies had a significant impact on Ukraine's capacity to resist the Russian invasion.

H2: Russia's role as the aggressor means it doesn't have to rely on independent ICT companies to support its war effort.

The selected within-cases were chosen on the basis of their prominence, the form of their support as dual-use (digital) infrastructure support as determined by the theoretical framework, and the availability of data on them. While there exists a myriad of smaller ICT companies which provided support to different sides of the conflict, investigating all of these cases would have extended far beyond the scope of this master thesis. The author therefore focused on support actions by the biggest companies, which have access to more resources - both financial and human -, and within Slaughter's theoretical framework present critical and well-connected nodes which determine a significant part of the power of a given network. The within-case studies were contextualized with the events unfolding on the frontlines at the time to assess their impact on the wider conflict. Because the Russian invasion of Ukraine continued during the writing of this thesis, it was necessary to define a cut-off point for the research. This was also influenced by the availability of data on technology company involvement, as the latest developments are often either still unclear under the fog of war, or not openly available for investigation. The research therefore generally focused on developments until the 31st of December 2023. Where circumstances and the availability of data allowed it, this timeframe was extended.

4. Analysis

The analysis was conducted by first looking at ICT companies supporting the Ukrainian side of the war, and after that the cases supporting the Russian side. The subject of the analysis was the relevant actions of the companies, in line with Slaughter's assumptions about networks. These actions were then contextualized with the wider strategic picture of the war at the time to qualitatively assess their impact on the war as best as possible.

For this purpose, the war until December 2023 was roughly divided into six different phases, based on the most significant events.[52] A general overview of the phases is presented here, while a more detailed look at the relevant phases is provided within the respective case studies. *Phase 1* of the war revolved around the initial invasion and the Battle for Kyiv from February to April 2022. *Phase 2* saw Russia shift its focus on a campaign in the South and East of Ukraine between April and August 2022, which resulted amongst other events in the capture of Mariupol and Luhansk Oblast. *Phase 3* presents the first Ukrainian counteroffensives from August until November 2022 which result in the recapture of Kharkiv and Kherson. *Phase 4* occurred during the winter and spring between November 2022 and June 2023 and was marked by attrition and stalemate, symbolized by the battle for Bakhmut. It also marks the beginning of widespread Russian long-range strategic strikes against Ukrainian civilian critical infrastructures.[53] During *Phase 5* the Ukrainian Armed Forces (UAF) launched its summer offensive in June, which would last until November when UAF commander-in-chief General Valery Zaluzhnyi declared another stalemate after

[52] Weber, "A Brief Timeline of Russia's War in Ukraine."
[53] Hoffmann, "Strategic Stability and the Ukraine War - Implications of Conventional Missile Technologies," 8–9.

the offensive failed to reach its objectives.[54] *Phase 6* saw the invasion enter into its second winter campaign.

4.1. Ukraine – Starlink

When analyzing ICT companies in the Russian invasion of Ukraine it is hard to ignore Starlink. Only a few dozen hours into the war, the subsidiary of SpaceX became one of the most visible supporters of Ukraine, with Elon Musk and other C-Suite executives covering its involvement via social media platforms for the public. It also became one of the most controversial involvements of a private company as the war progressed. Its actions therefore formed a sensible starting point for the analysis.

4.1.1. Actions

The primary support provided by Starlink to Ukraine is broadband internet. Starlink internet is based on the world's largest constellation of thousands of small satellites (SmallSats) in low-earth orbit (~550km altitude).[55] Starlink's current domination of this sector of internet services provision rests on the ability to have its SmallSats delivered to space by its parent company SpaceX.[56] The company offers very low-latency internet connection with up to 150 Megabits per second (Mbps) and beyond.[57] The distributed structure of the SmallSat constellation makes it especially resilient against physical attacks, which would require a

[54] Weber, "A Brief Timeline of Russia's War in Ukraine."
[55] Starlink, "Satellite Technology."
[56] Starlink.
[57] Yasar, "Starlink."

concerted effort to attack all satellites individually.[58] It is also resilient against cyberattacks, due to the ability to quickly access and alter the code by administrators.[59]

According to SpaceX COO Gwynn Shotwell, Starlink initially approached the Ukrainian government about the activation of Starlink in Ukraine already in January 2022, when the risk of a Russian invasion was becoming more tangible. But an answer by the Ukrainian side was pending until 26th February, when Minister Fedorov directed his bid at Musk via social media platform *X* (formerly *Twitter*), a move that was taken as the approval for the initial bid by SpaceX.[60] As mentioned before, Musk's famous reply on X twelve hours afterwards sealed the deal, and the by 28th February, the first shipment of Starlink terminals reached the Ukrainians.[61] According to the author of Musk's authorized biography, Walter Isaacson, Starlink donated about half of its services and hardware, while the other have was funded by Western governments and private donors.[62] By October 2022, Musk complained that if the U.S. government wouldn't share the expenses, he will have to discontinue operations in Ukraine.[63] As a result, since June 2023, Starlink services and hardware are provided by Starlink to Ukraine through a contract with the U.S. Department of Defense, whose terms have not been publicized.[64]

[58] Miller, Scott, and Bender, "UkraineX: How Elon Musk's Space Satellites Changed the War on the Ground."
[59] Foust, "SpaceX Worked for Weeks to Begin Starlink Service in Ukraine."
[60] Foust.
[61] Reese, "Can Elon Musk's Starlink Keep Ukraine Online?"
[62] Isaacson, "'How Am I in This War?': The Untold Story of Elon Musk's Support for Ukraine."
[63] Marquardt, "Exclusive: Musk's SpaceX Says It Can No Longer Pay for Critical Satellite Services in Ukraine, Asks Pentagon to Pick up the Tab."
[64] Stone and Roulette, "SpaceX's Starlink Wins Pentagon Contract for Satellite Services to Ukraine."

4.1.2. Impact

According to Forbes Magazine, 42,000 terminals have been deployed to Ukraine since the start of the war as of February 2024.[65] Their use has been both of civilian and military nature. The first days and weeks of the war were characterized by the Russian military's push for the Ukrainian capital city of Kyiv, including the airborne operation to take Hostomel Airport and the advance of Russian tank columns towards the city from the northern border with Belarus.[66] The Russian effort also included massive attempts at degrading Ukrainian Command & Control (C2).[67] This timeframe proved crucial, as according to Western observers, Russia seemed to intend disarraying Ukrainian troops in the area and forcing the capitulation or evacuation of the Ukrainian government, which was supposed to eventually result in the subjugation of the state.[68]

The use of Starlink broadband internet started immediately after the first terminals arrived on 28th February. One of its first applications was to generate additional communication capacities for the Ukrainian military command after the degradation of the satellite internet network Visasat KA-SAT, which was also used by the military, through a cyberattack. The Visasat Hack occurred in the early hours of the invasion on 24th February 2022, when hackers attributed by Western governments to being associated with the Russian government, accessed a VPN used by Visasat administrators and delivered a wiper malware coined 'AcidRain' to thousands of internet modems.[69] This malware rendered about 45.000 modems inoperable, leading to a substantial loss in communications, according to Ukrainian officials.[70] A second stage of the attack which overloaded Visasat servers with requests was

[65] Folk, "Russia Using Starlink Terminals Bought On 'Open Market' In Ukraine War, Report Says."
[66] Zabrodskyi et al., "Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022," 29–34.
[67] Zabrodskyi et al., 24–25.
[68] Zabrodskyi et al., 8.
[69] Vasquez and Groll, "Satellite Hack on Eve of Ukraine War Was a Coordinated, Multi-Pronged Assault."
[70] Vasquez and Groll.

only discovered later, and according to a Viasat executive, was targeting specific modems.[71] It has to be noted that the concrete impact of the Viasat Hack remains contested until this day, with conflicting accounts and assessments of the effects of the attack having surfaced, ranging from a detrimental loss of military communication, to only negligible effects.[72] Regardless of the ultimate impact, Starlink offered the Ukrainian military additional communications capacity, also as a redundancy against potential additional cyberattacks against its communication networks. By 1st March, SpaceX's Director of Starlink Operations Lauren Dreyer tweeted on X that Starlink was used by the UAF to maintain communication with theatre command centers.[73] This can be deemed especially important, since Ukrainian intelligence and defense services had previously focused about half of the Ukrainian military's maneuver forces to the Ukrainian Joint Forces Operation (JFO) located along the previous line of contact in the East of the country, where they assumed Russia's primary focus would be.[74] In the following days, Starlink was used for multiple operational communication purposes within the UAF, including the facilitation of real-time voice connections for Ukrainian special forces.[75] It also facilitated communications between the Ukrainian military and the United States' Joint Special Operations Command, possibly for the sharing of intelligence.[76]

Given the pressure directed by the Russian military against Ukrainian C2 by kinetic and non-kinetic means, the value of the additional, distributed communication capabilities provided by Starlink to the Ukrainian military becomes clear. Operationally, it enabled the Ukrainian

[71] Vasquez and Groll.
[72] Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," 5–6; Martin, "Cyber, MacGyver, and the Limits of Covert Power."
[73] Isaacson, "'How Am I in This War?': The Untold Story of Elon Musk's Support for Ukraine."
[74] Zabrodskyi et al., "Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022," 23–24.
[75] Isaacson, "'How Am I in This War?': The Untold Story of Elon Musk's Support for Ukraine."
[76] Isaacson.

military to coordinate its forces in the area around Kyiv after initial disarray. Strategically, it facilitated resilient communication channels with Western partners.

With the siege of Kyiv averted, Russia shifted its focus to the Ukrainian forces of the JFO in the Donbas.[77] The area along the southern and eastern axes of advance saw Russia rapidly achieve operational successes, with the capturing of Kherson and Melitopol and the encirclement of Mariupol in the South East constituting major flashpoints.[78] While the advance towards Kyiv was marked by maneuver warfare elements, using airborne units and mechanized units to quickly cover ground, Russia's offensive in the East quickly turned to employing massive, structured artillery support to cover the advance of troops.[79] Subsequently, Ukrainian counter-battery missions became critical in resisting the invading forces.[80]

According to Zabrodskyi et al. (2022), Unmanned Aerial Vehicles (UAVs) became a crucial component during this stage of the war, as they served a primary role in target acquisition for the UAF.[81] The conduct their missions, UAVs rely on internet connection. As early as March 2022, UAF units stated that they had started using Starlink for the operation of UAVs flying target acquisition missions.[82] Establishing a video link from the UAV to the operator was important to provide UAF artillery units with an accurate picture of the battlefield and potential targets, so that they could counter overwhelming Russian firepower with precision strikes.[83] During the second phase of the invasion, Starlink also can be said to have bought

[77] Zabrodskyi et al., "Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022," 34–35.
[78] Zabrodskyi et al., 28.
[79] Zabrodskyi et al., 37.
[80] Zabrodskyi et al., 38–39.
[81] Zabrodskyi et al., 37.
[82] Freund, "Ukraine Using Starlink for Drone Strikes"; Marquardt, "Exclusive: Musk's SpaceX Says It Can No Longer Pay for Critical Satellite Services in Ukraine, Asks Pentagon to Pick up the Tab."
[83] Zabrodskyi et al., "Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022," 37.

crucial time for the UAF: While the majority of the city of Mariupol fell relatively quickly to the encirclement of Russian forces at the beginning of April 2022, Ukrainian forces in defensive positions at the Azovstal steel plant resisted Russian attackers for weeks until the end of May. According to Zabrodskyi et al. (2022), this forced the Russian military to temporarily withhold troops from advancing north on the southern axis towards the Donbas, allowing UAF units to cover smaller frontages.[84] Starlink terminals were delivered to the defenders at the Azovstal complex by Ukrainian forces during Operation Air Condor.[85] This allowed the defenders to establish connection with the outside world, sharing photos and videos of the siege with reporters that went around the world.[86]

Since then, Starlink has been employed by the UAF in all the aforementioned roles, for facilitating communication between commanders and frontline troops, as well as running reconnaissance and seek-and-destroy missions of UAVs. The importance of Starlink only increased as Russia ramped up precision strikes against Ukrainian critical infrastructure, degrading civilian and military communication networks.[87]

But the support by Starlink and subsequently Elon Musk has also not been without problems. In Musk's biography, Walter Isaacson (2023) claims that in September 2022 Musk secretly asked Starlink engineers to turn off Starlink reception in and around Crimea to prevent the UAF from launching an unmanned submarine attack against Russia's Black Sea Fleet anchored in Sevastopol.[88] Musk's decision allegedly followed discussions between him and Russian officials about the threat of reprisals against Starlink, and whether it would become

[84] Zabrodskyi et al., 37.
[85] Schwirtz, "Last Stand at Azovstal: Inside the Siege That Shaped the Ukraine War."
[86] Schwirtz.
[87] Franke and Söderström, "Star Tech Enterprise: Emerging Technologies in Russia's War on Ukraine."
[88] Isaacson, "'How Am I in This War?': The Untold Story of Elon Musk's Support for Ukraine."

complicit in acts of war against Russia.[89] Musk responded on X by stating that Starlink was never turned on in the area around Crimea to begin with,[90] but confirmed that he had denied a request by the Ukrainian government to activate it in the area, with the intent of preventing his company from becoming directly complicit in an act of war.[91] The incident raised attention amongst commentators about the power and influence exerted in the war by a private individual.[92] Also, in February 2024, the Chief of the Ukrainian Main Directorate for Intelligence, Lt. General Kyrylo Budanov stated in a Wall Street Journal interview that Russian forces are using Starlink terminals in occupied territories of Ukraine.[93] According to Budanov, Russia is using proxy buyers such as private companies to acquire Starlink terminals from third-party vendors and then transfer them to Russian troops in Ukraine.[94] The source countries for the terminals are alleged to be Arab nations, as well as post-Soviet countries, with terminals also appearing on Russian online market sites.[95] While Starlink has reacted stating that their terminals don't work on the territory of Russia,[96] it doesn't rule out the use of these terminals on Ukrainian territory by Russian troops. Along with reports of Russian forces increasingly blocking the use of Starlink terminals,[97] it seems that the utility of Starlink for Ukraine is declining. This happens during a phase of the war where Ukraine

[89] Pennington and Lyngaas, "Starlink in Use on 'All Front Lines,' Ukraine Spy Chief Says, but Wasn't Active 'for Time' over Crimea."
[90] Musk, "Much Appreciated, Walter. The Onus Is Meaningfully Different If I Refused to Act upon a Request from Ukraine vs. Made a Deliberate Change to Starlink to Thwart Ukraine. At No Point Did I or Anyone at SpaceX Promise Coverage over Crimea. Moreover, Our Terms of Service Clearly Prohibit Starlink for Offensive Military Action, as We Are a Civilian System, so They Were Again Asking for Something That Was Expressly Prohibited. SpaceX Is Building Starshield for the US Government, Which Is Similar to, but Much Smaller than Starlink, as It Will Not Have to Handle Millions of Users. That System Will Be Owned and Controlled by the US Government."
[91] Musk, "There Was an Emergency Request from Government Authorities to Activate Starlink All the Way to Sevastopol. The Obvious Intent Being to Sink Most of the Russian Fleet at Anchor. If I Had Agreed to Their Request, Then SpaceX Would Be Explicitly Complicit in a Major Act of War and Conflict Escalation."
[92] Dress, "How Elon Musk Became a Power Player in the Ukraine War"; Copp, "Elon Musk's Refusal to Provide Starlink Support for Ukraine Attack in Crimea Raises Questions for Pentagon."
[93] Marson and Grove, "Russia Using Thousands of Musk's Starlink Systems in War, Ukrainian General Says."
[94] Marson and Grove.
[95] Marson and Grove.
[96] Folk, "Russia Using Starlink Terminals Bought On 'Open Market' In Ukraine War, Report Says."
[97] Satariano and Mozur, "Russia, in New Push, Increasingly Disrupts Ukraine's Starlink Service."

is again under heavy pressure from Russia, especially in the area around Kharkiv, which already led Western countries to the landmark decision of allowing Ukraine to use Western weapon systems to be used against targets in Russian territory bordering Kharkiv.

4.2. Ukraine – Palantir

Starlink is not the only prominent company that provided support to Ukraine through space-based dual-use assets. Palantir CEO Alex Karp became the first major Western company executive that personally met with Ukrainian president Volodymyr Zelenskyy on 2nd June 2022.[98] Palantir, co-founded in 2003 amongst others by billionaire investor Peter Thiel, is a public company since 2020 that offers data mining and analysis services to a wide range of private and public actors.[99] For a long time, the company was known for its contracts with U.S. security agencies, resulting from its early days when it was financially supported by the CIA's investment subsidiary In-Q-Tel to help the U.S. government counter terrorism after the 9/11 attacks.[100] The company has since undertaken efforts to change its public perception by taking on high-visibility contracts like tracking vaccine distribution for the UN World Food Programme during the Covid-19 pandemic.[101] Its services to Ukraine were initially provided free of charge, but Western governments have since started to subsidize the cooperation.[102]

4.2.1. Actions

Since June 2022, Palantir has offered Ukraine a range of services, with the primary contribution being the software MetaConstellation. MetaConstellation aggregates data from

[98] Bergengruen, "How Tech Giants Turned Ukraine Into an AI War Lab"; Dastin, "Ukraine Is Using Palantir's Software for 'targeting,' CEO Says."
[99] Greenberg, "How A 'Deviant' Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut."
[100] Greenberg.
[101] Bergengruen, "How Tech Giants Turned Ukraine Into an AI War Lab."
[102] Grylls, "Ukraine's Secret Weapon: The £40bn Tech Firm That 'Found Bin Laden.'"

hundreds of commercial satellites in space and integrates them with additional terrestrial and aircraft sensors to generate geographical situational awareness for its users.[103] Through partnerships with satellite imagery companies, Palantir deploys artificial intelligence to satellite platforms in an edge computing approach.[104] This means that data is already processed on the device in space, resulting in benefits such as bandwidth optimization, increased updateability, reduced latency and ultimately increased speed of operationalization of data.[105] MetaConstellation allows the UAF to obtain a close to real-time image of a certain geographical space with the ability to surveil enemy troop movements, fortifications, and other events.[106] Furthermore, MetaConstellation's image can be supplemented by other intelligence sources, such as reconnaissance UAVs and even enemy positions highlighted by ordinary citizens on the country's E-Enemy app.[107] To transfer these insights to the battlefield, UAF units are provided with Palantir's 'Skykit', a portable 'reconnaissance center' for field use by troops which contains everything from a small UAV to a laptop and battery supply.[108]

4.2.2. Impact

UAF have used MetaConstellation for improving its so-called target coordination cycle, the tracking, targeting, and prosecution (or attacking) of a military target.[109] Soldiers access MetaConstellation's intelligence on the Skykit and then choose from a range of strike options provided by the software's in-built algorithms to direct fire on the coordinates of a chosen

[103] Palantir, "MetaConstellation."
[104] Satellogic, "Satellogic Announces Strategic Partnership with Palantir Technologies."
[105] Palantir, "Palantir Edge AI in Space."
[106] Bergengruen, "How Tech Giants Turned Ukraine Into an AI War Lab."
[107] Grylls, "Kyiv Outflanks Analogue Russia with Ammunition from Big Tech."
[108] Armed Forces of Ukraine, "Ukrainian Armed Force Use Skykit Palantir."
[109] Maçães, "How Palantir Is Shaping the Future of Warfare."

target.[110] After target prosecution, the soldier is able to feed a damage assessment back into the system which leverages its AI capabilities to train the system in providing better options in the future.[111] Palantir's AI-supported software is able to reduce the time it takes to complete the target coordination cycle to mere minutes,[112] resulting in the acquisition of hundreds of targets per day, according to military experts.[113] Since Palantir's involvement in Ukraine started only in June 2022, it did not have any direct impact on the initial phases of the war, including the battle for Kyiv and the Russian re-focusing on the East and Southeast of Ukraine. MetaConstellation's deployment in June however coincides with the arrival of the first M142 High-Mobility Artillery Rocket System (HIMARS) units in Ukraine in late June.[114] Throughout July, the UAF used HIMARS units for precision strikes against fixed Russian targets, such as command centers and ammunition depots.[115] According to Zabrodskyi et al., the deployment of HIMARS by the UAF constituted a new phase of the war starting in the summer of 2022.[116] Over the summer and fall of 2022, Ukrainian counteroffensives were able to liberate the cities of Kharkiv and Kherson from Russian forces in a significant strategic shift.[117] Both counteroffensives were preceded by the degradation of Russian supply lines and logistics through high-precision HIMARS strikes.[118] The assessment of the direct impact of Palantir on these operations however is difficult: On 2nd February 2023, Palantir CEO Karp publicly claimed that Palantir's software was

[110] Grylls, "Kyiv Outflanks Analogue Russia with Ammunition from Big Tech"; Armed Forces of Ukraine, "Ukrainian Armed Force Use Skykit Palantir."
[111] Maçães, "How Palantir Is Shaping the Future of Warfare."
[112] Maçães.
[113] Grylls, "Kyiv Outflanks Analogue Russia with Ammunition from Big Tech."
[114] Porter, "Ukraine Celebrates US Long-Range Rocket Systems Arriving after Months of Asking. 'Summer Will Be Hot for Russian Occupiers.'"
[115] BBC, "Ukraine: What Are Himars Missiles and Are They Changing the War?"
[116] Zabrodskyi et al., "Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022," 43.
[117] Khurshudyan et al., "Inside the Ukrainian Counteroffensive That Shocked Putin and Reshaped the War."
[118] Glantz, "How Ukraine's Counteroffensives Managed to Break the War's Stalemate."

"responsible for most of the targeting in Ukraine".[119] One week later, The Washington Post contradicted this claim by citing Ukrainian officials stating that they "almost never launch HIMARS rounds without detailed coordinates provided by U.S. military personnel situated elsewhere in Europe".[120] This does not necessarily mean that Palantir is not involved in the targeting for HIMARS strikes around this time: According to Ignatius (2022), NATO has been supplying the UAF with targeting intelligence from a command post outside of Ukraine whose system is using MetaConstellation as well.[121] The difference between NATO's MetaConstellation instance and the one used inside of Ukraine is that the former also integrates data from Western intelligence sources not directly accessible to the latter, such as Western military satellites.[122] While the data source is different, it is still possible that target coordinates are communicated to the Ukrainian MetaConstellation instance from where target prosecution can be initiated. With the existing, publicly available data, it is however not possible to clearly establish this process. In any way, it demonstrates that Palantir's software was deeply involved in the facilitation of the operational success of the UAF during these counteroffensives. This is illustrated by the comments of Mykhailo Fedorov, who was quoted as saying that this process "was especially useful during the liberation of Kherson, Izium, Kharkiv and Kyiv regions".[123]

The use of MetaConstellation was also highlighted in preparation for the Ukrainian summer counteroffensive of 2023. Maçães (2023) cites a UAF commander describing how precision strikes likely using MetaConstellation were launched against C2 and logistical targets.[124] MetaConstellation was then used to identify, track and prosecute Russian reserve units

[119] Dastin, "Ukraine Is Using Palantir's Software for 'targeting,' CEO Says."
[120] Khurshudyan et al., "Ukraine's Rocket Campaign Reliant on U.S. Precision Targeting, Officials Say."
[121] Ignatius, "How the Algorithm Tipped the Balance in Ukraine."
[122] Ignatius.
[123] Ignatius.
[124] Maçães, "How Palantir Is Shaping the Future of Warfare."

moved to reinforce the defensive lines.[125] Despite this, the Ukrainian summer counteroffensive of 2023 did not yield the expected success due to a wide range of factors identified by Ukrainian officials and Western analysts.[126]

As early as November 2023, the Ukrainian government began to partner with Palantir in another dimension of the war: The battle against landmines. According to Bergengruen (2023), Ukraine has become the world's most contaminated country with regards to landmines since the start of the Russian invasion, surpassing countries like Afghanistan and Syria.[127] During an initial pilot program, a Palantir software platform integrated 82 sets of data from Ukrainian government institutions and telecommunication companies connecting "6 million buildings, 60,000 train segments, and one million road segments".[128] The goal was to use the platform to identify where and how de-mining efforts could achieve the highest efficacy.[129] Palantir and the Ukrainian government have since formalized this cooperation in a partnership on 4th March 2024, which would see Palantir generate a digital twin that reflects how mine hazards are connected to existing infrastructure and will help Ukrainian and international de-mining professionals determine the safest and most efficient locations and means to conduct removal efforts.[130] The agreement states that its ultimate goal is to ensure the usability of 80% of contaminated land within a ten-year timeframe.[131] While humanitarian demining is explicitly not done for military purposes, it does represent the 'recovery' aspect of resilience used by Slaughter.[132] Humanitarian demining offers economic benefits by repopulating previously decontaminated land and improving the safety

[125] Maçães.
[126] see Wilk and Żochowski, "Ukraine Confirms Its Counter-Offensive Has Failed. Day 617 of the War"; Gady and Kofman, "Making Attrition Work: A Viable Theory of Victory for Ukraine."
[127] Bergengruen, "Ukraine Is Using AI to Help Clear Millions of Russian Landmines."
[128] Bergengruen.
[129] Bergengruen.
[130] Palantir, "Palantir and Ministry of Economy of Ukraine Sign Demining Partnership."
[131] Palantir.
[132] Slaughter, *The Chessboard and the Web*, 2017, 80–81.

of Ukrainian citizens. But cleared areas on liberated land would also allow the UAF to move troops and equipment more efficiently towards and away from the frontlines.

It becomes clear that assessing Palantir's direct impact on the battlefield is not easy. Its products like MetaConstellation seem to have been well integrated into the way the UAF operates. But these systems are only as good as the data they have available to them. While the UAF has a plethora of data sources on its own territory, such as UAVs and even its own citizens reporting enemy movements on apps, Ukraine lacks its own sophisticated space capabilities. Palantir provides Ukraine with access to commercial space-based assets. But commercial satellite data on its own is not responsible for the UAF's ability to identify, track, and successfully hit high-value targets with the accuracy it demonstrated during its counteroffensives. The supplementation with data from Western space-based assets outside of Ukraine seems to have been a crucial element here. Nevertheless, without the integration of MetaConstellation through which target coordination data is streamed into UAF soldiers' hands, it is questionable whether the UAF could have succeeded in operations where accuracy is essential to overcome an adversary that enjoys superiority regarding the quantity of weapon systems and ammunition.[133] However, since the invasion evolved into a war of attrition throughout 2023, analysts have noted that low-quantity precision strikes cannot entirely make up for a lack of mass fire capability.[134] While Palantir might allow the UAF to continue to observe the battlefield on an unprecedented level, its capacity to achieve operational success is limited by the availability of weapon systems and ammunition. This highlights the direct relationship between the capabilities that technology companies bring

[133] Douro, "MLRS and the Totality of the Battlefield."
[134] see Fox, "The Russo-Ukrainian War: A Strategic Assessment Two Years Into the Conflict," 13; Michta, "Mass Still Matters: What the US Military Should Learn from Ukraine"; Saballa, "Ukraine War Exposes Flaws in America's Sophisticated Weapons: Analysts."

to Ukraine, and the traditional coercive instruments of war such as kinetic weapons and ammunition.

4.3. Ukraine – AWS/Google/Microsoft

Few ICT companies have been involved on the Ukrainian side of the war as much as Amazon Web Services (AWS), Google and Microsoft. Along with representing three of the five most valuable companies in the world at the time of the writing of this thesis,[135] these firms constitute some of the most significant financial donors to Ukraine's resistance effort, donating money and services worth hundreds of millions of U.S. dollars.[136] Since the services these companies have offered to Ukraine are similar and fall within the spectrum of digital infrastructure support, their contributions were assessed as a single within-case. Some of these companies' contributions enabled the proper functioning of the services discussed in the previous cases, but due to their nature are much less visible than a Starlink satellite constellation or a Palantir Skykit. This also made their impact on the operational and strategic level of war much more challenging to assess. Because the support by these companies is significant and takes many shapes, the level of detail of the analysis was limited here to stay within the scope of the thesis.

4.3.1. Actions

The relevant digital infrastructure support from these companies can be categorized roughly following the categorization of Lilly et al. (2023):

- Cloud services

[135] CompaniesMarketCap.com, "Largest Companies by Market Cap."
[136] Beaty and The Associated Press, "Microsoft Tops the List of Largest Private Donors to Ukraine with $430 Million—but Google Also Made the Cut."

- Cyber security/Cyber defense
- Technical infrastructure

Cloud services, including migration and operation, were and continue to be provided to the Ukrainian government by AWS and Microsoft.[137] Throughout 2023, Google provided tens of thousands of cloud-based, zero-trust security Workspace licenses to the Ukrainian government free of charge.[138] Regarding cyber security, Microsoft played a major role, given the prominence of its operating system Windows: throughout the conflict it has provided the Ukrainian government and people with extensive threat intelligence, malware detection, vulnerability discovery and subsequent patching.[139] In terms of technical infrastructure, Ukrainian government and embassy websites were included into Google's Project Shield, a software protecting websites against Distributed Denial of Service (DDoS) attacks, which are intended to overload servers and subsequently prevent access to the website.[140] Google also helped the Ukrainian government to set up an air red warning systems for mobile phones and adapted its services with support features for Ukrainian civilians.[141]

4.3.2. Impact

On 17th February 2022, mere days before the launch of the invasion, Ukraine's government decided to migrate its Critical Information Infrastructure (CII), which includes government data and public services, to the cloud.[142] The decision was made with the recognition that until then, government data and online services provided by the state were stored and on servers inside Ukraine that could potentially be destroyed or captured by Russian forces,

[137] Lilly et al., "Business@War," 74.
[138] Walker, "New Ways We're Supporting Ukraine."
[139] Lilly et al., "Business@War," 77.
[140] Walker, "New Ways We're Supporting Ukraine."
[141] Walker.
[142] Lilly et al., "Business@War," 74.

endangering the viability of the Ukrainian state.[143] To prevent this from happening, Ukraine's ambassador to the UK, Vadym Prystaiko met with AWS' Head of Government Digital Transformation Liam Maxwell in London on the day of the invasion to compile a list of important government data.[144] The list included data from multiple ministries, universities and dozens of large private companies such as financial institutions, containing amongst others the "population register, land and property ownership records, tax payment records, bank records, education registries, anti-corruption databases".[145] By 27th February, AWS was delivering the first of its portable so-called 'Snowball' data storage devices to Ukraine, which were used to transfer the data from the list.[146] During the first months of the invasion, the 'snowballs' transferred over 10 petabytes of data to AWS cloud servers around the world, essentially distributing the digital representation of the Ukrainian government across the globe.[147] The absence of any business relationship with Russia meant that the data was not stored or accessible through company assets in Russia.[148] Given the high uncertainty and confusion that marked the initial days of the invasion, a disintegration of the Ukrainian state did not seem unlikely. The capturing, degradation, or destruction of Ukrainian government data on domestic servers would have greatly increased Russia's ability to subdue the Ukrainian state in case its military objectives were achieved. The transfer of Ukrainian government data would have enabled the Ukrainian state to persist digitally and provide services to its citizens despite a physical occupation. Such data is also crucial for the capacity to resist militarily, as for example, the population register is important for the Ukrainian military to conduct its process of drafting personnel from the military-age male

[143] Mitchell, "How Amazon Put Ukraine's 'Government in a Box' — and Saved Its Economy from Russia."
[144] Mitchell.
[145] Mitchell.
[146] Lilly et al., "Business@War," 73.
[147] Lilly et al., 73.
[148] Mitchell, "How Amazon Put Ukraine's 'Government in a Box' — and Saved Its Economy from Russia."

population. According to Microsoft's CEO Brad Smith (2022), the Russian military intentionally targeted Ukrainian governmental data centers with cruise missiles.[149] The fact that analysts have determined both kinetic and cyberattacks by Russia against Ukrainian data centers have had little strategic impact on the war emphasizes the value of this cloud migration effort.[150] Deputy Prime Minister Fedorov would later even publicly state that "Amazon AWS literally saved our digital infrastructure".[151] To maintain the operability of the Ukrainian state apparatus, Google also allowed Ukrainian government officials to work and communicate securely and in a distributed manner through the free provision of its cloud-based Workspace service.[152] Microsoft has also provided Microsoft Cloud services to the Ukrainian government free of charge throughout 2022 and 2023.[153] Microsoft also reported on its cloud services being offered to major Ukrainian food and energy companies, which through the ability of cloud-based remote-work were able to maintain business continuity in critical fields of the Ukrainian economy.[154]

The cyber domain of the Russian invasion of Ukraine has been commented on widely since the start of the invasion. There is no doubt, that the cyberspace activity associated with this war has been immense. Cyber security company Mandiant (owned by Google Cloud) registered "more destructive cyber attacks in Ukraine during the first four months of 2022 than in the previous eight years with attacks peaking around the start of the invasion".[155] The first Russian strike against Ukraine was not launched kinetically on 24th February, but by a wiper malware termed FoxBlade on 23rd February, according to Smith (2022).[156] The

[149] Smith, "Defending Ukraine: Early Lessons from the Cyber War," 2.
[150] Burgan, "Ukraine Data Centers Became Physical Targets When Cyberattacks Failed."
[151] Amazon, "How Amazon Is Assisting in Ukraine."
[152] Walker, "New Ways We're Supporting Ukraine."
[153] Microsoft, "How Technology Helped Ukraine Resist during Wartime."
[154] Microsoft.
[155] Huntley, "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape."
[156] Microsoft, "Defending Ukraine: Early Lessons from the Cyber War.," 1.

malware was targeting multiple government agencies and critical infrastructures and was supposed to destroy data from these organization's computers.[157] Employees from Microsoft's Threat Intelligence Center (MSTIC) were the first to discover the malware.[158] Already in January, the MSTIC started detecting malware in Ukrainian networks and proceeded to inform the Ukrainian government about their presence before publishing their findings.[159] Since then, Microsoft has regularly published its efforts against disruptive cyber campaigns against Ukrainian networks and infrastructure, often directly attributing these attacks to Russian state institutions or organizations associated with these institutions. On 7th April 2022, Microsoft reported on its disruptive actions against a hacker group called Strontium which Microsoft associates with the Russian military intelligence service (GRU), which had been targeting Ukrainian government and media institutions.[160] On 27th April 2022, Microsoft's Digital Security Unit published a special report on Russia's cyberattack activity in Ukraine, providing a week-by-week list of destructive cyberattacks of the first months of the war, along with a contextualization of kinetic events in the invasion during the same time. The report calculates that 40% of destructive attacks target critical infrastructure organizations in Ukraine, with 32% affecting governmental institutions at all levels.[161] Overall, Mueller et al. (2023) identified 47 attributed cyberattacks by Russia against Ukraine between 21st November 2021 to 9th May 2022, based on Ukrainian government and Microsoft reports, not including attacks that haven't been publicized or detected.[162]

[157] Microsoft, 7.
[158] Microsoft, 7.
[159] Microsoft Digital Security Unit, "Special Report: Ukraine - An Overview of Russia's Cyberattack Activity in Ukraine," 3.
[160] Burt, "Disrupting Cyberattacks Targeting Ukraine."
[161] Microsoft Digital Security Unit, "Special Report: Ukraine - An Overview of Russia's Cyberattack Activity in Ukraine," 4.
[162] Mueller et al., "Cyber Operations during the Russo-Ukrainian War," 7.

Microsoft describes its response as establishing secure communication channels with Ukrainian officials, providing them with real-time intelligence on threats, guidance, and proactive systems updates to install countermeasures against attacks.[163] In June 2022, Microsoft reported that one of two major technical contributions to Ukraine has been software provided to Ukraine free of charge "that identifies and maps organizational attack surfaces, including devices that are unpatched against known vulnerabilities and therefore are the most susceptible to attack".[164] The other contribution being special authorization given to Microsoft by the Ukrainian government to change folder access in Ukrainian networks.[165]

In June, Microsoft reported that it was witnessing a decline in destructive wiper cyberattacks as the second phase of the war shifted Russia's focus to the Donbas.[166] However, in December 2022 Microsoft reported its findings on a resurgence of GRU-associated destructive cyberattacks in late October 2022 against Ukrainian critical infrastructure targets.[167] The cyberattacks were launched in concert with missile and drone attacks on the same targets, as the Russian military was pushed out of occupied territory by the Ukrainian counteroffensives.[168] Google-owned cyber security company Mandiant reported in November 2023, that it had responded to a cyberattack against a critical infrastructure organization in Ukraine which resulted in an unplanned power outage.[169] As the invasion progressed into 2023, Microsoft again reported on a new wiper campaign in January by

[163] Microsoft Digital Security Unit, "Special Report: Ukraine - An Overview of Russia's Cyberattack Activity in Ukraine," 16.
[164] Microsoft Digital Security Unit, 9.
[165] Microsoft Digital Security Unit, 9.
[166] Microsoft Digital Security Unit, 8.
[167] Watts, "Preparing for a Russian Cyber Offensive against Ukraine This Winter."
[168] Watts.
[169] Proska et al., "Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology."

actors associated with Russia, although with significantly smaller impact than previous campaigns.[170]

Measuring the impact of cyber defense efforts on the resilience of Ukraine again comes with challenges. In their discussion around the efficacy of offensive cyber measures in the war, Mueller et al. point out that the utility of offensive cyber operations has mainly manifested itself in intelligence and reconnaissance functions and not as support for kinetic battlefield operations.[171] They point out that the available data to them did not allow whether this effect was determined by the character of cyberspace in general or as a result of defensive cyber capabilities of Ukraine (with the support of multi-national technology companies).[172] While it might not be possible to establish a direct impact of cyber operations on the military operational level, the potential negative effects on the digital infrastructure of governmental institutions, critical infrastructures, and large companies have been clearly documented in many cases, such as the 2022 attack resulting in power outage reported by Mandiant. This suggests that defensive cyber efforts which don't directly affect the situation on the battlefield still contribute the overall resilience, meaning capacity to resist and recover, of the Ukrainian state. In this sense, the support by companies such as Microsoft and Mandiant can be judged to have contributed to that resilience, with an especially high impact during the first, critical phase of the invasion when Russian offensive cyber activity was at its highest point and Ukraine at its most vulnerable.

The integral role of digital technology infrastructure in this war became visible in another case of technology company support to Ukraine. Google's navigation software Google Maps once again played a role in the war that had been going on since 2014. In the years before

[170] Burt, "Disrupting Cyberattacks Targeting Ukraine."
[171] Mueller et al., "Cyber Operations during the Russo-Ukrainian War," 7.
[172] Mueller et al., 7–8.

the invasion, Google found itself under criticism by Western governments for altering the border demarcation around Crimea in different versions of Google Maps. Six weeks after disguised Russian troops invaded the peninsula in 2014, the Russian version of Google Maps indicated that Crimea was now Russian territory.[173] Dominating the global digital mapping market with an 80% market share, this meant that Google Maps displayed geopolitical facts.[174] In the early days of the Russian invasion in February 2022, Google seemed inclined to rectify its stance: After consulting with Ukrainian authorities, Google switched off the live traffic feature of Maps which indicates traffic jams based on anonymized user location data.[175] The rationale behind that was the discovery, that Google Maps could be used as an open-source intelligence tool to determine troop and refugee movements. Even before President Putin officially announced the invasion of Russian troops into Ukraine on 24th February, American researchers were able to track what turned out to effectively be Russian troop columns on the way from Belgorod, following the beginning of the invasion in real-time.[176] If this technology could be used for this purpose by researchers, the fear was that the Russian military could start to use the same technique to identify and target traffic jams of Ukrainians fleeing from the invading forces.[177] Disabling the function prevented the Russian military from utilizing it and thereby protected Ukrainian civilians and possibly Ukrainian troop movements.

By early March 2022, Google also obliged to Ukrainian authorities' bid to publish an air raid warning system for Ukrainian users' mobile phones.[178] This was significant, as this air raid warnings originating from the Ukrainian government could now leverage the ubiquitousness

[173] Katz, "Why a Russian Invasion of Ukraine Would Be a Big Test for Google Maps."
[174] Katz.
[175] Cieslak and Gerken, "Ukraine Crisis: Google Maps Live Traffic Data Turned off in Country."
[176] Paleja, "How Did Google Maps' Traffic Data Become a Tool for the Ukraine War?"
[177] Cieslak and Gerken, "Ukraine Crisis: Google Maps Live Traffic Data Turned off in Country."
[178] Walker, "Helping Ukraine."

of Google's Android mobile operating system, which at the time of the start of the invasion was running on over 80% of Ukrainian mobile phones.[179] Leveraging the existing market share of its products, Google was able to provide Ukraine with additional protection for its civilians from Russian attacks.

The cases of support to Ukraine from these companies showcase the character of dual-use, digital infrastructure support well. Not only were these companies able to provide support help to Ukraine much faster than any government at the time through informal channels.[180] Mostly invisible to the naked eye, their impact extends to the strategic level of war rather than the operational. Cloud migration, critical infrastructure protection through cyber defense, and the leveraging of existing technical infrastructure describe more subtle forms of Slaughter's concept of resilience. Integral to their impact is also their effect through time: Many of these services such as disabling live traffic on Google Maps and migrating the Ukrainian government to the cloud were most needed and effective in the first weeks of the invasion, when the survival of the Ukrainian state was at its greatest risk and Western military kit hadn't arrived yet. But their effects continue to persist throughout time, as can be seen with the cyber defense provided to Ukraine by companies such as Microsoft and Mandiant. But the changing character of the war, from air landing operations and armored assaults towards more static fronts in combination with long-range strikes against civilian infrastructure targets, also means that the significance of some of this support becomes less visible and harder to assess because the overall resilience of Ukraine is now measured in military success on the Eastern and Southern fronts rather than pure survival of the state.

[179] StatCounter, "Mobile Operating System Market Share Ukraine."
[180] Fox and Probasco, "Volunteer Force," 2.

And military success in this sense results from military capabilities such as weapon systems and troop numbers rather than civilian digital infrastructure.

4.4. Russia

After looking into the Ukrainian side of 'Big Tech' support during the invasion, the same investigation was to be conducted on which support was offered by ICT companies to Russia. But here the picture is very different. First of all, when looking at the biggest and highest valued ICT companies in the world, almost all of these firms happen to be American.[181] Not a single Russian public ICT company features in the top 100 most valuable global companies.[182] While this already hints that less resources would be available for such private support to the Russian war effort, it is still worth investigating how some of Russia's most significant ICT companies behaved towards the Russian government during the war, namely Yandex and Kaspersky. But just as most of the technology company support provided to Ukraine stems from companies of allied companies and not domestic champions, it was also investigated how companies from countries friendly to Russia supported the Russian government. Based on the research, the impact of this support on the Russian war effort was assessed by putting it into context with the Russian military strategy throughout the invasion until December 2023. It has to be stressed that for the research for this sub-chapter, only English language sources were considered.

[181] CompaniesMarketCap.com, "Largest Companies by Market Cap."
[182] CompaniesMarketCap.com.

4.4.1. Actions

Yandex LLC., also referred to as 'Russia's Google', was once seen as the poster child of an emerging Russian digital technology sector.[183] After its foundation in 1997 it was one of the first independent Russian internet companies and managed to build a dominant market position over the years, representing the third biggest web search engine in the world after Google and Bing.[184] It also developed prominent ride-hailing and e-commerce platforms.[185] In Russia, Yandex web search engine dominates the market with processing around 70% of web searches in the country.[186] It also remains by far Russia's highest valued internet company in 2024.[187] As early as 2008, around the time of the Russian invasion into Georgia, Yandex experienced increasing attempts of influence by Kremlin, a situation its owners had tried to anticipate by registering the company in the Netherlands a year earlier.[188] Russian authorities demanded that Yandex displayed only results approved by the Kremlin in its search engine, and in 2009 acquired a decisive stake in the business after being declared an asset of national importance by the government.[189] Since then, Yandex saw its platform become more and more politicized as Kremlin influence grew, especially with regards to the negative portrayal of domestic political opposition.[190] With the onset of the Russian invasion of Ukraine in February 2022, Yandex now faced additional pressure both from Western sanctions and new Russian 'disinformation' laws which threatened its economic viability.[191] This ultimately resulted in the companies' co-founder and CEO Arkady Volozh resignation

[183] Reuters, "In Biggest Corporate Exit since Ukraine War, Search Engine Yandex's Owner to Leave Russia in $5.2 Billion Deal."
[184] StatCounter, "Search Engine Market Share Worldwide."
[185] Beri, "The World's Third Most Used Search Engine, Yandex, Is up on Sale."
[186] Kravets-Meinke, "The Sad Fate of Yandex: From Independent Tech Startup to Kremlin Propaganda Tool."
[187] Statista, "Leading Internet Companies in Russia as of February 2024, by Value."
[188] Kravets-Meinke, "The Sad Fate of Yandex: From Independent Tech Startup to Kremlin Propaganda Tool."
[189] Kravets-Meinke.
[190] Kravets-Meinke.
[191] Kravets-Meinke.

by June 2022, who the following year publicly voiced his criticism of the invasion.[192] Finally, in February 2024, the Dutch holding company of Yandex divested its Russian assets, comprising amongst others of the search engine services, in a $5.21 billion deal to a fund owned by Russian state companies.[193]

Kaspersky Lab Inc. is another globally renown Russian ICT company that offers cyber security services to private individuals, companies, and public institutions. Its relationship with the Kremlin has been similarly complicated as Yandex', but some notable differences exist. As Russia's sixth most valued ICT company,[194] Kaspersky's antivirus software has made it to the devices of millions of users worldwide, including in Western countries. But due to the sensitive nature of its product, along with the Russian emphasis on cyber operations as part of a wider hybrid warfare approach in the years preceding the full-scale invasion of Ukraine, the company has struggled to rid itself of Western suspicions regarding ties to Russian intelligence and security services.[195] A 2015 Bloomberg article criticized the company for filling senior management positions with former security services officials, which was later denied by the company's founder and CEO Eugene Kaspersky.[196] Yet in 2017, the U.S. government took the step to exclude Kaspersky software from its networks due to national security concerns resulting from the company's suspected ties to the Kremlin.[197] At the start of the invasion, Kaspersky was trying to navigate the political tightrope as a Russian firm with an international customer base. This saw Eugene Kaspersky term the unfolding invasion as "the situation in Ukraine",[198] drawing widespread

[192] Kravets-Meinke.
[193] Reuters, "In Biggest Corporate Exit since Ukraine War, Search Engine Yandex's Owner to Leave Russia in $5.2 Billion Deal."
[194] Statista, "Leading Internet Companies in Russia as of February 2024, by Value."
[195] Vicens, "Can Kaspersky Survive the Ukraine War?"
[196] Matlack, Riley, and Robertson, "The Company Securing Your Internet Has Close Ties to Russian Spies."
[197] Baker, "US Bans Kaspersky Software for Alleged Russian Links."
[198] Lapienytė, "Kaspersky Neutral Stance in Doubt as It Shields Kremlin."

condemnation from the non-Russian cyber security sector. On 1st March 2022, cyber security researchers discovered that Russian governmental websites, including the Ministry of Defense which was under attack from cyber activists at the time, were protected from DDoS attacks by Kaspersky software.[199] Then in late April 2024, researchers from open-source intelligence collective InformNapalm released the content of a 100GB stash of data from a Russian company which cooperated with Kaspersky on the development of neural networks for UAVs with dual-use potential since 2018 and after the start of the 2022 invasion.[200] Kaspersky responded to this publication by denying the accusation, claiming that the cooperation only occurred at the lab level and was conducted for purely humanitarian purposes.[201]

As Ukraine's biggest private digital infrastructure support stems from foreign companies, it is necessary to determine how ICT companies from countries friendly to Russia have supported Russia. Of the countries that can be assumed close allies of Russia,[202] none boast a significant ICT sector other than China. But just as their government, Chinese tech multinationals have been wary of providing overt concrete support to Russia's invasion of Ukraine. The pattern that has instead been observable, differs from the one regarding the Ukrainian side. Russia's relationship with Chinese companies revolves mainly around business contracts which concern the provision of high-tech dual-use components needed for the manufacturing of weapons and drones.[203] This markedly differs from the provision of digital infrastructure by Western multinationals to Ukraine on a voluntary and sometimes even cost-free basis. Ukrainian IT infrastructure and telecommunication networks exhibit a

[199] Lapienytė.
[200] InformNapalm, "AlabugaLeaks. Part 2: Kaspersky Lab and Neural Networks for Russian Military Drones."
[201] Vigliarolo, "Kaspersky Hits Back at Claims Its AI Helped Russia Develop Military Drone Systems."
[202] Allik, "Stand by Me? Vladimir Putin's Remaining Allies."
[203] Sher, "Behind the Scenes: China's Increasing Role in Russia's Defense Industry."

strong dependence on Chinese components manufactured by Huawei and ZTE, who were central to Ukraine's rollout of 3G, 4G and 5G telecommunication networks before the war.[204] Despite this vulnerability, the research for this thesis yielded no publicly available evidence that Chinese tech companies compromised their infrastructure in Ukraine or provided backdoor access to support Russia. This is in line with China's general caution regarding the open support of Russia. It also can be interpreted as a bi-product of the close public-private relationship that exists especially in the Chinese technology ecosystem of civil-military fusion: Under this concept, the Chinese government is closely involved with private companies to leverage and transfer private resources and research for policy goals, especially military capabilities.[205] Through this close enmeshment of the private and public sphere, the Chinese Communist Party (CCP) exerts close control over the actions of private companies, especially where they relate to national interests. This presents a stark contrast to the Western system of governance where private companies have much more political independence, enabling unsanctioned support in situations like the Russian invasion of Ukraine. Thus, it is possible to see that 'web actor' support on the Russian side of the war is subjected to 'chessboard actor' government authorization. This is exemplified in the pattern of the Kremlin appropriating existing free-market solutions and bringing them under its more or less direct control, instead of granting companies independence from political influence.[206] When looking more directly at the impact of company actions in the context of the invasion, this concept becomes even more clear.

[204] Runde, "China and Russia Are Closer than Ever. So Why Is Ukraine Relying on Chinese Tech Firms?"
[205] Cary, "How Six Advanced Persistent Threat-Connected Chinese Universities Are Advancing AI Research," 6; Daniels, "CSET Analyses of China's Technology Policies and Ecosystem - The PRC's Domestic Approach," 11.
[206] Kravets-Meinke, "The Sad Fate of Yandex: From Independent Tech Startup to Kremlin Propaganda Tool."

4.4.2. Impact

Until its sale to a Russian fund in February 2024, Yandex was struggling to maintain a semblance of political neutrality as a globally operating internet firm. In June 2023, Yandex was fined a small fine for refusing repeatedly to share information of its users with Russian domestic intelligence agency FSB.[207] Kaspersky's infrastructure efforts to protect Russian government websites from hacktivists' DDoS attacks in the initial stages of the invasion were mostly successful.[208] But despite repeated warnings by the U.S. government, no evidence of Kaspersky providing backdoors of users to the Russian government has been established to this day. The extent of Kaspersky's research and development efforts for UAVs after the beginning of the invasion remain unclear. In both cases of Russian domestic ICT champions, the available data suggests that their impact on the Russian war effort has been minimal.

Unlike Ukraine being able to leverage Google's market domination in areas such as web search and digital mapping, Russia was either not able or unwilling to exploit its IT companies' assets to a significant degree for digital infrastructure support. Its relationship with the ICT sector in the invasion exhibits core differences to that of Ukraine. But these are not necessarily tied to Russia's strategic position. Russia began the invasion strategically conducting an offense as the aggressor. By perceiving war as an instrument of foreign policy, Russia acted in accordance with the classical paradigm of the chessboard view of international politics. The means it uses to prosecute its invasion of Ukraine therefore seemed to primarily be dictated by state-centric chessboard tools. But throughout the invasion, the Russian military found itself in a defensive posture on multiple occasions, for

[207] Reuters, "Russia's Yandex Fined for Refusing to Share User Information with Security Services."
[208] Barrett, "Security News This Week: DDoS Attempts Hit Russia as Ukraine Conflict Intensifies."

example during the Ukrainian counteroffensives in late 2022 and in the summer of 2023. As a consequence, resilience started to become an issue for the Russian government.

While Russia did not primarily look to tech companies for voluntary help, its war effort is nevertheless dependent on ICT to a significant extent. Despite being largely de facto state-owned,[209] the Russian defense industry just like any other national defense industry relies on a complex external supply chain of electronic components to manufacture sophisticated weapons such as precision-guided missiles, as well as communication systems and electronic warfare systems. These components often originate from the consumer electronics market, which is dominated by private companies.[210] Analyzing 27 modern Russian military systems, Byrne et al. (2022) found that more than 450 components were sourced from outside Russia.[211] They also found that only some of these components were sourced from China, while many of them originated from Europe and the United States.[212] Since the beginning of the full-scale invasion, Western export controls have made it more difficult but far from impossible for the Russian defense industry to acquire these components. In addition to lackluster implementation of export controls,[213] Russia is relying heavily on China to either directly or indirectly supply it with critical technological components. According to calculations by Sher (2024), China exports dual-use goods for military production in excess of $300 million to Russia on a monthly basis.[214] While China maintains that the exports of these goods which are subjected to Western sanctions, have been made my private companies and not on order by the state, the aforementioned deep enmeshment of the CCP in Chinese companies casts doubt on these claims.[215] This means even where

[209] Luzin, "Russia's Defense Industry and Its Influence on Policy: Stuck in a Redistributive Feedback Loop."
[210] Mackinnon, "Russia's War Machine Runs on Western Parts."
[211] Byrne et al., "Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine," 5.
[212] Byrne et al., 10, 13–14.
[213] Mackinnon, "Russia's War Machine Runs on Western Parts."
[214] Sher, "Behind the Scenes: China's Increasing Role in Russia's Defense Industry."
[215] Sher.

private companies are involved in the support of the Russian war effort, involvement by the government of these companies remains highly likely, especially in the case of China, Russia's most important supplier of dual-use components for military production.[216] Chinese customs data demonstrates that the longer the full-scale invasion progressed, the more Russia's dependence on these Chinese imports grew in the absence of domestic supply chains, reaching 89% in 2023 according to calculations by Sher.[217]

But Russia is also relying on private tech companies in a different strategic area of the war. U.S.-based social media platforms such as Facebook and *X* (formerly Twitter) have been used by Russian actors to spread Russian narratives about the invasion. While many of these companies such as Meta, the parent company of Facebook, have voluntarily made efforts to curb the spread of Russian disinformation campaigns, these campaigns continue to persist and expand their reach.[218] For example, Russian influence operations thrived on Facebook using advertisements in the context of the European parliamentary elections in June 2024.[219] A 2023 study by the European Commission showed that the degradation of safety standards of *X* as a result of owner Elon Musk's approach to online freedom of speech has resulted in an increased reach and influence of Russian online disinformation campaigns against Ukraine.[220] Vera Jourova, the European Commission's vice president publicly named *X* as "the platform with the largest ratio of misinformation or disinformation posts".[221]

[216] Sher.
[217] Sher.
[218] Menn, "Musk's New Twitter Policies Helped Spread Russian Propaganda, E.U. Says."
[219] Goujard, "Big, Bold and Unchecked: Russian Influence Operation Thrives on Facebook."
[220] Menn, "Musk's New Twitter Policies Helped Spread Russian Propaganda, E.U. Says."
[221] Carter, "Elon Musk's X Is Being Used as a Key 'weapon of Mass Manipulation' for Russian Disinformation, the EU Says, and Warns It Is 'Watching' the Social Network."

In countries like Slovakia, Russia is able to pursue its online influence operations successfully via its embassy's Facebook page and other social media platforms.[222] These activities ramped up drastically before the Slovakian general elections in September 2023, which saw Robert Fico become prime minister.[223] Fico has become infamous for his Russia-friendly stance and has been actively trying to undermine his country's and NATO's support for Ukraine.[224] But Slovakia is not the only NATO country where Russian online influence has been observed to have considerable impact. A 2024 Washington Post investigation showed that Russia undertook a significant online influence operation on U.S. social media platform while the U.S. Congress was debating a billion-dollar aid package to Ukraine.[225] The crucial aid package proceeded to be stuck in Congress for months until its ultimate sign-off. While the direct impact of these campaigns is hard to measure, they certainly can't be ignored. Ukraine remains heavily dependent on Western public and political support to maintain its resistance against the invasion. Shifts in public perception shaped by disinformation efforts threaten this support and could yield detrimental effects for the Ukrainian war effort. Whether through negligence or intentional lowering of content moderation standards, Western social media platforms hold great sway over this domain of strategic communication as vessels for public discourse in the democratic countries that support Ukraine. They might not actively intend to support Russia, but they can inadvertently end up doing so nevertheless.

Chinese social media platforms on the other hand leave Russian narratives in relation to the war mostly unmoderated. Especially during the first months of the invasion, these narratives

[222] Hajdari, "Russian Embassy in Slovakia Uses Facebook to Push Propaganda. Why Are so Many Slovaks Buying It?"
[223] Sauvage, "Slovakia Swamped by Disinformation Ahead of Parliamentary Elections."
[224] Odarchenko, "Slovak Vote Shows Need for NATO Action on Russian Disinformation."
[225] Belton and Menn, "Russian Trolls Target U.S. Support for Ukraine, Kremlin Documents Show."

found their way around massive platforms with hundreds of millions of users such as WeChat, Weibo, and Douyin through state officials, influencers, and direct adoption of Russian state media reports.[226] In a cross-platform analysis of Chinese social media discourse on the Russian invasion of Ukraine, Rogers & Zhang (2024) find that the framing of the war differs between Chinese platforms but overlaps on themes that generally follow the CCP's foreign policy from before the full-scale invasion.[227] This suggests that the spread of Russian narratives in Chinese social media isn't as relevant for Russia as the spread of its narratives in Western social media, where public opinion more directly affects policymakers.

After catastrophic blunders in the first, mobile phases of the war, Russia bets on its capacity to both maintain military pressure on the frontlines as well as its capacity to degrade Ukraine's base of political and military support, in what has increasingly become a war of attrition. The former capacity relies in part on the supply of dual-use components for military production purposes while the latter includes disseminating political narratives in Western public discourse. As was shown above, ICT companies play a key role in sustaining the resilience of Russia's war effort. Yet their agency with regard to Russia largely differs from that towards Ukraine. Russia either pursues the import of critical manufacturing components along governmental relations with friendly countries or exploits the existing liberal ecosystem of Western ICT companies for state-led strategic communication. In both cases, it perceives the war primarily through a chessboard lens. While the war is still ongoing, and no reliable predictions about its outcome can be made, it is noteworthy that following

[226] Yang, "How Russian Propaganda Dominates Chinese Social Media"; White, "China's Tech Platforms Become Propaganda Tools in Putin's War."
[227] Rogers and Zhang, "The Russia–Ukraine War in Chinese Social Media."

Ukraine's unsuccessful summer offensive of 2023, Russia's approach has resulted in what Western analysts deem a strategic advantage going into 2024.[228]

5. Discussion

This thesis dealt with two main research problems: The first was to describe how the involvement of big ICT companies shapes the Russian invasion of Ukraine. The second one was led by Slaughter's theory of strategic interconnection and aimed to determine whether countries which obtain the support of such companies have a strategic advantage in armed conflicts over the countries which don't have access to this support. With regards to the second research problem, two hypotheses were generated from the theory, with H1 assuming that *Big Tech involvement has had significant influence on Ukraine's capacity to resist the Russian invasion*, and H2 assuming that *Russia's role as the aggressor means it doesn't have to rely on independent ICT companies to support its war effort.*

Regarding the first research question, the analysis was able to demonstrate that ICT companies have played a significant role in this war. Especially on the Ukrainian side, these companies provide a myriad of services from broadband internet connection, over targeting data analysis and integration, cloud services, and technical infrastructure, to providing cyber threat intelligence and the defense of digital networks and assets. As some of these companies belong to the biggest in the world and their products form an integral part of civilian and even military infrastructure, their actions or inactions have significant effects.

This becomes clearer when looking at how the analysis relates to the second research question. With regards to the first hypothesis, the analysis supports the assumption that the

[228] For examples see Gressel, "Ukraine's Survival: Three Scenarios for the War in 2024"; Willasey-Wilsey, "What Lies Ahead for the War in Ukraine in 2024?"

involvement of big ICT companies has significantly impacted Ukraine's capacity to resist the Russian invasion. Rushing to Ukraine's side in the first days of the invasion and even before, their actions can be said to have had a direct effect on both the battlefield and the wider strategic picture in favor of Ukraine. Their services helped Ukraine survive as a state in case of territorial loss and political defeat, maintained the operability of the Ukrainian government, kept Ukraine online and connected to the world and on the battlefield, and enabled Ukrainian military operations. Their actions also provided Ukraine with high accuracy targeting, especially in a situation of ammunition inferiority. And even in cases of civilian applications like humanitarian de-mining, they free up capacities for the UAF. In short, it provided Ukraine with distributed (digital) infrastructures that reduced the risk for critical failure and subsequently enhanced the country's capacity to resist external pressure and recover from it. This is in line with Slaughter's claims about the function of defense networks.

But it also has to be noted that the voluntary support by ICT companies comes with some important caveats: Companies are private actors that generally don't act out of the goodness of their hearts or political ideals. Economical motives naturally underlie their actions as primarily profit-seeking actors. While this is not problematic in itself, it might have an impact on whether companies come to the aid of a country or not. In the case of a war of aggression, constituting an obvious breach of international law and resulting in public outcry, companies face less costs offering their support to the victim. When the situation is less clear, there might be hesitation from the same executives exposing their companies to significant risk. Economic considerations also mean that their long-term involvement faces challenges. Especially big public companies are subject to the shareholder value principle. They might be incentivized to not uphold their support indefinitely if there's not a significant

return on their investment. Furthermore, the case of Starlink demonstrates the dangers of creating reliance on a company that is subject to the volatility of its executive. A single individual can suddenly make decisions which can impact a whole nation because the country is so reliant on their service. These executives on the other hand can be subjected to pressure or disinformation much easier than a political institution. If a country becomes too dependent on a service like Starlink, the issue of Slaughter's scale-free networks appears: these networks offer great benefits to the whole network by leveraging strongly connected central nodes. But at the same time, these nodes constitute points of critical failure for the whole network in case they are compromised or cease function. In this regard, Slaughter's concept of defense networks continues to provide relevant guidance to inform the process of increasing Ukraine's resilience.

The analysis has shown that the available data partly supports the second hypothesis. While it was found that Russia emphasizes its state power to a much greater extent than Ukraine, it is indeed relying on independent ICT companies for some purposes. Russia puts great emphasis on attrition and fire superiority, both on the battlefield and in its attacks on civilian infrastructure. Lacking a highly developed technology sector however means that it is reliant on Western and Chinese companies supplying it with high-tech components for military systems manufacturing. Russia is also aware that external political support is vital to the resilience of Ukraine, a support it is trying to degrade by influencing the public discourses in countries allied to Ukraine. For this, Russia conducts influence operations on Western social media platforms with varying degrees of success. While both of these areas highlight Russia's need for resilience, its behavior towards ICT companies differs markedly from that of Ukraine. The Kremlin's approach seems to be either driven by governmental relations, as is the case with pursuing high-tech components through China. Or it exploits business

models and liberal concepts of free speech, as is the case with Western social media platforms. While the West and Ukraine engage with companies under a liberal paradigm, recognizing their agency, Russia engages with them through a state-centric paradigm. Both approaches seem to offer advantages and disadvantages.

Interpreting the results of this analysis, it can be seen that Slaughter's concept of defense networks which rely on distributed infrastructure finds application in Ukraine in the early months of the invasion. By providing distributed networks of (digital) infrastructure, ICT companies enhanced the country's resilience in the context of a military invasion. The findings of Fox & Probasco further demonstrated Slaughter's claim that interconnected non-state actors are able to generate action much faster than governments through informal communication channels and without being hindered by bureaucratic processes.[229] This speed helped Ukrainian resilience at a critical point in time. But as time progresses, this web support seems to become volatile or offers diminishing returns. Some big tech services like cloud migration and disabling certain features in Google Maps had critical value at the onset of the invasion. But their value decreased as the character of the invasion changed. Likewise, other forms of support gained importance when the strategic picture changed in later phases of the war. Starlink internet and Palantir-enabled targeting significantly shifted the battlefield in favor of Ukraine once weapon systems and ammunition from the West arrived in Ukraine *en masse*. But even these assets saw their returns diminished when the conventional warfare balance changed and the UAF began identifying more targets than it had ammunition to fire at. This suggests that chessboard politics came to the foreground again as the tools needed to maintain resilience long-term are more traditionally rooted in the sphere of government, namely the production and employment of weapons and

[229] Fox and Probasco, "Volunteer Force," 1.

ammunition. And even when ICT support is actively providing value to a resistance effort, it most effectively does so not in the absence, but in conjunction with these chessboard tools: Starlink provided essential communication capabilities, but these only translated into resilience because there were troops and equipment to communicate with. MetaConstellation provided exceptional targeting capabilities, but it really translated into battlefield advantages once the UAF was in control of advanced artillery systems capable of hitting the identified targets.

Slaughter's argument that the world needs to be seen in stereo is emphasized by the findings of this thesis. The web and the chessboard exist next to each other and ideally complement each other, especially when it comes to armed conflict. In any way, it is clearly visible that in an increasingly digitalized world, companies that provide civilian dual-use products and services stand to play a more and more critical role even in armed conflict. But while they can provide countries with crucial capabilities and potentially also withdraw them again at a whim, concerns that these companies now have the potential to become harbingers of victory or defeat in armed conflict do not find confirmation in this thesis.

Looking into the future, this raises some important questions. Especially the tensions between China and the U.S. concerning Taiwan have led many commentators to speculate how Western technology companies will behave in a potential armed conflict.[230] Here, the two different approaches towards Big Tech might face a litmus test. Would liberal Western ICT companies voluntarily offer their support against a country harboring a significant part of their business interests? Would the U.S. abandon a liberal public-private partnership approach towards its tech companies and instead subject them to government direction as it did during WWII? Analyzing these questions therefore presents salient opportunities for

[230] See for example Lilly et al., "Business@War"; Fox and Probasco, "Volunteer Force."

further research. Below the threshold of a great power confrontation for example it would also be of great value to investigate what shapes the motivation of these companies to voluntarily offer their support to a conflict party in the first place. A fourth important opportunity for research consists of more closely investigating how the support of these companies changes over time, and how this affects the strategic balance of a conflict as it evolves. The phenomenon of ICT and the companies that provide them in a geopolitical context seems likely to play a greater role in the future as great powers engage in a race for sophisticated technologies. Efforts to understand it better could therefore offer great value to the discipline of geopolitical studies.

Conclusion

This master thesis attempted to enrich the existing literature on ICT company involvement in the Russian invasion of Ukraine with a theory-driven approach. The involvement of these companies has garnered much attention in non-academic publications and has brought with it a considerable amount of hype about their impact on the war. At its core, the thesis assessed two research problems:

First, *"How does the involvement of big ICT companies shape the Russian invasion of Ukraine?"*.

And second, *"Do countries which obtain the support of big ICT companies have a strategic advantage in armed conflicts over the countries which cannot count on their support?"*.

The thesis answered the first research question by describing and analyzing the actions of these companies in the war in a descriptive way. To answer the second research question of

the impact these companies had on the strategic balance of the war, two hypotheses were tested, one relating to the Ukrainian side and one to the Russian side:

H1: The involvement of ICT companies had a significant impact on Ukraine's capacity to resist the Russian invasion.

H2: Russia's role as the aggressor means it doesn't have to rely on independent ICT companies to support its war effort.

The analysis lends support to the first hypothesis, finding that ICT company support has had a significant impact on Ukraine's capacity to resist the Russian invasion by providing crucial capabilities that helped the Ukrainian state to withstand and recover from external military pressure. On the other hand, the analyzed data only partly supported the second hypothesis according to which Russia as the aggressor doesn't need to rely on these non-state actors for its war effort. It was found that Russia does rely on ICT companies, but in a different way, namely, to maintain sophisticated military systems production and to degrade Ukrainian external political and public support. Russia also engages with these companies under a state-centric approach, compared to the more liberal approach of Ukraine that leaves these non-state actors with greater agency.

Situating these research problems within Slaughter's theory of the 'Chessboard' and the 'Web' helped to understand the strategic value these networks of non-state actors can deliver in an armed conflict. It also highlighted its challenges compared to state-owned assets in a domain traditionally dominated by the chessboard logic. Despite being published years before the full-scale Russian invasion and under the context of hybrid warfare, Slaughter's theoretical concepts find application in this conventional interstate conflict. Leveraging networks of actors of the 'web' and structuring them accordingly can indeed increase a

country's resilience. However, over-emphasis of these concepts ignores the pivotal role that traditional instruments of foreign policy continue to play, especially in war. Where web strategy is not supported by chessboard capabilities, it offers diminishing returns. This should be taken into account when attempting to apply these concepts to future cases.

Reaching these conclusions did not come without its limitations and challenges: On the side of data collection, the so-called *fog of war* means that obtaining accurate and useful data becomes a challenge in itself. Much information will either not find its way into the public domain at all due to confidentiality reasons, gets released only much later due to operational security concerns, or cannot be determined at all because of the sheer complexity of the situation. This thesis also almost exclusively considered sources in English at the risk of overseeing potentially relevant Ukrainian or Russian language sources. However, this approach to research was considered justifiable, as the thesis analyzed observable actions by companies and not for example domestic political discourse around these actions. Resorting to secondary sources was thus chosen to mitigate the risk that potentially relevant phenomena were missed as a result of limiting the sources by language.

As was also pointed out repeatedly, assessing the direct impact of many of these technologies on the strategic balance of the war is very difficult. The number of confounders that exist in shaping a war is remarkable, including political and military decisions, armed forces sizes, military capabilities, military structures, force employment, domestic support, and external support, just to name a few. Dissociating the support of these companies from the greater strategic balance presents a major issue that can distort their actual impact. This becomes visible when considering how the dimension of time seems to influence the interpretation of findings. Setting the cut-off date at the end of 2022 would mean that the impact of technology company support is only measured in the short-term, yielding an outsized impact compared

to observing it until the end of 2023. While the hypotheses around Slaughter's theory find support in the data, this support might vary when looking at a different selection of case studies. To this end, exploring further case studies would contribute greatly to the understanding of the phenomenon at hand. To provide more insight into *why* ICT company support gets generated, it would also be of great value to further assess the formal and especially informal relationships that exist between government and these companies to inform scholarly understanding of how independent companies actually are under such circumstances.

What this thesis was nevertheless able to do was to provide a theory-led perspective that takes non-state 'web' actors seriously, in a domain which for a long time was conceived exclusively in chessboard terms. Observing the existence and performance of distributed defense networks not only in hybrid warfare, but full-on interstate war raises awareness to the level of importance that digital technology companies have gained in today's world. This thesis was able to demonstrate that these companies have become actors that cannot be ignored by states any longer in matters of war, whether by the defender's or the aggressor's side.

List of References

Allik, Henry-Laur. “Stand by Me? Vladimir Putin’s Remaining Allies.” *Deutsche Welle (DW)*, June 20, 2024. https://www.dw.com/en/stand-by-me-vladimir-putins-remaining-allies/a-69428963.

Amazon. “How Amazon Is Assisting in Ukraine.” *About Amazon* (blog), June 21, 2023. https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine.

Armed Forces of Ukraine. “Ukrainian Armed Force Use Skykit Palantir.” *Mil.in.Ua* (blog), February 16, 2023. https://mil.in.ua/en/news/ukrainian-armed-force-use-skykit-palantir/.

Baker, Graeme. “US Bans Kaspersky Software for Alleged Russian Links.” *BBC News*, June 20, 2024. https://www.bbc.com/news/articles/ceqq7663wd2o.

Baran, Paul. “On Distributed Communications: I. Introduction to Distributed Communications Networks.” RAND Corporation, 1964. https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf.

Barrett, Brian. “Security News This Week: DDoS Attempts Hit Russia as Ukraine Conflict Intensifies.” *Wired* (blog), February 26, 2022. https://www.wired.com/story/russia-ukraine-ddos-nft-nsa-security-news/.

Bateman, Jon. “Russia’s Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications.” Working Paper. Cyber Conflict in the Russia-Ukraine War. Washington, D.C: Carnegie Endowment for International Peace, December 16, 2022. https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications?lang=en.

BBC. “Ukraine: What Are Himars Missiles and Are They Changing the War?,” August 30, 2022. https://www.bbc.com/news/world-62512681.

Beaty, Thalia, and The Associated Press. “Microsoft Tops the List of Largest Private Donors to Ukraine with $430 Million—but Google Also Made the Cut.” *Fortune*, February 23, 2023. https://fortune.com/europe/2023/02/23/ukraine-war-top-private-donors-microsoft-google/.

Belton, Catherine, and Joseph Menn. “Russian Trolls Target U.S. Support for Ukraine, Kremlin Documents Show.” *The Washington Post*, August 4, 2024. https://www.washingtonpost.com/world/2024/04/08/russia-propaganda-us-ukraine/.

Bergengruen, Vera. “How Tech Giants Turned Ukraine Into an AI War Lab.” *Time Magazine*, August 2, 2024. https://time.com/6691662/ai-ukraine-war-palantir/.

———. “Ukraine Is Using AI to Help Clear Millions of Russian Landmines.” *Time Magazine*, February 11, 2023. https://time.com/6330445/demining-ukraine/.

Beri, Devesh. “The World’s Third Most Used Search Engine, Yandex, Is up on Sale.” *MS PowerUser* (blog), May 2, 2024. https://mspoweruser.com/the-worlds-third-most-used-search-engine-yandex-is-up-on-sale/.

Burgan, Kate. “Ukraine Data Centers Became Physical Targets When Cyberattacks Failed.” *MeriTalk* (blog), November 22, 2022. https://www.meritalk.com/articles/ukraine-data-centers-became-physical-targets-when-cyber-attacks-failed/.

Burt, Tom. “Disrupting Cyberattacks Targeting Ukraine.” *Microsoft - On The Issues* (blog), July 4, 2022. https://blogs.microsoft.com/on-the-issues/2022/04/07/cyberattacks-ukraine-strontium-russia/.

Byrne, James, Gary Somerville, Joe Byrne, Jack Watling, Nick Reynolds, and Jane Baker. “Silicon Lifeline: Western Electronics at the Heart of Russia’s War Machine.” Royal United Services Institute (RUSI), August 8, 2022. https://www.rusi.org/explore-our-research/publications/special-resources/silicon-lifeline-western-electronics-heart-russias-war-machine.

Carter, Tom. “Elon Musk’s X Is Being Used as a Key ‘weapon of Mass Manipulation’ for Russian Disinformation, the EU Says, and Warns It Is ‘Watching’ the Social Network.” *Business Insider*, September 27, 2023. https://www.businessinsider.com/elon-musks-x-most-active-platform-for-russian-disinformation-2023-9.

Cary, Dakota. “How Six Advanced Persistent Threat-Connected Chinese Universities Are Advancing AI Research.” CSET Issue Brief. Center for Security and Emerging Technology, March 2021.

Cieslak, Marc, and Tom Gerken. “Ukraine Crisis: Google Maps Live Traffic Data Turned off in Country.” *BBC News*, February 28, 2022. https://www.bbc.com/news/technology-60561089.

CompaniesMarketCap.com. “Largest Companies by Market Cap.” CompaniesMarketCap.com, June 18, 2024. https://companiesmarketcap.com/.

Copp, Tara. “Elon Musk’s Refusal to Provide Starlink Support for Ukraine Attack in Crimea Raises Questions for Pentagon.” *PBS*, November 9, 2023. https://www.pbs.org/newshour/economy/elon-musks-refusal-to-provide-starlink-support-for-ukraine-attack-in-crimea-raises-questions-for-pentagon.

Daniels, Owen J. “CSET Analyses of China’s Technology Policies and Ecosystem - The PRC’s Domestic Approach.” Policy Brief. Center for Security and Emerging Technology, September 2023. https://cset.georgetown.edu/publication/the-prcs-domestic-approach/.

Dastin, Jeffrey. “Ukraine Is Using Palantir’s Software for ‘targeting,’ CEO Says.” *Reuters*, February 2, 2023, sec. Technology. https://www.reuters.com/technology/ukraine-is-using-palantirs-software-targeting-ceo-says-2023-02-02/.

Donnelly, Jack. *Realism and International Relations*. 1st ed. Cambridge University Press, 2000. https://doi.org/10.1017/CBO9780511612510.

Douro, Morgan. "MLRS and the Totality of the Battlefield." Commentary. Royal United Services Institute (RUSI), February 21, 2023. https://rusi.org/explore-our-research/publications/commentary/mlrs-and-totality-battlefield.

Dress, Brad. "How Elon Musk Became a Power Player in the Ukraine War." *The Hill*, September 13, 2023. https://thehill.com/policy/defense/4200944-how-elon-musk-become-a-power-player-in-the-ukraine-war/.

Ero, Comfort. "Tech Companies Are Fighting for Ukraine. But Will They Help Save Lives in Other Global Conflicts?" *Digital Front Lines* (blog), September 6, 2023. https://digitalfrontlines.io/2023/06/09/tech-companies-are-fighting-for-ukraine/.

European Commission. "White Paper - How to Master Europe's Digital Infrastructure Needs?" European Commission, February 21, 2024. https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs.

European Parliament, and The Council of the European Union. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Pub. L. No. Directive (EU) 2022/2557 (n.d.). https://eur-lex.europa.eu/eli/dir/2022/2557/oj.

Folk, Zachary. "Russia Using Starlink Terminals Bought On 'Open Market' In Ukraine War, Report Says." *Forbes*, February 15, 2024. https://www.forbes.com/sites/zacharyfolk/2024/02/15/russia-using-starlink-terminals-bought-on-open-market-in-ukraine-war-report-says/#:~:text=Since%20the%20war%20began%2C%20Ukraine,military%20communications%20and%20drone%20strikes.

Foust, Jeff. "SpaceX Worked for Weeks to Begin Starlink Service in Ukraine." *Spacenews* (blog), August 3, 2022. https://spacenews.com/spacex-worked-for-weeks-to-begin-starlink-service-in-ukraine/.

Fox, Amos C. "The Russo-Ukrainian War: A Strategic Assessment Two Years Into the Conflict." Land Warfare Paper. Association of the United States Army, February 2024. https://www.ausa.org/publications/russo-ukrainian-war-strategic-assessment-two-years-conflict.

Fox, Christine, and Emelia Probasco. "Volunteer Force." Center for Security and Emerging Technology, May 2023. https://doi.org/10.51593/20230015.

Franke, Ulrike, and Jenny Söderström. "Star Tech Enterprise: Emerging Technologies in Russia's War on Ukraine." Policy Brief. European Council on Foreign Relations, May 9, 2023. https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-war-on-ukraine/.

Freund, Alexander. “Ukraine Using Starlink for Drone Strikes.” *Deutsche Welle (DW)*, March 27, 2022. https://www.dw.com/en/ukraine-is-using-elon-musks-starlink-for-drone-strikes/a-61270528.

Gady, Franz-Stefan, and Michael Kofman. “Making Attrition Work: A Viable Theory of Victory for Ukraine.” International Institute for Strategic Studies (IISS), September 2, 2024. https://www.iiss.org/en/online-analysis/survival-online/2024/01/making-attrition-work-a-viable-theory-of-victory-for-ukraine/.

Gerring, John, and Dino Christenson. *Applied Social Science Methodology: An Introductory Guide*. 1st ed. Cambridge University Press, 2017.

Giles, Keir. “Tech Giants Hold Huge Sway in Matters of War, Life and Death. That Should Concern Us All.” *The Guardian*, September 12, 2023. https://www.theguardian.com/commentisfree/2023/sep/12/tech-giants-war-elon-musk-ukraine-starlink.

Glantz, Mary. “How Ukraine’s Counteroffensives Managed to Break the War’s Stalemate,” September 19, 2022. https://www.usip.org/publications/2022/09/how-ukraines-counteroffensives-managed-break-wars-stalemate.

Goujard, Clothilde. “Big, Bold and Unchecked: Russian Influence Operation Thrives on Facebook.” *Politico*, April 17, 2024. https://www.politico.eu/article/russia-influence-hackers-social-media-facebok-operation-thriving/.

Greenberg, Andy. “How A ‘Deviant’ Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut.” *Forbes*, August 14, 2013. https://www.forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut/.

Gressel, Gustav. “Ukraine’s Survival: Three Scenarios for the War in 2024.” European Council on Foreign Relations, January 31, 2024. https://ecfr.eu/article/ukraines-survival-three-scenarios-for-the-war-in-2024/.

Grylls, George. “Kyiv Outflanks Analogue Russia with Ammunition from Big Tech.” *The Times*, December 24, 2022. https://www.palantir.com/assets/xrfr7uokpv1b/1Fw2bFxYXmu3RWX7FvssB9/e64d19b6f042bda3d2a61e4fc43ea6ec/TheTimes.pdf.

———. “Ukraine’s Secret Weapon: The £40bn Tech Firm That ‘Found Bin Laden.’” *The Times*, March 29, 2024. https://www.thetimes.com/world/russia-ukraine-war/article/ukraines-secret-weapon-the-40bn-tech-firm-that-found-bin-laden-fg73fb567.

Hajdari, Una. “Russian Embassy in Slovakia Uses Facebook to Push Propaganda. Why Are so Many Slovaks Buying It?” *Euronews.Com*, March 29, 2023. https://www.euronews.com/2023/03/29/russian-embassy-in-slovakia-uses-facebook-to-push-propaganda-why-are-so-many-slovaks-buyin.

Hoffmann, Fabian. “Strategic Stability and the Ukraine War - Implications of Conventional Missile Technologies.” Center for Naval Analyses (CNA), February

2024. https://www.cna.org/reports/2024/02/Strategic-stability-and-the-Ukraine-War.pdf.

Horton, Christine. “Microsoft Creating a Front Line to Help Ukrainian Government.” *Channel Futures* (blog), May 23, 2022. https://www.channelfutures.com/channel-business/microsoft-creating-a-front-line-to-help-ukrainian-government.

Huntley, Shane. “Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape.” *Google Threat Analysis Group* (blog), February 16, 2023. https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/.

Hurska, Alla. “Russian Attacks on Ukrainian Critical Infrastructure Become Hybrid Threat to Europe.” Eurasia Daily Monitor. The Jamestown Foundation, May 14, 2024. https://jamestown.org/program/russian-attacks-on-ukrainian-critical-infrastructure-become-hybrid-threat-to-europe/.

Ignatius, David. “How the Algorithm Tipped the Balance in Ukraine.” *The Washington Post*, December 19, 2022. https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/.

InformNapalm. “AlabugaLeaks. Part 2: Kaspersky Lab and Neural Networks for Russian Military Drones.” *InformNapalm* (blog), April 29, 2024. https://informnapalm.org/en/alabugaleaks-part-2-kaspersky-lab-and-neural-networks-for-russian-military-drones/.

Isaacson, Walter. “‘How Am I in This War?’: The Untold Story of Elon Musk’s Support for Ukraine.” *The Washington Post*, July 9, 2023. https://www.washingtonpost.com/opinions/2023/09/07/elon-musk-starlink-ukraine-russia-invasion/.

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

Katz, Catherine Grace. “Why a Russian Invasion of Ukraine Would Be a Big Test for Google Maps.” *Time Magazine*, February 15, 2022. https://time.com/6148040/google-maps-influences-international-affairs/.

Khurshudyan, Isabelle, Dan Lamothe, Shane Harris, and Paul Sonne. “Ukraine’s Rocket Campaign Reliant on U.S. Precision Targeting, Officials Say.” *The Washington Post*, September 2, 2023. https://www.washingtonpost.com/world/2023/02/09/ukraine-himars-rocket-artillery-russia/.

Khurshudyan, Isabelle, Paul Sonne, Serhiy Morgunov, and Kamila Hrbachuk. “Inside the Ukrainian Counteroffensive That Shocked Putin and Reshaped the War.” *The Washington Post*, December 29, 2022.

https://www.washingtonpost.com/world/2022/12/29/ukraine-offensive-kharkiv-kherson-donetsk/.

Kravets-Meinke, Daria. “The Sad Fate of Yandex: From Independent Tech Startup to Kremlin Propaganda Tool.” ZOiS Spotlight. Zentrum für Osteuropa- und internationale Studien, May 15, 2024. https://www.zois-berlin.de/en/publications/zois-spotlight/the-sad-fate-of-yandex-from-independent-tech-startup-to-kremlin-propaganda-tool.

Lapienytė, Jurgita. “Kaspersky Neutral Stance in Doubt as It Shields Kremlin.” *Cybernews* (blog), March 30, 2022. https://cybernews.com/security/kaspersky-neutral-stance-in-doubt-as-it-shields-kremlin/.

Lawson, Aidan, and June Rhee. “Usage of the Defense Production Act throughout History and to Combat COVID-19.” *Yale School of Managment* (blog), March 6, 2020. https://som.yale.edu/blog/usage-of-the-defense-production-act-throughout-history-and-to-combat-covid-19#:~:text=5710%2C%205729).,government%20contracts%20for%20national%20defense.

Lilly, Bilyana, Kenneth Geers, Greg Rattray, and Robert Koch. “Business@War: The IT Companies Helping to Defend Ukraine.” In *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, 71–83. Tallinn, Estonia: IEEE, 2023. https://doi.org/10.23919/CyCon58705.2023.10181980.

Luzin, Pavel. “Russia’s Defense Industry and Its Influence on Policy: Stuck in a Redistributive Feedback Loop.” *Russia Matters* (blog), March 11, 2021. https://www.russiamatters.org/analysis/russias-defense-industry-and-its-influence-policy-stuck-redistributive-feedback-loop.

Maçães, Bruno. “How Palantir Is Shaping the Future of Warfare.” *Time Magazine*, October 7, 2023. https://time.com/6293398/palantir-future-of-warfare-ukraine/.

Mackinnon, Amy. “Russia’s War Machine Runs on Western Parts.” *Foreign Policy*, February 22, 2024. https://foreignpolicy.com/2024/02/22/russia-sanctions-weapons-ukraine-war-military-semiconductors/.

Marquardt, Alex. “Exclusive: Musk’s SpaceX Says It Can No Longer Pay for Critical Satellite Services in Ukraine, Asks Pentagon to Pick up the Tab.” *CNN*, October 14, 2022. https://edition.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html.

Marson, James, and Thomas Grove. “Russia Using Thousands of Musk’s Starlink Systems in War, Ukrainian General Says.” *The Wall Street Journal*, February 15, 2024. https://www.wsj.com/world/russia-using-thousands-of-musks-starlink-systems-in-war-ukrainian-general-says-29303242?st=z1ibzrkmiilubzp&reflink=article_copyURL_share.

Martin, Ciaran. “Cyber, MacGyver, and the Limits of Covert Power.” *Lawfare* (blog), March 6, 2024. https://www.lawfaremedia.org/article/cyber--macgyver--and-the-limits-of-covert-power.

Matlack, Carol, Michael Riley, and Jordan Robertson. “The Company Securing Your Internet Has Close Ties to Russian Spies.” *Bloomberg*, March 19, 2015. https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies.

Matthews, James K., and Cora J. Holt. *So Many, So Much, So Far, So Fast: United States Transportation Command and Strategic Deployment for Operation Desert Shield/Desert Storm*. Office of the Chairman of the Joint Chiefs of Staff, 1996. https://www.jcs.mil/Portals/36/Documents/History/Monographs/Transcom.pdf.

Menn, Joseph. “Musk’s New Twitter Policies Helped Spread Russian Propaganda, E.U. Says.” *The Washington Post*, January 9, 2023. https://www.washingtonpost.com/technology/2023/09/01/musk-twitter-x-russia-propaganda/.

Michta, Andrew A. “Mass Still Matters: What the US Military Should Learn from Ukraine.” *Atlantic Council* (blog), March 10, 2023. https://www.atlanticcouncil.org/blogs/new-atlanticist/mass-still-matters-what-the-us-military-should-learn-from-ukraine/.

Microsoft. “Defending Ukraine: Early Lessons from the Cyber War.” Microsoft, June 22, 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

———. “How Technology Helped Ukraine Resist during Wartime.” *Microsoft CEE Multi-Country News Center* (blog), January 20, 2023. https://news.microsoft.com/en-cee/2023/01/20/how-technology-helped-ukraine-resist-during-wartime/.

Microsoft Digital Security Unit. “Special Report: Ukraine - An Overview of Russia’s Cyberattack Activity in Ukraine.” Microsoft, April 27, 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

Miller, Christopher, Mark Scott, and Bryan Bender. “UkraineX: How Elon Musk’s Space Satellites Changed the War on the Ground.” *Politico*, June 9, 2022. https://www.politico.com/news/2022/06/09/elon-musk-spacex-starlink-ukraine-00038039.

Mitchell, Russ. “How Amazon Put Ukraine’s ‘Government in a Box’ — and Saved Its Economy from Russia.” *Los Angeles Times*, December 15, 2022. https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data.

Mueller, Grace B., Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias. “Cyber Operations during the Russo-Ukrainian War.” Center for Strategic & International Studies, July 13, 2023. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.

Musk, Elon. “Much Appreciated, Walter. The Onus Is Meaningfully Different If I Refused to Act upon a Request from Ukraine vs. Made a Deliberate Change to Starlink to Thwart Ukraine. At No Point Did I or Anyone at SpaceX Promise Coverage over Crimea. Moreover, Our Terms of Service Clearly Prohibit Starlink for Offensive Military Action, as We Are a Civilian System, so They Were Again Asking for

Something That Was Expressly Prohibited. SpaceX Is Building Starshield for the US Government, Which Is Similar to, but Much Smaller than Starlink, as It Will Not Have to Handle Millions of Users. That System Will Be Owned and Controlled by the US Government." X, September 9, 2023. https://x.com/elonmusk/status/1700345943105638636?lang=en.

———. "There Was an Emergency Request from Government Authorities to Activate Starlink All the Way to Sevastopol. The Obvious Intent Being to Sink Most of the Russian Fleet at Anchor. If I Had Agreed to Their Request, Then SpaceX Would Be Explicitly Complicit in a Major Act of War and Conflict Escalation." X, August 9, 2023. https://x.com/elonmusk/status/1699917639043404146?lang=en.

Odarchenko, Kateryna. "Slovak Vote Shows Need for NATO Action on Russian Disinformation." *CEPA* (blog), January 31, 2024. https://cepa.org/article/slovak-vote-shows-need-for-nato-action-on-russian-disinformation/.

Öztemel, İlknur Şebnem. "Digital Hegemony and the Russia-Ukraine War." *İletişim ve Diplomasi*, no. 8 (July 26, 2022): 43–57. https://doi.org/10.54722/iletisimvediplomasi.1124928.

Palantir. "MetaConstellation." Palantir.com, 2024. https://www.palantir.com/offerings/metaconstellation/.

———. "Palantir and Ministry of Economy of Ukraine Sign Demining Partnership." *Palantir Investor Relations* (blog), April 3, 2024. https://investors.palantir.com/news-details/2024/Palantir-and-Ministry-of-Economy-of-Ukraine-Sign-Demining-Partnership/.

———. "Palantir Edge AI in Space." *Medium* (blog), April 4, 2022. https://blog.palantir.com/edge-ai-in-space-93d793433a1e.

Paleja, Ameya. "How Did Google Maps' Traffic Data Become a Tool for the Ukraine War?" *InterestingEngineering.Com* (blog), January 3, 2022. https://interestingengineering.com/transportation/google-maps-a-tool-for-war.

Pennington, Josh, and Sean Lyngaas. "Starlink in Use on 'All Front Lines,' Ukraine Spy Chief Says, but Wasn't Active 'for Time' over Crimea." *CNN*, October 9, 2023. https://edition.cnn.com/2023/09/10/europe/ukraine-starlink-not-active-crimea-intl-hnk/index.html.

Porter, Tom. "Ukraine Celebrates US Long-Range Rocket Systems Arriving after Months of Asking. 'Summer Will Be Hot for Russian Occupiers.'" *Business Insider*, June 23, 2022. https://www.businessinsider.com/ukraine-hails-arrival-himars-predicts-pain-for-russia-2022-6.

Proska, Ken, John Wolfram, Jared Wilson, Dan Black, Keith Lunden, Daniel Kapellmann Zafra, Nathan Brubaker, Tyler McLellan, and Chris Sistrunk. "Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology." *Google Cloud* (blog), September 11, 2023. https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/?hl=en.

Quigley, Samantha L. “Detroit Defied Reality to Help Win World War II.” *United Services Organization* (blog), December 20, 2015. https://www.uso.org/stories/112-detroit-defied-reality-to-help-win-world-war-ii.

Reese, Isaac. “Can Elon Musk’s Starlink Keep Ukraine Online?” *Reason.Com* (blog), March 5, 2022. https://reason.com/video/2022/03/05/can-elon-musks-starlink-keep-ukraine-online/.

Reuters. “In Biggest Corporate Exit since Ukraine War, Search Engine Yandex’s Owner to Leave Russia in $5.2 Billion Deal.” *The Indian Express*, May 2, 2024. https://indianexpress.com/article/business/companies/yandex-nv-leave-russia-biggest-corporate-exit-since-ukraine-war-9145220/.

———. “Russia’s Yandex Fined for Refusing to Share User Information with Security Services.” *Reuters*, June 19, 2023. https://www.reuters.com/technology/russias-yandex-fined-refusing-share-user-information-with-security-services-2023-06-18/.

Rogers, Richard, and Xiaoke Zhang. “The Russia–Ukraine War in Chinese Social Media: LLM Analysis Yields a Bias Toward Neutrality.” *Social Media + Society* 10, no. 2 (April 2024): 20563051241254379. https://doi.org/10.1177/20563051241254379.

Rouse, Margaret. “Information and Communication Technology (ICT).” *Techopedia* (blog), June 27, 2023. https://www.techopedia.com/definition/24152/information-and-communications-technology-ict.

Runde, Daniel F. “China and Russia Are Closer than Ever. So Why Is Ukraine Relying on Chinese Tech Firms?” *The Hill*, September 5, 2023. https://thehill.com/opinion/international/3994402-china-and-russia-are-closer-than-ever-so-why-is-ukraine-relying-on-chinese-tech-firms/.

Saballa, Joe. “Ukraine War Exposes Flaws in America’s Sophisticated Weapons: Analysts.” *TheDefensePost.Com* (blog), May 22, 2024. https://www.thedefensepost.com/2024/05/22/ukraine-war-flaws-weapons/.

Sánchez, Irene, and José Ignacio Torreblanca. “Ukraine One Year on: When Tech Companies Go to War.” *European Council on Foreign Relations* (blog), March 7, 2023. https://ecfr.eu/article/ukraine-one-year-on-when-tech-companies-go-to-war/.

Satariano, Adam, and Paul Mozur. “Russia, in New Push, Increasingly Disrupts Ukraine’s Starlink Service.” *The New York Times*, May 24, 2024.

Satellogic. “Satellogic Announces Strategic Partnership with Palantir Technologies.” *Satellogic.Com* (blog), January 2, 2022. https://satellogic.com/news/press-releases/satellogic-announces-strategic-partnership-with-palantir-technologies/.

Sauvage, Grégoire. “Slovakia Swamped by Disinformation Ahead of Parliamentary Elections.” *France24*, August 28, 2023. https://www.france24.com/en/europe/20230928-disinformation-swamps-slovakia-ahead-of-parliamentary-elections.

Schwirtz, Michael. “Last Stand at Azovstal: Inside the Siege That Shaped the Ukraine War.” *The New York Times*, July 24, 2022. https://www.nytimes.com/2022/07/24/world/europe/ukraine-war-mariupol-azovstal.html.

Sher, Nathaniel. “Behind the Scenes: China’s Increasing Role in Russia’s Defense Industry.” *Carnegie Politika* (blog), June 5, 2024. https://carnegieendowment.org/russia-eurasia/politika/2024/05/behind-the-scenes-chinas-increasing-role-in-russias-defense-industry?lang=en.

Slaughter, Anne-Marie. *The Chessboard and the Web: Strategies of Connection in a Networked World*. The Henry L. Stimson Lectures Series. New Haven: Yale University Press, 2017.

Smith, Brad. “Defending Ukraine: Early Lessons from the Cyber War.” *Microsoft - On The Issues* (blog), June 22, 2022. https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

Starlink. “Satellite Technology.” Starlink, 2024. https://www.starlink.com/technology.

StatCounter. “Mobile Operating System Market Share Ukraine.” StatCounter, 2024. https://gs.statcounter.com/os-market-share/mobile/ukraine/2022.

———. “Search Engine Market Share Worldwide.” StatCounter, May 2024. https://gs.statcounter.com/search-engine-market-share.

Statista. “Leading Internet Companies in Russia as of February 2024, by Value.” Statista, February 2024. https://www.statista.com/statistics/1063103/leading-russian-internet-companies-by-value/.

Stone, Mike, and Joey Roulette. “SpaceX’s Starlink Wins Pentagon Contract for Satellite Services to Ukraine.” *Reuters*, January 6, 2023. https://www.reuters.com/business/aerospace-defense/pentagon-buys-starlink-ukraine-statement-2023-06-01/.

Timmermans, Remco. “Satellite Imagery Companies in Support of Ukraine.” *Groundstation* (blog). Accessed February 11, 2024. https://www.groundstation.space/business/satellite-imagery-companies-in-support-of-ukraine/.

United Nations Security Council. “Escalating Attacks on Ukraine’s Civilian, Energy Infrastructure Making Humanitarian Aid Delivery Even More Dangerous, Relief Chief Tells Security Council.” *United Nations Meetings Coverage and Press Releases* (blog), May 14, 2024. https://press.un.org/en/2024/sc15695.doc.htm.

Van Benthem, Tsvetelina J. “Privatized Frontlines: Private-Sector Contributions in Armed Conflict.” In *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, 55–69. Tallinn, Estonia: IEEE, 2023. https://doi.org/10.23919/CyCon58705.2023.10182177.

Vasquez, Christian, and Elias Groll. “Satellite Hack on Eve of Ukraine War Was a Coordinated, Multi-Pronged Assault.” *Cyberscoop* (blog), October 8, 2023. https://cyberscoop.com/viasat-ka-sat-hack-black-hat/.

Vicens, Aj. “Can Kaspersky Survive the Ukraine War?” *Cyberscoop* (blog), August 28, 2022. https://cyberscoop.com/kaspersky-ban-europe-russia-government/.

Vigliarolo, Brandon. “Kaspersky Hits Back at Claims Its AI Helped Russia Develop Military Drone Systems.” *The Register* (blog), March 5, 2024. https://www.theregister.com/2024/05/03/kaspersky_russia_military_drone_claims/.

Walker, Kent. “Helping Ukraine.” *The Keyword* (blog), April 3, 2022. https://blog.google/inside-google/company-announcements/helping-ukraine/.

———. “New Ways We’re Supporting Ukraine.” *The Keyword* (blog), January 12, 2022. https://blog.google/outreach-initiatives/public-policy/new-ways-were-supporting-ukraine/.

Watts, Clint. “Preparing for a Russian Cyber Offensive against Ukraine This Winter.” *Microsoft - On The Issues* (blog), March 12, 2022. https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/.

Weber, Peter. “A Brief Timeline of Russia’s War in Ukraine.” *The Week*, May 14, 2024. https://theweek.com/russo-ukrainian-war/1025988/timeline-russia-ukraine-war.

White, Edward. “China’s Tech Platforms Become Propaganda Tools in Putin’s War.” *Financial Times*, November 3, 2022. https://www.ft.com/content/d460c6f6-ffc7-4d61-9350-bef378fcc5c5.

Wilk, Andrzej, and Piotr Żochowski. “Ukraine Confirms Its Counter-Offensive Has Failed. Day 617 of the War.” *Centre for Eastern Studies (OSW)* (blog), March 11, 2024. https://www.osw.waw.pl/en/publikacje/analyses/2023-11-03/ukraine-confirms-its-counter-offensive-has-failed-day-617-war.

Willasey-Wilsey, Tim. “What Lies Ahead for the War in Ukraine in 2024?” *King’s College London* (blog), February 1, 2024. https://www.kcl.ac.uk/what-lies-ahead-for-the-war-in-ukraine-in-2024.

Yang, William. “How Russian Propaganda Dominates Chinese Social Media.” *Deutsche Welle (DW)*, June 4, 2022. https://www.dw.com/en/ukraine-war-how-russian-propaganda-dominates-chinese-social-media/a-61375386.

Yasar, Kinza. “Starlink.” *TechTarget.Com* (blog), August 2022. https://www.techtarget.com/whatis/definition/Starlink.

Zabrodskyi, Mykhaylo, Jack Watling, Oleksandr V Danylyuk, and Nick Reynolds. “Preliminary Lessons in Conventional Warfighting from Russia’s Invasion of Ukraine: February–July 2022.” Royal United Services Institute (RUSI), November 30, 2022. https://www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-conventional-warfighting-russias-invasion-ukraine-february-july-2022.