UNIVERSITÀ DEGLI STUDI DI MILANO

NETWORK FOR THE ADVANCEMENT OF SOCIAL AND POLITICA STUDIES

DEPARTMENT OF SOCIAL AND POLITICAL STUDIES

PHD PROGRAM OF POLITICAL STUDIES - INTERNATIONAL STUDIES

PHD COORDINATOR:

PROF. FABIO FRANCHINO

DOCTORAL DISSERTATION

Geography and Cyberspace.
The Forgotten Relevance of Territory for Digital Power

PhD Candidate

EDOARDO MARIA LANDONI

Supervisor:

PROF. ANDREA CARATI

Co-Supervisor:

PROF. ANDREA LOCATELLI

38th Cycle

Geography and Cyberspace. The Forgotten Relevance of Territory for Digital Power

Edoardo Maria Landoni

CONTENTS

Preface

In *Retropia* (2017), one of Bauman's posthumously published works, the sociologist captured an important shift in the relationship between power and space. Globalization and hyperconnectivity, he argued, had led to an «emancipation of power from territory» (Bauman 2017, 22) whereby power could float free of the bounds of geography. Capital, information, and people, now moved across the globe with unprecedented ease, eroding the once-firm link between sovereignty and soil. Nation-states, with their increasingly "porous" borders, found themselves no longer able to fulfill many of their traditional functions. This detachment of power from place – a core feature of what Bauman named liquid modernity – dealt a «deadly blow» to the conventional primacy of territory in politics, undercutting the presumed omnipotence of the modern state. In the optimistic (or apocalyptic) visions of the 1990s, geography itself was seemingly eclipsed: distance and location appeared irrelevant in a world knit together by instant digital communication and global markets. The political order envisioned in this era was one where borders mattered little, states were just one actor among many in a deterritorialized network, and power flowed in transnational circuits beyond the grasp of any single government. The end of geography and territoriality? Many thinkers at the turn of the millennium believed exactly that – that globalization together with the most recent information communications technologies (ICT) were rendering physical location moot and heralding a borderless world society. Yet even as such *end-of-geography* narratives gained traction, cracks in the facade began to show. The vision of a flat, borderless world never fully materialized in practice. Over time, the limits of deterritorialization became apparent. Economic globalization produced winners and losers still tied to specific places; cultural and political backlash against placeless power grew a renewed focus on territoriality and the relevance of place and location slowly returned.

Today, even in an almost fully developed *digital world*, we witness a resurgence of geography and territoriality as key determinants of power. Far from heralding the end of the state, the dynamics of digital globalization have instead provoked a reassertion of sovereignty on new spatial foundations. Scholars such as Wu (2021) have described this trend as a global "territorial turn" in cyberspace governance. By this, Wu refers to states' efforts to delimit boundaries and erect barriers regulating the inflow and outflow of information, irrespective of their specific motivations. The notion of a territorial turn thus captures the growing determination of governments to control and confine digital flows within defined territorial realms, thereby reinscribing borders into the architecture of cyberspace. The early utopian ideal of a borderless internet is therefore increasingly giving way to an *ethos* of digital borders, as nations realize that control over data and networks is tantamount to control over economic and political destiny. In other words, the "pendulum" is swinging back: power is

seeking ground once more. As Wu (2021) observes, the «utopia of a borderless and interconnected cyberspace» has lost its charm, replaced by what he refers to as «sovereignty fever» – a drive by states to reclaim autonomy and control that had seemed to slip away in the digital revolution. This sovereignty drive seems to guide the actions of authoritarian and democratic governments alike, both invoking "cyber sovereignty", insisting on jurisdiction over the internet within their national borders. Economically, states recognize data as fundamental resources, enforcing data localization and cloud sovereignty policies to ensure that information generated by their citizens remains subject to national law. Strategically, the security concerns of the digital age – from cyber espionage to infrastructure sabotage – have underscored that location still matters, and that keeping critical digital assets *within* one's territory (or that of trusted allies) can be as crucial as defending physical frontiers.

Indeed, it is impossible not to note that the very notion of "territory" has undergone a metamorphosis in the digital era. In a way, and it is indeed undeniable, territory has ceded ground to virtual spaces – domains composed of network topologies, cloud infrastructures, and online environments that do not correspond neatly to physical geography. These digital spaces are structured through protocols, platforms, and code rather than natural frontiers or political borders. They constitute layers of connectivity that appear detached from the material world, creating the impression of a placeless realm of flows immune to fences or walls. On the other hand, however, the digital realm still manifests itself in physical space: in undersea cables and satellites, in data centers and server farms, in the smartphones and routers that populate our cities and in the antennas scattered across our countryside. The production and movement of data depend on this very grounded infrastructure. Thus, the state's territorial base now extends into what can be described as a hybrid domain: the space of technology and innovation, at once material and immaterial, over which sovereignty is being re-claimed. Under our eyes, an inversion of Bauman's trajectory is taking place. Rather than power drifting irretrievably into the cloud, states are actively pulling the cloud down to Earth. They are territorializing cyberspace by building national firewall regimes, fencing off segments of the internet, and leveraging their physical jurisdiction over fiber-optic landing stations, exchange points, and server locations. The result is a new geography of the internet: a patchwork of digital territories, each subject to varying degrees of state control. Global cyberspace is fragmenting into what is often called a "splinternet" or a "balkanized cyberspace" – interlinked, yet partitioned by borders both technical, legal and political.

To make sense of this reassertion of space on a conceptual level, it is useful to turn to the concept of nomos, a term meaning a fundamental spatial order. *Nomos* (from the Greek *nomos*, related to dividing and distributing) refers to the way in which space is partitioned and rendered meaningful through law and power. In the political theory of Carl Schmitt, every stable political order rests upon

a concrete spatial division – a primal act of land-appropriation and boundary-making that establishes the contours of authority. Schmitt famously evoked the image of a furrow cut by a plough into the earth: this literal line in the ground is the first delineation of mine versus yours, ours versus theirs, and thus the starting point for sovereignty and legal and political order. In his view, sovereignty is not an abstract principle but something grounded – it emerges directly from the act of grounding authority in space, from taking and holding territory as the condition for law to operate. Historically, the Schmittian Nomos of the Earth was the grand spatial division that underlay the international order – for instance, the division of the world among colonial empires, or the demarcation of sovereign nation-states after Westphalia. Space, in short, is never neutral: it is actively carved up, assigned meaning, and imbued with power structures. Applying this lens to cyberspace, despite early claims that cyberspace was a realm of pure flows beyond borders, current trends suggest that a new spatial order is indeed being inscribed upon the digital world. If nomos involves acts of division, demarcation, and appropriation, then we are witnessing many such acts in the cyber domain. States drawing "digital borders" around their national internet segments, companies partitioning markets and ecosystems, and international bodies debating norms for cyberspace – all these signal an emerging geography of cyberspace shaped by power. We might speak of a re-territorialization: cyberspace is being split into zones, much like land was once parceled into sovereign territories. Sovereignty and control are exercised through new and old territorial demarcations: national routing rules, localized data storage, geofenced content regimes, and even physical cable geopolitics, where nations compete for influence over undersea fiber-optic routes. These demarcations amount to lines in the digital sand – an attempt to impose "order" on the Wild West of the early "frontier" that the internet represented. A plural landscape of sovereign digital enclaves, each with its own centers of control, its boundaries, and its peripheries. Instead of a single global village, we see a mosaic of cyber fiefs, where different rules and authorities hold sway. In this new order, sovereignty is being reinscribed in the very architecture of the internet: from the physical placement of servers to the logic of internet protocols that increasingly allow filtering by location. Power in cyberspace is taking a spatial form. Cyberspace is not immune to geography; rather, it is generating a new spatial order – one that may fundamentally redefine how sovereignty and control are organized in the 21st century.

Introduction

Mainstream depictions of cyberspace often rely on an implicit abstraction: the digital is treated as a purely virtual realm of disembodied flows, detached from the frictions of geography and the constraints of materiality. This dissertation begins from a different premise. It approaches the digital order as irreducibly spatial and physically grounded: however transformative digital connectivity may be in compressing distance and facilitating interactions across space, it does not abolish space, geography and location. On the contrary, the networks that enable global data circulation are anchored in geographic space and therefore subject to the pressures of environment, logistics, and the control of actors exercising political power over the territory. If the 1990s view − so influential for decades in shaping how cyberspace was thought and perceived – wanted to imagine it as the quintessential space far away from politics and its territoriality, recent years have made apparent a profound shift.

Indeed, we are witnessing a dual "return" in cyberspace: that of politics, on the one hand, and of geography, on the other, both of which had long seemed to be relegated to the background by narratives of deterritorialized digital flows. Cyberspace is increasingly permeated by politics: governments now seek, in the ways available to them, to discipline digital circulation and to pull it back within the reach of their territorial jurisdiction. Through regulatory, technical, and infrastructural interventions, they attempt to constrain, channel, and enclose what once appeared borderless, reasserting state-power over networks, data, and the critical nodes on which connectivity depends. In this sense, the digital domain is no longer approached as an autonomous realm of flows, but as a contested space where territorial power is actively reproduced and reconfigured. Thus, geography re-emerges as well, as a source of friction that roughens the apparently smooth surface of a globalized world, reintroducing constraints, bottlenecks, and asymmetries where narratives of seamless flow had suggested none.

The aim of this dissertation is exactly to trace, understand, reconstruct, and critically examine the dynamics behind this transformation: to analyze how the centripetal force of territory and territoriality continues to draw into itself the dialectical movements of politics, and to explore the role of geography – understood not merely as a set of physical coordinates but as a fundamental condition of friction, constraint, and resistance shaping human action – in conditioning the states' attempt to reappropriate the *cloud* by re-grounding it in the *earth*.

To achieve this goal, the study will be guided by two central research questions, each of which reflects a different but interrelated dimension of the inquiry. The first asks: *How do geographical factors*

influence the spatial distribution of cyberspace infrastructures? This question directs attention to the material underpinnings of the digital realm – cables, servers, data centers, satellite systems – and to the ways in which their placement, accessibility, and vulnerability are conditioned by geography. It underscores the need to investigate how physical location, proximity to chokepoints, climate, human geography shape the flows of information and, ultimately, the structures of power. The second question asks: *To what extent does the pursuit of cyber power by major states translate into territorial and spatial strategies of cyberspace governance?* Here the focus shifts from infrastructure to agency, and from the descriptive to the strategic: it concerns how states, as the principal actors in the international system, reassert sovereignty in the digital domain, territorialize cyberspace through law and policy, and employ spatial logics to secure advantage in a global competition for control. Together, these questions establish a framework that bridges the material and the political, the infrastructural and the strategic, in order to capture the interplay between geography, power, and cyberspace, filling a relevant gap in the literature.

However, before turning to the research design, this introduction will pause to consider several issues that, although they do not fall within the analytical scope of the present dissertation, cannot be dismissed in silence. Foremost among them is the conceptual category of "empire", whose analytical and normative fascination has recently been revived in attempts to interpret the asymmetries and hierarchies of the digital age. While this study does not adopt it as its primary lens, reflecting on its utility allows us to situate contemporary debates on cyberspace within a broader and developing literature. Alongside this, it is also necessary to acknowledge other pressing debates. In fact, closely connected to the question of cyber power are the pervasive narratives of "cyber war", "information warfare", and "hybrid warfare". These issues, although not systematically examined in the chapters that follow, constitute an important part of the intellectual and political horizon within which the present study is situated. This dissertation will contribute indirectly to these discussions, particularly to the ongoing debate over whether cyber power should be understood as a leveler of power or rather as a power multiplier. Addressing these debates, even if only in passing, is essential: they shape the conceptual terrain on which the argument unfolds, delineate the boundaries of the inquiry, and at the same time connect this work to the broader literature on the subject.

States, Corporations and Empires. Actors and Power in Cyberspace.

One tempting notion to conceptualize and analyze the developments that brought about the disruptive change of the contemporary international systems is that of "empire". *Empire* is a category that continues to exert a profound analytical and even normative fascination in the study of international power. Far from being a relic of premodern history, the idea of empire endures as a lens through which

to interpret large-scale hierarchies and dominions. In conceptual terms, empire denotes a political formation fundamentally spatial and expansionist: a core power radiating authority across extended territories and diverse peoples under a single overarching order. Pier Paolo Portinaro (2025, 24) in his latest and very sophisticated analysis of this concept, emphasizes that empire is a recurrent pattern in history – a form of rule driven by what he calls the «impulse to the maximization of *dominium*». This imperial impulse propels expansion beyond original borders and resists static limits. Empires are thus defined by incessant outreach into new spaces, the integration of far-flung domains, and a hierarchical ordering of space in which a center asserts asymmetric authority over peripheral territories (colonies, vassals, spheres of influence). Classic empires integrated vast territories and resources under a central command, treating frontiers not as fixed boundaries between equals but as zones to be penetrated or pushed outwards. The imperial center justified its dominance often with a civilizing mission or universal ideology, reinforcing a centralized structure of power. The enduring analytical appeal of the empire concept lies in how it highlights logics of control and integration on a global scale, illuminating patterns of rule that transcend the nation-state. Empire draws our attention to the drive to bind multiple regions into one polity, managing diversity through hierarchy – and this logic, as Portinaro suggests, finds echoes even in today's world of digital interconnection and supply chain interdependence. Indeed, contemporary history has not nullified the imperial paradigm so much as forced it to hybridize and adapt. The rise of the sovereign nation-state was once imagined to mark a metamorphosis of empires into a world of equal states and later free markets. Yet, as Portinaro (2025, 32) observes, this modernist hope was confuted by history: markets and civil societies never fully escaped the «protective shell» of the state, and the incomplete transformation of imperial forms means we still live in a world where oligopolistic markets and empires compete for primacy[1]. Global

[1] It should also be noted that some authors have explicitly adopted the term *empire* to capture the transformations produced by digital platforms. Vili Lehdonvirta, for instance, in his recent *Cloud Empire* (2022), applies the category directly to the private actors who extend their reach into the cloud and exercise control over networks at a level that is not territorial but rather virtual, one that appears to depart significantly from geography. As Lehdonvirta recalls, the early Internet was often perceived as a lawless frontier, a space of opportunism and risk. The emergence of major platforms such as Amazon, eBay, Apple, and Upwork introduced order and trust, but at the price of concentrating authority in the hands of a few corporations. Over time, these companies have come to rule the Internet in ways that resemble the logic of autocracy, transforming users and workers alike into subjects of vast online economic empires. In his words, digital platforms have acquired forms of *statelike dominance* over our everyday lives, establishing a new social order with little or no accountability. Neither workers nor users can "vote with their feet," since in most cases there are no meaningful alternatives to the dominant platforms. Attempts to curtail this dominance through antitrust legislation or decentralisation have proven limited in effect. For Lehdonvirta, the crucial step is to recognize digital platforms for what they are: institutions as powerful as states themselves. However, this will not be the model nor adopted nor discussed at length in

capitalism and territorial power have become deeply intertwined. Giovanni Arrighi's (2014) insight that territorial logic (land and people as ends, capital as means) and capitalist logic (capital as end, territory as means) inevitably intermingle is borne out in practice. Modern empires, in fact, can no longer be defined purely by land-grabs; they also penetrate through economic and technological dominance. Portinaro further notes that even in the "deterritorialized" age of digital wealth, we witness an unexpected new alliance between territorial control – for example, of rare earth minerals crucial for tech supply chains – and cutting-edge technology. In other words, high-tech prowess has fused with classic territorial resource control to produce what he terms imperial capitalism. An oligarchy of global corporations acting under the aegis of great powers. Such hybrid form of empire of today retain the old logics of asymmetric power and cultural ambition, even as they shed the overt trappings of colonial rule. Empire, in short, persists as a malleable idea – a shape-shifting political order that can reconfigure itself in modern garb and thus remains a fascinating framework for interpreting large-scale power dynamics.

Nowhere is the contemporary resonance of empire more evident than in the arena of cyberspace and emerging technologies. Scholars Francesca and Luca Balestrieri (2024) explicitly invoke the notion of new "technological empires" to describe how power operates in the age of artificial intelligence, 5G networks, cloud computing, and data dominance. These authors contend that we have not moved into a harmonious global village, but rather into a fractured landscape of rival imperial-like blocs grounded in technological infrastructures. Crucially, these technological empires are not based on classic territorial annexation or colonial administrations; instead, they are built on control of the digital and infrastructural grids that connect and sustain modern societies. In Balestrieri's vision, technology itself has become the principal medium of imperial power, much as territory was for historical empires. The new great powers seek to command the key platforms and pipelines of the information age – mastery over AI ecosystems, telecom networks, satellite constellations, supply

the present work, since the who writes these words is persuaded of almost the opposite view: namely, that the power of digital platforms is ultimately constrained by the state jurisdictions in which they operate, and above all by the legal and political orders in which they are incorporated. What may appear as autonomous empires in the cloud are, in practice, entangled formations whose authority is mediated and often subordinated to political sovereignty. The oscillations of Big Tech in the United States, shifting from open confrontation with political leaders to overt gestures of accommodation, reveal not so much the emancipation of digital power from the state as its profound dependence upon it. In this sense, the apparent autonomy of platforms is better understood as a precarious condition, always subject to recalibration in the face of shifting constellations of political authority (for instance see Razzante 2025).

chains of critical minerals, and troves of data. Digital networks and standards thus become the new provinces and frontiers of empire.

Despite the lack of formal colonization, hierarchical asymmetry is reproduced in these technological domains. A technological empire, in the hybridized form that Portinaro alludes to, typically has a dominant core – for example, a leading state or a consortium of firms allied with a state – that serves as the provider of crucial tech infrastructure, setting rules and norms that others downstream must follow. Balestrieri and Balestrieri describe how the imperatives of advanced technology are re-drawing the map of international relations in ways that mirror imperial patterns. The structure of global supply chains for strategic tech – semiconductors, AI, telecommunications – creates new centers and peripheries defined not by geography alone but by functional dependence, drawing new hierarchies of spaces and creating a new geography of linkages and dependencies. In this landscape, smaller states or regions become pivotal if they hold key resources (like lithium, cobalt, rare earths) or if they host essential infrastructure, much as colonies or buffer zones were pivotal to old empires. Moreover, these technological empires wield power not just through hardware, but through norms and standards, echoing the way past empires imposed laws or religions. In the digital realm, the dominant powers promulgate technical standards, protocols, and regulatory models that function as instruments of quasi-imperial informal control. For instance, a smaller nation that adopts one empire's AI surveillance platforms may find itself bound into that power's security and data ecosystem, much as a vassal once depended on imperial protection. The key point is that, even without formal conquest, the power asymmetry and integrative reach of empire are very much present: a hegemon in tech can dictate terms to users and client states, extract value (data, rents, political alignment) from them, and shape the environment to its advantage. In short, the concept of empire – as an expansive, integrative, hierarchical order – resonates strongly with the power dynamics of cyberspace today. The analogy illuminates how contemporary great powers (and their corporate proxies) behave not merely as Westphalian states dealing in mutual sovereignty, but as *de facto* imperial centers organizing global networks around themselves. The resonance with the traditional concept of empire is thus powerful: we see normative universalisms, each tech bloc claiming to represent a model for all, economic extraction in form of monopolistic platforms accumulating wealth globally, and political dependency, states aligning under digital umbrellas, all at work in cyberspace.

At the same time, the divergences should be underscored. Technological empires differ from classical empires in important ways. They are less about direct territorial occupation and more about controlling the "connective tissue" of globalization as stressed by Arrighi (2014). Authority is often exercised through contracts, intellectual property, and infrastructure ownership rather than through

governors and garrisons. In essence, coercion is subtler – exerted via technological indispensability or economic leverage rather than naked military force. Yet, as noted, this softer appearance masks a hard hierarchy: the subordinate nodes in the network have little recourse against the central power that can weaponize interdependence (on this see, for instance, Farrell and Newman 2019).

Given the rich insights the imperial paradigm offers, one might ask why this dissertation does not adopt "empire" as its primary analytical lens. Indeed, the concept of empire is alluring: it captures grand strategic patterns, highlights hierarchies and dependencies, and connects contemporary phenomena to a deep historical lineage. However, for the purposes of this study, the decision is to treat empire as a suggestive background concept rather than as the central framework. The principal unit of analysis remains the state. This choice is both methodological and substantive. Methodologically, focusing on the sovereign state provides clarity and concreteness. States are the formally constituted actors in international law and the custodians of coercive and regulatory power; even when they behave in imperial-like ways, they do so through state institutions and state interests. By analyzing how states assert power in cyberspace – through policies, alliances, and rivalries – we can ground the discussion in tangible actors and avoid the potential vagueness of an "empire" metaphor. As several scholars caution, "empire" as an analytical category, while evocative, can be nebulous and risk blurring important distinctions (see Portinaro 2025, 22). Modern great powers certainly exhibit imperial tendencies, but they have not self-identified as empires *per se*; they operate through the idiom of nation-states, jealously guarding their sovereignty even as they infringe on others'. Thus, retaining a state-centric lens allows this work to engage with the concrete mechanisms of power (e.g. national cybersecurity strategies, interstate competition for technological standards, digital sovereignty initiatives) without overextending the empire analogy beyond its utility.

Substantively, the state remains the linchpin of international order and the primary *locus* of accountability, even in a world of transnational networks. By foregrounding states, this work will examine how states actually deploy their state apparatuses – legal, military, economic – to shape cyberspace, and how other states respond or align. The empire concept certainly enriches this analysis by providing a vocabulary of core-periphery relations, hegemonic orders, and integration through power. It reminds us that what may appear as a collection of bilateral state interactions can amount to a systemic logic of domination reminiscent of empires. However, this dissertation will use those insights as a contextual backdrop rather than as the primary explanatory model. The risk of adopting empire as the main lens is that it might treat diverse phenomena as monolithic. Instead, by focusing on states, we acknowledge the agency of a wider array of actors – including middle powers and even private sector players that operate through state jurisdictions – and avoid implying a foregone imperial

structure. In sum, while the category of empire is undeniably useful for interpreting the power asymmetries and integrative ambitions characterizing cyberspace today, it will serve here as an illuminating analogy and historical reference rather than as the defining framework. The dissertation proceeds on the premise that states, not empires, are the primary actors in the contemporary international system – even if those states at times behave in ways that *evoke* the imperial typical behavior although in new hybrid forms. By keeping empire in view conceptually but not letting it dictate our analytical boundaries, we can better appreciate its relevance yet remain focused on the concrete dynamics of state power in the cyber arena. This approach harnesses the richness of the empire idea as a background insight while ensuring that the study's lens remains sharply attuned to the strategic behavior of states and the evolving norms of state-centric order in cyberspace.

Cyberspace as a New Domain of Conflict

Cyberspace recently emerged as a new domain of military competition (Martino 2018), and for great powers the appearance of a new domain often spurs ambition (Rovner 2023, 1068). The opportunity to control a new space is typically compelling as such control can yield significant security and economic advantages. This is evident in historical efforts to master the sea, control airspace, and dominate supra-atmospheric space. Although fundamentally different from these natural domains because it is entirely artificial − a vast network of communications infrastructure and data storage constructed and sustained by humans − the principle remains consistent in the realm of cyberspace. Today, the cyber domain, similarly to the other domains, offers strategic opportunities for those who can effectively govern its expanse, and vulnerabilities for those who cannot. Given the increasing reliance on cyberspace, it is crucial for nation-states to develop technical capabilities that minimize vulnerabilities and mitigate the risk of potential attacks. The militarization and weaponization of cyberspace is not only a historical fact, but it is an ongoing process. Consequently, states are formulating and imagining comprehensive grand strategies[2] for cyberspace, clearly identifying the

[2] Here the concept of grand strategy, following Silove's (2018) thorough analysis, will be understood as an «organizational principle» that functions as a guiding or overarching framework shaping and directing a state's foreign policy and decision-making processes. Rather than being a detailed, prescriptive plan, it provides a strategic framework or set of core ideas that inform and influence long-term policy choices. This approach emphasizes broad, consistent principles rather than specific, step-by-step plans. An "organizational principle" that in some way «tells a logical story about how states and non-state actors keep themselves safe». As opposed to "strategy" that will be defined as: «Strategy is a theory of victory, a logical story explaining how the use of force will help combatants achieve their political goals» (Rovner 2023, 1067-1068).

factors necessary to maximize their security and power and get ready to wage war in this domain. However, debate has long swirled around what exactly *cyberwar* means – and even whether it truly exists as a form of war. Not everyone agrees that operations in cyberspace constitute a warfighting domain in the classical sense. Cyberspace is a man-made network largely driven by private sector infrastructure and civilian information flows, which makes the label "war" contentious. Skeptics in fact argue that calling it "war" risks stretching the concept beyond usefulness (see for instance, Valeriano & Maness, 2015), especially given the traditional Clausewitzian conception of war as violent, political conflict between adversaries, inherently implying lethal violence and state policy aims. Following this logic, political scientist Thomas Rid (2012) in his as influential as polemic article *Cyber War Will Not Take Place* contends that most so-called cyber "attacks" do not meet the threshold of actual war. Indeed, no cyber attack caused direct loss of life or physical destruction on par with traditional warfare. Rather, most cyber operations resembled espionage, sabotage, or subversion, all activities adjacent to war but not war itself in the sense.

This Clausewitzian litmus test remains a central point of contention. Rid and like-minded scholars note that cyber operations so far have served as adjuncts to conventional force or as intelligence-gathering and propaganda tools, but not as independent war-winning weapons. Others have similarly observed that the "currency" of cyberspace is information, not violence – making cyber conflict more akin to an intelligence contest or covert operations competition than a traditional battlefield clash. In this view, common cyber tactics such as hacking, data theft, or disruption of networks lack the kinetic force that characterizes true warfare. On the other hand, more concerned strategists and scholars maintain that cyberwar could attain war-like effects, especially as societies become ever more dependent on digital infrastructure. As early as the 1990s, analysts warned of a coming ability to paralyze economies and critical systems via cyber means alone – a sort of bloodless warfare in the ether. Governments and militaries have certainly treated cyberspace as a new domain of strategic competition, establishing dedicated cyber commands and doctrines. Many strategists see cyberspace operations as offering the prospect of swift, decisive outcomes: by blinding the enemy's communications and intelligence, a cyber offensive might induce "operational sclerosis" in adversary forces, potentially yielding quick victory with minimal bloodshed (on the concept of "strategic cyberwar" see Molander et al.,1996; Clarke and Knake, 2012; Kallberg, 2016, Lavorio 2025). This alluring vision has driven substantial investment in cyber capabilities worldwide. Notably, former U.S. official Richard Clarke in his book written with Robert Knake (2012, 62) warned the United States of the looming real possibility of a devastating surprise attack that could cripple national infrastructure «without a single terrorist or soldier ever appearing in this country». Such scenarios posit that cyberweapons might render an enemy defenseless by crashing its ability to understand what

is happening and to react. Using Warden's (1995) organicist metaphor, a successful cyber campaign can be imagined as an assault that renders the adversary's "nervous system" paralyzed: by disrupting the transmission of signals and impulses, attackers can incapacitate communication networks and thus render the organism dysfunctional. Cyber operations that target communications, power grids, or financial systems do not merely create temporary inconvenience; they can interrupt the nerve-like flows that sustain governance and the state's material capacities, degrading both the administrative skeleton and the muscular apparatus of the polity. In consequence, the state's ability to coordinate, to project force, and to sustain public order may be seriously impaired, all while the perpetrator remains hidden behind a computer screen (Betz 2011). These dire warnings stand in stark contrast to the skeptics' insistence that cyber operations, while disruptive, have yet to equate to the destructiveness of traditional war and instead largely serve as operations in support of conventional "kinetic" combat. Martin Libicki (2009) provides a clear distinction between two visions and two possible uses of cyberwar. For the American scholar, strategic cyberwar is «a campaign of cyberattacks launched by an entity against a state and its society, primarily, but not exclusively, with the purpose of influencing the behaviour of the targeted state» (Libicki 2009, 117). In this understanding, cyberwar is an instrument of political agency: it operates largely outside the strictly military perimeter, striking the critical nodes of society in the information age and paralysing or preventing a potential response. It erodes the adversary's strategic advantage through dispersed or surgical attacks. This deep attack on the enemy's social, economic, and political fabric bears strong similarities to theories of strategic aerial bombardment. Operational cyberwar, by contrast, consists of «cyberattacks in support of combat» (Libicki 2009, 6) and, more generally, of the «use of computer network attack in support of physical military operations» (Libicki 2009, 117). It takes place within the framework of kinetic conflict and warfighting; it acts as a force multiplier for kinetic war at the tactical and operational levels; it contributes to monitoring and understanding the operational environment in real time (situational awareness); and it strengthens interoperability among deployed units.

Alongside the narrow question of cyberwar's definition, a broader conceptual landscape has developed around information-age conflict. Terms like information warfare, netwar, and hybrid war[3] have emerged to describe the changing character of warfare in the late 20th and early 21st centuries. Tracing these ideas historically reveals both overlaps and important distinctions in how thinkers have

[3] On this, particularly interesting is the contribution of Stefanachi's *Guerra ibrida: Origine, significati ed equivoci di un concetto ambiguo* (2024) in which it is highlighted the origins and the use of this vague term. See also Mattis & Hoffman (2005), and Hoffman (2007).

envisioned the interplay of cyber capabilities, information operations, and traditional military force. Early RAND theorists in the 1990s were among the first to grapple with how the ongoing information revolution might transform warfare. In a milestone 1993 article titled "Cyberwar is Coming!", John Arquilla and David Ronfeldt argued that the advent of advanced computing, networking, and precision sensors augured a profound shift in how wars would be fought generating a *sui generis "*cyberwar" (On this see also the reflection of Stefanachi 2023). Drawing lessons from the U.S. victory in the 1991 Gulf War, Arquilla and Ronfeldt foresaw that information would become the decisive factor on the battlefield, perhaps more crucial than sheer weight of firepower, as wielding information was indeed a power multiplier. In their vision, future militaries would battle over information – victory going to the side that could secure its own information systems while blinding the enemy in a "fog" of confusion. Achieving this would require reorganization of forces and doctrine: militaries would need dedicated units and strategies for managing and attacking information networks. Figures like Arquilla and Ronfeldt saw cyber capabilities as intertwined with traditional military power, not a magic bullet that would obviate tanks and bombs. Indeed, Arquilla later warned against narrowing cyberwar to just the "virtual domain" insisting that its military dimension – including physical force – must remain central.

The debate over what constitutes a "cyberwar" is not moot as it also has important consequences for who is thought capable of waging − and winning − conflict in the digital domain. If cyber operations can, by means of a single networked device, paralyze a far stronger adversary, then cyberspace becomes the quintessential weapon of the weak: the proverbial sling with which David can fell Goliath. Conversely, if the image of spectacular, independent cyberwar remains largely hypothetical, and what we more plausibly mean by cyberwar is a form of conflict that exploits informational asymmetries and institutional leverage, then mastery of the domain is likely to remain the preserve of central actors − those located at the hubs of global networks with the capacity to deploy sensors, devices, cables and platforms, to gather and process vast quantities of data, and to project influence through political, financial and psychological operations. In short, the stakes of the definitional debate are not abstract: they determine whether cyberspace is a strategic equalizer or a power multiplier. There is in fact an open debate in the literature concerning that, in other terms, is concern on the question if cyberspace presents itself as a weapon of the strong or as a weapon of the weak (Dossi 2018, 357-363). According to various authors, in fact (see for example: Khuel 2009; Nye 2011), cyber space provides opportunities even for smaller and weaker states to develop significant cyber capabilities. Nye's stresses the fact that:

> It is cheaper and quicker to move electrons across the globe than to move large ships long distances through the friction of salt water. The costs of developing multiple carrier task forces and submarine fleets create enormous barriers to entry and make it possible to speak of American naval dominance. In contrast, the barriers to entry in the cyber domain are so low that nonstate actors and small states can play significant roles at low cost (Nye 2011).

However, while it appears that anyone can enter cyberspace due to its relatively low barriers, controlling it to effectively wield cyberpower presents a distinct challenge. The commanding U.S. officer of Cryptologic Warfare Activity, Robert "Jake" Bebber, noted (2022) that as when thinking about sea power it is common to focus:

> Over fleet size while neglecting the industrial base and logistics. Similarly, [when thinking about cyberspace and cyberpower] they focus on "hacking" without considering training and talent, cyber infrastructure, capabilities, operational concepts, or nesting into larger campaign plans or strategies.

While data may be intangible, they are derived from physical elements that are dispersed across geographical and political spaces. As a result, building the necessary infrastructure for controlling the data flow and storage, and developing the technical skills required for processing them is crucial for achieving dominance in the cyber domain. Furthermore, the capacity of a nation to innovate and produce new technologies and standards, thereby extending its power and influence geographically by providing these technologies and infrastructures, is an expensive undertaking that only major powers can afford. This is equally true for the development of specialized skills necessary to operate effectively in the cyber realm[4].

One of the main contributions of this dissertation, as said, is to advance this debate and will do so by supporting the perspective of those who argues for it to be power multiplier: in fact, rather than providing weaker actors with an effective weapon against stronger adversaries, cyberspace tends to amplify the advantages of those who can secure and sustain, through the building and managing of infrastructure, central positions within its networks. By examining both the geographical and topological dimensions of cyberspace − its material infrastructures such as cables, data centers, and satellite systems, as well as its virtual architectures of platforms and standards − this study demonstrates how centrality consistently generates strategic benefits. Central actors are better able to regulate flows, interdict adversaries, and extend their influence across borders, converting connectivity into a source of geopolitical leverage. This dynamic is visible in the way established

[4] As for smaller states this holds true also for non-states actors or militant organizations (see Arquilla 2021, 46-53).

great powers have historically entrenched their network centrality, and in the efforts of rising states to create alternative hubs of influence. For instance, the long-standing U.S. dominance in digital infrastructures and the more recent Chinese attempts to build competing standards and infrastructure ecosystems illustrate how centrality functions as a positional resource in cyberspace. Its architecture rewards those positioned at the core of global networks, where geography and technology converge to generate control and resilience. By situating cyberspace within its spatial and infrastructural logics, this dissertation shows that centrality systematically reproduces hierarchies, reinforcing the power of dominant actors while constraining the strategic options of those relegated to the periphery.

Research Design

This section outlines the overall structure and general research design of the dissertation, clarifying how its empirical components relate to the two research questions and to one another. It is intentionally presented at a synthetic level: the full specification of the design, the procedures, the operationalization of variables, and the detailed justification of analytical choices are developed in greater detail in Chapter II (under the section *"A New Methodological Approach to Cyber Infrastructure: Historical Reconstruction, Mapping and Network Analysis"*) and in Chapter III (under the section *"Introduction and Methodological Framework"*), where each methodological step is explicitly motivated in relation to the chapter-specific hypotheses and evidence.

The research design underpinning this dissertation naturally reflects the dual ambition of the project: to investigate cyberspace as both a material domain structured by geography and as a political arena in which states pursue strategies of power through territorial and infrastructural control. In order to meet these objectives, the study adopts a design that combines quantitative spatial analysis and network analysis with qualitative interpretative inquiry, thereby bridging the geo-strategic dimensions of cyber power. This is to connect two analytically distinct dimensions of cyber power: first, the infrastructural "conditions of possibility" that shape how digital connectivity is organized and where dependencies and chokepoints emerge; and second, to read and understand the strategic behavior through which major states attempt to translate those conditions into political leverage by reasserting sovereignty, managing interdependence, and shaping the governance of the digital domain.

At the center of this design stand the two already stated research questions. The first concerns the ways in which geographical factors influence the spatial distribution of cyberspace infrastructures. This question directs attention to the physical *substratum* of the digital realm, namely the cables, servers, datacenters, and satellite systems upon which all virtual flows ultimately depend. While much of the literature has treated cyberspace as detached from material constraints, this dissertation starts from the premise that its architecture is profoundly shaped by spatial logics. The placement of

infrastructures, their accessibility, and their vulnerabilities cannot be understood independently from their geography. Proximity to maritime chokepoints, exposure to natural hazards, climate conditions, and human geography all play a role in shaping how information circulates and, by extension, how power is distributed. The second research question shifts the analytical lens from the descriptive to the strategic, asking to what extent the pursuit of cyber power by major states translates into territorial and spatial strategies of cyberspace governance. Here the focus is less on the infrastructures themselves than on the agency of states and in particular great powers. The question addresses how governments seek to reassert sovereignty in the digital domain, territorialize cyberspace through law, policy, and standards, and employ spatial logics to secure economic, political and military informational advantage.

Testing these questions requires an explicit set of hypotheses, which the dissertation develops in line with its chapter structure. Chapter II is devoted to the first research question and the analysis focuses mainly on submarine cables and data centers. This chapter advances the hypothesis that spatial and geographical factors are not merely contextual but constitutive elements shaping the distribution of these infrastructures. After a detailed historical reconstruction of these infrastructures, more specifically, four hypothesis are advanced. Two hypotheses address submarine cables: the first posits that these infrastructures are disproportionately concentrated around major maritime chokepoints, while the second suggests that the global cable system has a hierarchical structure, with a limited number of states acting as central anchors of connectivity, and peripheral regions remaining dependent on strategic gateways and brokers located at regional intersections. A parallel set of hypotheses concerns the distribution of data centers. The first argues that their global location is highly concentrated in economically advanced and digitally interconnected regions, rather than randomly dispersed. The second maintains that siting decisions reflect a balance between environmental advantages, avoidance of natural hazard-prone areas, and proximity to major population centers. The *rationale* behind this is that operators seek cooler climates and reliable energy supplies in order to reduce costs, but they must also remain sufficiently close to concentrations of digital demand to ensure low latency and efficient service delivery. These empirical claims about infrastructures and their geography set the stage for the second part of the analysis, which shifts from structures to agency.

The empirical testing of these hypotheses relies on a combination of data sources, selected to capture both the infrastructural and the strategic dimensions of cyberspace. For submarine cables, the research draws on Greg's Cable Map, the only publicly available dataset providing a global inventory of 285 fiber-optic cables and 586 landing stations, with information on capacity and routes. For data centers,

the primary source is DatacenterLocation.com, which offers addresses of facilities worldwide. These addresses were geocoded into geographic coordinates using QGIS, reducing the initial dataset of over 4,000 entries to 2,422 usable cases. This dataset, though imperfect and biased in its representation of certain regions remains the most comprehensive available source for systematic spatial analysis.

To situate these infrastructures within their environmental context, additional datasets were integrated. Climate data were drawn from the WorldClim 2.1 dataset, providing annual mean temperatures for each data center location, which allowed the analysis of how climate conditions shape siting decisions. Hazard exposure was assessed using NASA's *Global Multihazard Frequency and Distribution* dataset, with the Point Sampling Tool in QGIS used to link each data center to levels of natural risk, ranging from floods to earthquakes. Population density was incorporated through NASA's *Gridded Population of the World, Version 4 (GPWv4)*, which makes it possible to evaluate the proximity of data centers and landing stations to concentrations of digital demand. In this way, the infrastructural analysis systematically combines technological, environmental, and human-geographical variables to test the hypotheses of concentration, hierarchy, and risk. As said, the technical procedures and the specific operations carried out on each dataset − from the geocoding and spatial analysis of infrastructures to the analysis of state strategies − will not be exhaustively detailed here, but will be presented more systematically in the respective chapters, where the analytical choices and the empirical findings are closely examined.

Beyond the construction of a cartography, Chapter II treats GIS as an analytical framework. Spatial data on cables, landing stations, and data centers are not only mapped but interrogated through standard GIS operations − such as heatmaps, proximity and overlays with environmental and demographic layers − to identify spatial regularities and patterns of possible unexpected variability. Then, the analysis "moves from maps to networks" by transforming the submarine-cable dataset into a relational graph in which countries are modelled as nodes and cable links as weighted ties (by nominal capacity). Network analysis is also applied to conceptualize the global submarine cable system as a graph, in order to identify patterns of centrality, hierarchy, and dependency. These methods make it possible to operationalize abstract ideas of "centrality" and "peripherality" into measurable spatial patterns. Centrality measures are used to identify hubs, intermediaries, and structurally peripheral actors, thereby capturing degrees of dependence and exposure that are not immediately visible on a geographic map. Community detection further reveals meso-level regional groupings and patterns of integration, while brokerage-oriented indicators highlight gateway states that bridge otherwise weakly connected clusters. Taken together, GIS and network analysis allow the chapter to go beyond descriptive mapping and to interrogate the relational architecture of digital

infrastructure, showing how material geography and political influence are inscribed in the topology of global connectivity. Finally, in addition to mapping and network analysis, Chapter II also introduces an exploratory modelling step that links observed spatial patterns to theoretically salient correlates of data center siting. Specifically, the mapped regularities − strong clustering in techno-economic centers and a visible attraction toward temperate belts − are translated into a deliberately parsimonious statistical framework that examines associations between the intensity of datacenter location and a small set of covariates capturing demand, operating conditions, and environmental exposure. This modelling exercise is explicitly not intended to establish causal mechanisms of location selection, rather, it serves as a transparent bridge between cartographic patterns and theoretical expectations, offering a baseline quantification of how population concentration, climatic conditions, and hazard exposure co-vary with the global footprint of datacenter infrastructure.

Chapter III develops a different but complementary hypothesis, focused on the agency of states. The central claim here is that major powers, in their pursuit of cyber power, systematically resort to territorial and spatial strategies to govern cyberspace. In contrast to narratives that depict cyberspace as inherently free and de-territorialized, the argument is that governments are actively reasserting sovereignty, embedding cyberspace within territorial logics, and seeking centrality in infrastructures and standards as a means of consolidating geopolitical power. The empirical analysis is organised as a structured comparison of the United States and China. Their selection is motivated not by an interest in regime-type opposition − liberal versus authoritarian cyberspace − but by their paradigmatic value as two actors that combine both the capability and the intention to shape digital infrastructures and the rules that govern them; the logic of this case selection is specified more fully in Chapter III.

To ensure conceptual precision and prevent the concepts of “cyber power” and “territoriality” from remaining underspecified, the dissertation translates the two abstract notions in ways that support systematic empirical assessment.

The conceptualization of “cyber power” used here is broad enough to capture its multidimensionality, yet bounded enough to remain empirically tractable. It is understood as the capacity of a state to produce preferred outcomes in and through cyberspace, whether through (I) operational, (II) regulatory, or (III) infrastructural means. This definition does not presuppose which mechanism is dominant rather, it provides a consistent conceptual basis for assessing through observable practices whether territorial and spatial strategies of governance constitute a central pathway through which major powers pursue cyber power.

As for “territoriality”, it is operationalized by translating the abstract notion of “territorial and spatial logics” into three analytically distinct dimensions: (I) reshoring and localisation, expressed in efforts to re-embed data, cloud services, and critical digital assets under domestic or allied jurisdiction; (II) resistance to foreign control, visible in screening regimes and enforced restrictions on rival ownership or operation of core nodes of the national digital ecosystem; and (III) outward supply and projection, whereby states export digital infrastructures and technological ecosystems to third countries, using finance, standards, and infrastructure provision to shape alignments and dependencies while excluding strategic competitors. Evidence is evaluated through a coding protocol that distinguishes declaratory authority from implemented practice by assigning a trichotomous score (0 = absent; 1 = capacity/intent; 2 = territorial practice). In addition, falsifiers are incorporated to prevent the inflation of findings through rhetorical or symbolic policy declarations: systematic non-execution of pledged measures, the persistence of rival control over core nodes despite documented security externalities, or permissive cross-border handling of sensitive data despite localisation mandates constitute disconfirming evidence that overrides otherwise supportive indicators.

As with any research design, this study is not exempt from constraints and trade-offs, which must be openly acknowledged. While the combination of quantitative and qualitative methods allows for a richer analysis, the datasets on infrastructures, though among the most complete available, are incomplete and potentially biased, leaving some regions underrepresented. The rapid evolution of digital infrastructures means that the analysis provides a snapshot rather than a definitive account. Moreover, the sensitive and proprietary nature of many data sources constrains the granularity of the analysis. On the political side, public documents may only partially reveal the strategic intentions of states, requiring careful interpretation. Finally, while the broader debates on cyberwar and information warfare form part of the intellectual horizon of the dissertation, they are not directly taken into consideration, as the focus remains on the interplay between geography, infrastructure, and great powers’ grand strategy and their “territorial imperative”.

Taken together, this research design allows the dissertation to advance its central argument: that cyberspace, far from being an immaterial or deterritorialized realm, is deeply conditioned by geography, and that the pursuit of cyber power by states is increasingly articulated through territorial and spatial logics. After reconstructing the dynamics of the events that led to the current state of affairs in cyberspace, by combining the material and the political, the infrastructural and the strategic, the study not only fills a gap in the literature but also provides a framework for understanding the geographical foundations of digital power in the twenty-first century.

Chapters Outline

Chapter I offers a historical and conceptual reconstruction of how cyberspace was imagined, instituted, and subsequently re-politicized and why geography and territory matter for its control. Beginning with the Cold War genealogy of global communications, it shows how strategic imperatives prefigured the infrastructures of connection. It then tracks the liberal interlude of the 1990s-2000s − market primacy, deregulation, and the ideology of a borderless web − and follows the slow undoing of that imaginary as sovereignty claims, security concerns, and infrastructural rivalries reinserted borders into the digital. The chapter restores geography to its rightful place as a structuring condition, setting up the empirical investigation that follows.

Chapter II constitutes the analytical core of the dissertation and turns to the material foundations of the digital realm to show that cyberspace has a geography and that this geography matters. The chapter reconstructs the contemporary cartography of connectivity by examining submarine cables, landing stations, and data centers together, treating them as a coupled system rather than as isolated assets. It first maps the oceanic matrix of fiber-optic routes and identifies recurrent spatial regularities: the persistent pull of maritime chokepoints, the emergence of regional gateways, and the hierarchical organization of routes that privilege a limited number of hubs while relegating others to dependency at the network's margins. This discussion does not merely inventory lines on a map; it shows how route geometry, landing-point clustering, and brokerage positions translate into differentiated capacities to steer, surveil, and interrupt flows. From the sea to the shore, the chapter follows the network inland and interrogates the siting of data centers as the terrestrial anchors of the cloud. It demonstrates that their distribution is patterned rather than random, with clear concentrations in advanced and highly interconnected regions. It then unpacks the siting calculus that produces these clusters: climatic advantages and energy stability that lower operating costs; exposure to multihazard risk − floods, earthquakes, sea-level rise − that conditions resilience planning (although the relation is not as straightforward as one could expect); and proximity to population and demand that compresses latency. The analysis places these factors in tension, cooler climates versus distance to markets, cheap power versus regulatory constraints, showing how different combinations yield distinct regional geographies of the cloud.

Throughout, the chapter insists that infrastructure is never "just technical". Ownership structures, jurisdictional reach at landing sites, and the legal status of data facilities confer leverage that is at once material and political. By reading the submarine system as a relational topology and the data-center landscape as a layered spatial field, the chapter brings to light patterns of centrality and peripherality that concentrate both control and vulnerability. It shows how redundancy and route

diversity are unevenly distributed; how a handful of hubs act as brokers between regional clusters; and how the very configurations that maximize throughput also enlarge the attack surface. The result is a picture of infrastructural power in which geography − maritime passages, coastal morphologies, energy geographies, hazard belts, urban demand basins − shapes who can move, see, slow, or sever digital flows. In this sense, Chapter II provides the empirical hinge of the dissertation: it demonstrates that the architecture of connectivity is a spatial order, and that this order underwrites asymmetric capacities for control, interdiction, and resilience.

Chapter III moves from structures to strategies and examines how major states translate the pursuit of cyberpower into practices of territorialization. It analyzes how governments reassert sovereignty in and through the digital by aligning law and policy with infrastructural leverage − localizing data, constraining extraterritorial control, sponsoring domestic ecosystems, and projecting influence outward through technology provision, standards promotion, and external infrastructure. The comparative discussion draws on the most salient practices of leading actors to illustrate both convergence (sovereign governance of infrastructures) and divergence (varieties of jurisdictional reach and industrial policy), showing that competition for positional centrality has become a defining feature of contemporary geopolitics of the network.

Bibliography

Annino, A. *Regni o colonie? Ancora sulle ambivalenze dell'orbe ispanico*. In P. P. Portinaro (a cura di), *Le metamorfosi degli imperi* (2025). Milano: Solferino.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy, 12*(2), 141–165.

Arrighi, G. (2014). *Il lungo XX secolo*. Milano: Il Saggiatore.

Bauman, Z. (2017). *Retrotopia*. Cambridge: Polity Press.

Bebber, R. J. (2022, December). Cyber power is a key element of sea power: Rebuilding American sea power will require the skillful use of cyber power to prepare the battlespace, fight, and win. *Proceedings, 148*(12), 1438.

Betz, D. (2011). "Cyberwar" is not coming. *Infinity Journal*, (3), 21–24.

Balestrieri, F., & Balestrieri, L. (2024). *Tecnologie dell'impero: AI, quantum computing, 6G e la nuova geopolitica del potere*. Roma: LUISS University Press.

Clarke, R. A., & Knake, R. (2012). *Cyber War: The next threat to national security and what to do about it*. New York, NY: Ecco.

Dossi, S. (2018). Confronting China's cyberwarfare capabilities: A "weapon of the weak" or a force multiplier? In M. Clementi, M. Dian, & B. Pisciotta (Eds.), *US foreign policy in a challenging world: Building order on shifting foundations*. Springer.

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security, 44*(1), 42–79.

Fick, S. E., & Hijmans, R. J. (2017). WorldClim 2: New 1-km spatial resolution climate surfaces for global land areas. *International Journal of Climatology, 37*(12), 4302–4315.

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies.

Kallberg, J. (2016), "Strategic Cyberwar Theory – A Foundation for Designing Deci sive Strategic Cyber Operations", The Cyber Defense Review, 1(1): 113-128.

Lavorio, A. (2025). *Miti e limiti della "strategic cyberwar": Un'analisi del conflitto russo-ucraino*. Rivista di Digital Politics, 5(1), 195–216.

Libicki, M. (2009), Cyberdeterrence and Cyberwar, Santa Monica, Rand Corporation.

Martino, L. (2018). La quinta dimensione della conflittualità: L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale. *il Mulino*.

Mattis, J. N., & Hoffman, F. G. (2005). Future warfare: The rise of hybrid wars. *Naval Institute Proceedings, 131*(11), 30–32.

Molander R. C., Wilson P. A. e Mussington D. A. e Mesic R. (1998), Strategic Information Warfare Rising, Santa Monica, Rand Corporation.

Nye, J. S., Jr. (2011). Nuclear lessons for cybersecurity? *Strategic Studies Quarterly, 5*(4), 18–38.

Portinaro, P. P. (2025). *Le metamorfosi degli imperi*. Milano: Solferino.

Razzante, R. (2025, mese giorno). Trump e il servilismo delle Big Tech nei suoi confronti. *La Nuova Bussola Quotidiana*.

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies, 35*(1), 5–32.

Rovner, J. (2023). Strategy and grand strategy in new domains. In H. Brands (Ed.), *The New Makers of Modern Strategy* (pp. 1067–1092). Princeton, NJ: Princeton University Press.

Silove, N. (2018). Beyond the buzzword: The three meanings of “grand strategy.” *Security Studies, 27*(1), 27–57.

Stefanachi, C. (2023). Una certa idea di cyberwar: John Arquilla’s reflections on war in the information age. *Quaderni di Scienza Politica, 30*(3), 295–334.

Stefanachi, C. (2024). Guerra ibrida: Origine, significati ed equivoci di un concetto ambiguo. *Storia del pensiero politico, 2*(2024), 239–264.

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press.

Warden, J. A. (1995). The enemy as a system. *Airpower Journal, 9*(1), 40–55.

Wu, C.-H. (2021). Sovereignty fever: The territorial turn of global cyber order. *Heidelberg Journal of International Law (ZaöRV), 81*(3), 651–676.

Chapter I - Cyberspace, Cyberpower and Geopolitics. From the Liberal Order to a New Contested Reality

The World Has Grown Smaller

On October 2, 1872, in an opulent room of the Reform Club, a group of London gentlemen exchanged opinions about the recent escape of a particularly daring thief, as reported by the *Daily Telegraph*. During their discussion, they noted that the world seemed, in some way, to have shrunk. «Well, but where can he fly to?» one gentleman remarked. Another promptly responded, «Oh, I don't know that. The world is big enough». At this point, the protagonist of Jules Verne's novel, Phileas Fogg, interjected in a low and decisive tone, «It was once». «And now?» the gentlemen, surprised, replied, «Has the world grown smaller? »[5].

In this spontaneous exchange, which set the stage for the adventurous story narrated in the novel *Around the World in Eighty Days*, Jules Verne effectively captured many of the objective implications that the technological advancements of the XIXth century had on geographical space. He vividly illustrated how these innovations transformed the perception of that space, no longer seen as boundless but instead as smaller and more interconnected, encircled by an unbroken network of established shipping routes and railways that allowed people and goods to traverse it within set timeframes along predetermined paths.

The rapid technological advancements at the end of the 19th century were, unsurprisingly, also recognized by numerous scholars who sought to understand how these changes might alter the distribution of political and military power across the globe. It can be argued that this awareness gave rise to the critical thinking of authors, particularly in the Anglo-Saxon sphere, such as Alfred T. Mahan and Halford J. Mackinder. In his seminal essay *Geopolitical Hypotheses in a Technological Perspective* (1963), Harold Sprout examined the evolution of the ideas of these two authors, highlighting how both drew inspiration from similar events and foundational concepts, yet arrived at strikingly different predictions. He noted: «Here one beholds two first-class intellects, viewing the same events, each deriving inspiration from the ideas of the other, and both building their geopolitical

[5] The quotations are taken from Jules Verne, *Around the World in Eighty Days*, Andrews UK Limited, 2010, p. 15.

"castles in the air" upon essentially the same earthy foundations. Yet they produced nearly opposite predictions of the shape of future international politics». Sprout identified the contrasting geopolitical visions of Mahan and Mackinder as stemming from their differing evaluations and perceptions of the transformative role of technology. By the late 19th and early 20th centuries, as said, evidence of rapid technological advancement – such as the expansion of railway networks, the emergence of motor vehicles, submarines, and aircraft – was abundant. However, Mahan's intellectual framework, according to Sprout, was deeply anchored in the paradigms of the 17th and 18th centuries focusing almost exclusively on maritime power as the decisive factor in global politics (see Maurer 2023). For Mahan, in fact, the geopolitical future was envisioned as a continuation of the past, where control of sea lanes and naval supremacy remained the ultimate determinants of global power. Consequently, he underestimated the disruptive potential of overland transportation and emerging technologies. Mackinder, on the other hand, was more perceptive to the geopolitical implications of technological change, particularly in the realm of overland transportation. His observations of the Russo-Japanese War highlighted the strategic significance of railways, especially the ability of the Trans-Siberian Railway, to sustain military operations across vast distances. This recognition led Mackinder to predict the possibility that railways would soon proliferate across Asia, fundamentally altering the ability of a great power to reorganize that vast expanse at the heart of Eurasia, thereby shifting the balance of global power.

Clearly, both thinkers acknowledged that the "world had shrunk" thanks to technology, but through what lenses did they filter this transformation[6]? On one side Mahan, an American, with the publication of his 1890 work *The Influence of Sea Power Upon History*, had the right sensitivity to anticipate some of the themes later explored in Frederick Jackson Turner's (1893) famous essay, *The Significance of the Frontier in American History.* Turner underscored that the closing of the American frontier did not mean that: «the expansive character of American life has now entirely ceased». Instead, he foresaw that, «American energy will continually demand a wider field for its exercise». Mahan's work, in this light, offered a vision for the next chapter of American history, proposing that the oceans could serve as that new frontier. As he argued, «Americans must now begin to look outward» (Mahan 1897, 21). At the same time, Mahan recognized that while Americans had long

[6] It is clear that the contrast between Mahan and Mackinder's thought is not as manichean as it might appear in this brief presentation. The goal here is simply to emphasize how their perspectives differed, shaped by the contexts they belonged to, which naturally influenced their objectives. Mackinder was undoubtedly influenced by the Russophobia prevalent in certain British circles of his time, while Mahan was primarily concerned with acting as an advisor to the prince, in this case, Theodore Roosevelt (see Bordonaro, 2018).

viewed the oceans as natural barriers – a cornerstone of what historian Vann Woodward described as «free security», provided primarily by the Atlantic to the east, the Pacific to the west, and the Arctic to the north – advancements in technology were transforming naval warfare[7] and for this reason it was now time to leverage these oceans not as barriers but as avenues for projecting the American power, fostering economic growth, and achieving greater security in a shrinking world[8].

On the other hand, Halford Mackinder, as a British geographer, approached the implications of technological advancements from a fundamentally different perspective. While Mahan, as said, focused on the need of a naval projection to secure American coasts, Mackinder, deeply influenced by Britain's status as a maritime power, directed his attention to the dangers posed by the consolidation of a land-based empire in Eurasia. In fact, he articulated his geopolitical vision in the concern over the possibility that a single dominant power could emerge in the "Heartland" of Eurasia. This power, using a network of interconnected railways, could reorganize the vast resources of the continent and deploy its military forces with remarkable speed and efficiency. Mackinder (1904, 436) warned that such dominance could even extend to naval supremacy, as it «would permit the use of vast continental resources for fleet-building» and that would place global hegemony within reach.

The same innovations can generate contrasting interpretations, depending on what the Sprouts (1979, 28) would have called the "psycho-milieu" of the observers, meaning «images or ideas, derived from some sort of interaction between what he selectively receives from his milieu (via his sensory apparatus) and his scheme of values, conscious memories, and subconsciously stored experience». Understanding the impact of technological transformations on geopolitics requires an analysis that transcends their mere technical innovations and delves into the subjective perceptions of those interpreting and responding to these changes. Rather than engaging in a neutral or purely technical reality, actors operate within a world filtered through their minds, which profoundly influences how they assess risks, opportunities, and strategic priorities. This is not, by any means, an argument that succumbs to constructivism, where facts are dismissed in favor of pure individual interpretation. Rather, it is an acknowledgment that reality must be analyzed with an awareness that different actors

[7] Mahan, in particular, highlights (1890, 86–97) that while a naval blockade of the United States' coasts was previously inconceivable due to the vast extent of the coastline and the prohibitive costs such an endeavor would impose on an enemy power, advancements in ship speed and maneuver had rendered this scenario both feasible and a tangible threat. Consequently, he argued for the necessity for the United States of building a capable naval fleet to keep potential adversaries far from American shores.

[8] For a comprehensive analysis of the role these two authors played in reshaping the American political-geographical imaginary, see Stefanachi (2015, 2017).

apply distinct filters when interpreting events and phenomena, and these filters are themselves part of reality. Furthermore, with the benefit of hindsight and a different perspective, it becomes possible to evaluate whether certain interpretive frameworks were more or less effective in identifying and understanding the constraints, opportunities, and strategic priorities of a given moment.

Just over thirty years ago, the world once again "grew smaller". To many, it seemed as though it had finally consolidated into a unity, an indivisible whole. On one side, the collapse of communism; on the other, the global expansion of capitalist economies, carrying with it the prevailing assumption that the spread of capital would naturally be accompanied by the diffusion of the liberal-democratic paradigm. A globalized unity emerged – one that inherently contained its own contradictions. These were not merely the tensions of previous eras but new contradictions, now de-spatialized, detached from traditional territorial constraints. Phenomena such as international terrorism and economic crises no longer remained confined within specific regions but spread rapidly across the globe, transmitted along the intricate and interwoven networks of global societies and value chains. As Galli and Parsi (2011) noted, this de-spatialization extended beyond economic and security dimensions to the realm of political imaginaries, fostering conceptualizations of a borderless political order, such as the idea of a *global empire*, the universal expansion of democracy, and the assumption that governance and political legitimacy could transcend territorial boundaries.

This flattening of the world, driven by economic, political, and cultural unification, did not simply compress space, but it erased – at least to some extent – traditional notions of distance and territorial and social differentiation. In this context, globalization was not merely seen as a process of integration but one of absorption, where distinct spaces, histories, and sovereignties were increasingly subsumed into a singular framework of interdependence. The result was the proliferation of influential narratives proclaiming the closure of spatiality itself, encapsulated in notions such as *"*The end of history", "the death of distance", and "the end of geography". Whether these concepts were true or not they undeniably reflected the widespread belief at that time that the world had entered a final stage of political and economic organization – one in which territorial divisions and spatial constraints had become obsolete, giving the illusion of a new immutable order that was no longer geopolitical.

This vision of a closed, interconnected, and interdependent world was undoubtedly reinforced just a few years earlier with the disruptive technological change brought about by the emergence of cyberspace – a new reality that, at least in appearance, seemed to completely *de-spatialize* human interactions. A new domain capable of eliminating distances, rendering communication nearly instantaneous, and, perhaps most crucially, enabling financial transactions to occur seamlessly across this new "flat" globe. Cyberspace, precisely because of these effects – and also, in part, due to the

intellectual climate of the time, shaped by liberal ideas and with the illusions of ending the tyranny of territoriality – was widely perceived as a non-territorial, virtual space, a new frontier open to all for the human minds to freely explore. It was imagined as a realm unbound by physical constraints, where individuals and ideas could transcend geopolitical barriers, reinforcing the notion that traditional territorial logics had become obsolete and certainly something that was not applicable in this domain. Many authors (see among others: Hardy 1994; Barlow 1996; Johnson 1996) quickly began to conceptualize cyberspace as a domain requiring entirely new categories of sovereignty and spatiality – a space fundamentally distinct from the physical world and therefore deserving of exceptional treatment. It was envisioned as a free and open realm, one that transcended territorial borders, defied traditional geopolitical constraints, and challenged the very feasibility and legitimacy of applying laws rooted in geographic boundaries. In this view, cyberspace was not simply a technology that helped overcoming physical natural barriers but a radically new frontier, one that demanded a rethinking of governance, jurisdiction, and the very nature of territorial control. Some (Goldsmith, 1998), of course, argued against this *"*cyber exceptionalism*"* and the libertarian vision of cyberspace. However, what is truly striking is that the liberal conviction of the time was so strong that even the United States, as Mueller (2019) points out, under the Clinton administration (Clinton & Gore 1997) fully embraced this exceptionalism. In the broader context of the Washington Consensus (see for instance Gore 2000; Babb 2013), the United States – many countries across Latin America, Eastern and western Europe – were swept up in the liberal euphoria of deregulation and market-driven governance. This ideology, which championed privatization, free trade, and minimal state intervention, naturally shaped the way cyberspace was conceptualized and managed in its early years. Cyberspace was thus allowed to develop outside the traditional frameworks of state control, its intricate and delicate web of cables, antennas, and nodes expanding according to the purest logic of liberalization, decentralization and, naturally, following a pure demand-driven model. The prevailing belief was that a self-regulating, borderless network would foster economic prosperity, global connectivity, and ultimately capable of bringing about the diffusion of liberal democratic values all over the world.

Cyberspace emerged as both a reflection and a catalyst of the prevailing liberal vision of a post-historical, borderless world. As a technological phenomenon, it reinforced the perception of an interconnected reality, where physical distance no longer constrained human interaction, economic exchange, or political engagement. Yet, at the same time, it was conceptualized through the very same ideological filters that had defined the era – imagined as an inherently open, self-regulating space, detached from the mechanisms of state power and immune to the constraints of territoriality. This reciprocal dynamic solidified the illusion that cyberspace existed beyond geopolitics, a domain where

markets and ideas could flow freely, unencumbered by the traditional logics of sovereignty and strategic rivalry. An illusion, of course, that not only shaped its early development but also produced long-lasting effects on its management, persisting for decades. Even in the face of mounting warnings about the security risks and vulnerabilities inherent in this unregulated, decentralized approach, it took a prolonged and gradual process for states to reconsider their initial assumptions. The shift in perspective was neither immediate nor linear, as we will see later in the case of the United States, analyzing the DoD strategies for cyberspace; despite clear indications of emerging threats, the entrenched belief in a borderless, self-regulating cyberspace delayed meaningful policy responses and strategic adaptations. Only over time did states come to recognize that this "non-space" was not detached from power dynamics but deeply intertwined with geopolitical competition and national security imperatives.

Today, the liberal euphoria has largely faded, and the international system has undergone a profound transformation. The transition to a global order distinct from American hegemony to a contested world (see Colombo 2025) – if not yet fully realized under every dimension – is undeniably underway. As a result, new analytical filters are required to understand cyberspace, filters capable of capturing its materiality, vulnerabilities, threats, and strategic opportunities. It is therefore essential today to reassess cyberspace through the recovery of spatial concepts, bringing geographical analysis back to the forefront in order to grasp the implications of its complex and multifaceted infrastructural topology. This also means bringing back to the center of the debate the relationship between politics and space, as states seek to reclaim – or preserve, as rightly pointed out by Galli & Parsi (2011) – the logics of sovereign political control over territory. While spatial control is not the only determinant of power, it remains one among others and must be understood and represented as such even when addressing cyberspace. Finally, it is essential to understand how the Schmittian political distinction – the most political of all categories, between friend and enemy (Schmitt 2007 [1932]) – becomes just as central in cyberspace, a domain once "flat", immaterial and "post historical", and now contested and full of enemies.

This chapter aims to critically engage with the scholarly debate on globalization, a debate that has long been polarized between two opposing visions: on one side, those who argued that globalization had steered the global order in a world where economic interdependence and technological progress had dissolved traditional boundaries. On the other, those who maintained that these ideas were mere illusions, and that the constraints of geography, the persistence of political conflict, and the primacy of strategic considerations had never truly disappeared. This work firmly aligns with the latter perspective, arguing that the belief in a post-historical, post-geographical order was a delusion even

in the cyber realm. In fact, by engaging with this debate, the chapter seeks to reconstruct the evolution of the conceptualization of cyberspace, from its techno-political inception, then tracing how it was initially defined and imagined, shaped by the dominant ideological frameworks of the time, and how this perception has gradually eroded in the face of new geopolitical and security realities. The originality of this review lies in its approach to narrating the history of the Internet and cyberspace, steering away from the conventional "mythical" foundation story centered on visionary American engineers and computer scientists (Isaacson 2014). While these accounts remain important, this work move the focus toward the political forces that have shaped the development of cyberspace, emphasizing the strategic imperatives, ideological frameworks, and political pressures that have influenced its trajectory. Following insights from the literature, I have outlined three distinct phases in the evolution of cyberspace: the Cold War phase, in which its emergence was driven by strategic and prestige-related concerns; the era of the liberal illusion, from the late 1980s to the early 2000s, the era of an open, borderless and free domain; and finally, the phase of insecurity, spanning from 2001 to the present, characterized by growing concerns over state-based cyber threats, digital sovereignty, and the securitization of cyberspace. However, it is important to introduce, from the outset, an obvious principle of caution. In fact, it is better not to push too far with the elegance and coherence of the periodization. These should not be considered as rigid, definitive periods, as the three marked periods are intended to be broad phases within each of which we find elements that also characterize the subsequent or preceding period. Nonetheless, the goal is to provide a temporal and spatial reference (we refer mainly to the trajectory of cyberspace as experienced and perceived by the United States and the Western world) for the different stages that this domain has undergone.

Throughout this analysis there is a sustained focus on how these phases reflect changing perceptions of space and geography. Naturally, the way we conceive geography is inextricably linked to technological developments, as innovations reshape our relationship with physical space and redefine how we perceive as geographical data. Yet, technology itself does not exist in a vacuum, its meaning, function, and implications evolve alongside broader political transformations.

Central to the analysis is the examination of how early visions and definitions of cyberspace – deeply embedded in the logic of liberal globalization, deregulation, and technological utopianism – initially framed it as a metaphorical space detached from traditional power struggles, where sovereignty was obsolete and governance could be decentralized and self-regulating. Yet, as this chapter will demonstrate, these assumptions have proven untenable. The very forces that once seemed to dissolve territorial constraints have, over time, contributed to their reassertion, leading to the fragmentation of what was once imagined as an open, global, and unified virtual space. This process of re-

territorialization underscores that the fundamental dynamics of power, control, and geopolitical competition have not only persisted but have become increasingly relevant in cyberspace, much as they have always been in the physical world.

The Political Cradle of Cyberspace

In order to undertake an examination of the history of cyberspace and the Internet, it is necessary to first explore the «prehistory of the Internet», as defined by Madeline Carr in her seminal work *US Power and the Internet in International Relations: The Irony of the Information Age* (2016, 46). This phase must be situated within the context of technological competition between the two superpowers during the Cold War after 1956, and it represents a crucial preliminary stage in the evolution of the Internet as we understand it today. Those were the years of nuclear and space competition during the Cold War, the period of the so-called "competitive coexistence". It was an era characterized in the West by a widespread conviction that, after a prolonged and patient waiting period – perfectly in line with what was predicted in 1946 by George Kennan in his *Long Telegram* – the inherent contradictions of the Soviet communist system would eventually surface, demonstrating the political superiority of pluralistic institutions and the greater efficiency of the market economy system (Di Nolfo 2020, 384–540).

Nevertheless, the Americans viewed with considerable concern and surprise Khrushchev's ability to swiftly occupy the spaces left vacant by the United States, presenting the Soviet model as an equal and opposite alternative to the American one. The control of their respective spheres of influence and the credibility with which the two superpowers could position themselves to reorganize the global chessboard to their advantage naturally also involved technological and nuclear competition – most evident in the race to develop intercontinental ballistic missiles (ICBMs) and to be the first to launch an artificial satellite into space. The Americans were convinced that they had a significant advantage in both competitions and precisely because of this deep-rooted belief, the announcement of the Soviet Union's launch of Sputnik on 4 October 1957 provoked in the U.S. reactions bordering on hysteria (Di Nolfo 2020, 404). The announcement of Sputnik's launch, for instance, prompted then Senate Majority Leader Lyndon B. Johnson to remark that «soon they will be dropping bombs on us from space like kids dropping rocks on cars from highway overpasses» (Carr 2016, 47). The perception of being overtaken in the space race, combined with Soviet advances in missile technology, transformed the previously theoretical threat of attack into a tangible reality, leading to widespread panic inflicting

a severe blow to American security and prestige – both essential factors in maintaining credibility in the eyes of its allies.

Out of this profound state of anxiety came the need to "catch up" and surpass the Soviets, to regain control of the technological race. Thus, driven by the need of a renewed security space and simultaneously following a thymotic impulse to restore American prestige, the federal government funded and promoted several initiatives aimed at reestablishing U.S. dominance in global science and technology. Among these – parallel to the reinforcement and refinement of the U.S. nuclear arsenal and the capability to launch artificial satellites into space – was the establishment in 1958 of the Advanced Research Projects Agency (ARPA), specifically tasked with regaining America's leading edge through the application of cutting-edge technology to military capabilities. ARPA identified promising projects within the research and development community, providing essential funding and support to advance their objectives. Among ARPA's earliest research initiatives, as described by Carr (2016, 46–50), there was a project driven by the government's goal of interconnecting large computer systems to maximize their capability to support other research. During this period, computers were exceptionally costly and possessed computational resources far exceeding the requirements of the limited number of individuals who had access to them but by networking these computers, particularly across the globe, ARPA anticipated that their substantial capacities could be more fully and effectively utilized. This was expected to foster significant advancements in various fields of scientific and technological research dependent upon robust computational resources and crucially – as noted by Tarnoff (2016) in his brief history of the Internet – this initiative was also envisioned as a means of fundamentally transforming the management of global military communications: «Picture a jeep in the jungles of Zaire, or a B-52 miles above North Vietnam. Then imagine these as nodes in a wireless network linked to another network of powerful computers thousands of miles away. This is the dream of a networked military using computing power to defeat the Soviet Union and its allies. This is the dream that produced the internet» (Tarnoff, 2016).

As early as the late 1950s, ARPA had begun funding and supporting research that would later bring about the development of networking protocols, both internally within its own research divisions and externally through collaborations with prominent academic computer scientists throughout the United States. As networking technologies matured and practical computer networking became more feasible, ARPA and collaborating researchers began to conceptualize specific applications of these emerging technologies. As said, a key envisioned application was the creation of a secure communications network to enhance US military communication and to organize credible second-strike capabilities in the event of a nuclear conflict (Abbate 2000, 10-13). At the time, existing

communications infrastructures – meaning the telephone and telegraph – relied on a fundamentally vulnerable architecture characterized by a central node through which all messages were routed and then redistributed to their recipients, the so-called *circuit switch* model (Baran 1964, 2).

This specific context served as the cradle for the emergence of the Internet and cyberspace, shaped by strategic and political imperatives that profoundly influenced the design of early networks. From its inception, then, the network architecture was built around military objectives, embedding them within its technological framework. It prioritized resilience, flexibility, and high performance, while commercial factors such as cost efficiency, simplicity, and consumer appeal remained secondary (Abbate 2000, 6). With these objectives in mind, researchers at ARPA conceptualized and eventually adopted *packet switching*, a novel approach to data transmission that departed from the conventional circuit-switched model of telephone networks. Instead of establishing a dedicated, continuous connection between two communicating parties, packet switching fragmented messages into smaller, independent packets – bite-sized units – that could travel across the network through multiple possible paths before being reassembled at their destination (Steed 2019, 8-9).

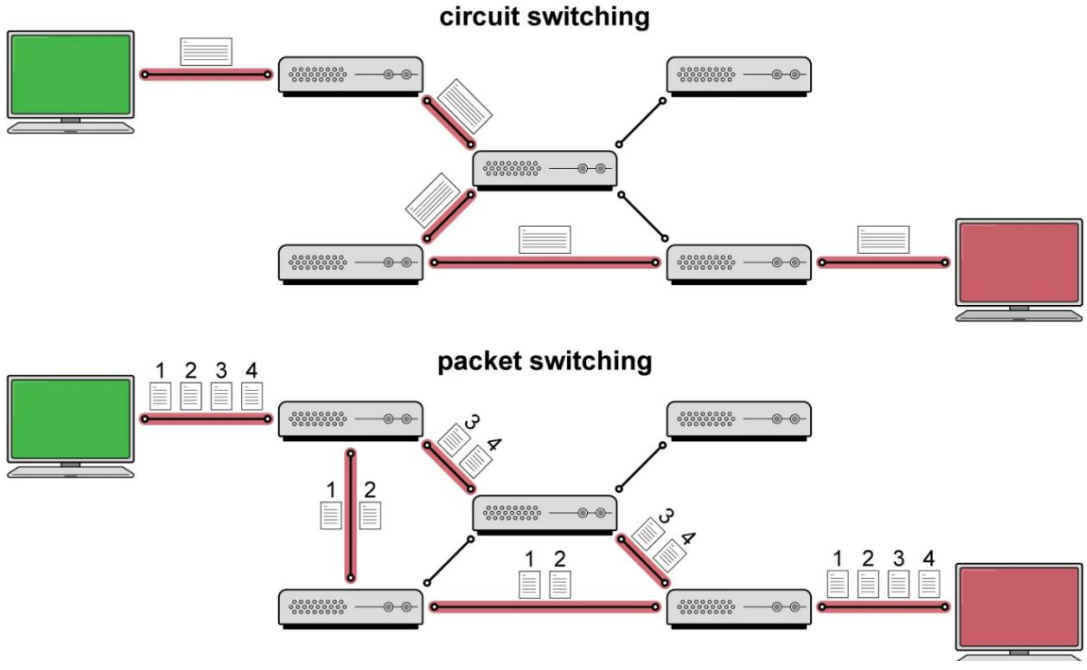

Figure 1 - Packet Swithcing Network and Circuit Switching Network (Encyclopædia Britannica)

In terms of security, this decentralized routing mechanism not only strengthens the network's ability to withstand failures, including the destruction of certain central nodes, but also makes interception

and targeted denial of service significantly more difficult. Since data does not travel along a predetermined path, it becomes harder for adversaries to monitor or block communications effectively. These characteristics, as Steed (2019) emphasizes, were central to the strategic and security-driven design of early networks and remain key advantages of packet switching in modern cyberspace infrastructure.

ARPANET was the first publicly accessible packet-switched network and marked a fundamental shift in computer communications. Its first successful test took place in October 1969, following an intensive year of development led by the technology consultancy firm Bolt Beranek and Newman (Britannica, *cit*.). The network's design was based on the theoretical models and technical innovations of Paul Baran and Donald Davies, whose pioneering work on packet-switching provided the foundation for ARPANET's decentralized architecture. Initially, this network only connected four locations: the University of California at Los Angeles, Stanford Research Institute, the University of California at Santa Barbara, and the University of Utah. Over the following years, the network expanded significantly, reaching 57 nodes by 1975 and as Carr (2016, 49) notes, by the end of the decade, the number of connected computers had grown to approximately 200, despite remaining restricted to government and scientific institutions, serving primarily as an experimental research tool rather than a publicly available communication network. Steed (2019, 10) emphasizes that while packet switching revolutionized data transmission across networks, it also necessitated the establishment of a standardized communication protocol to ensure interoperability between computers, networks, and data packets. This necessity arose from the fact that different networks operated with incompatible protocols, obstructing data exchange. To resolve this issue, a universal framework was required – one capable of facilitating consistent communication across heterogeneous networks. This led to the development of the Transmission Control Protocol/Internet Protocol (TCP/IP). On January 1, 1983, ARPANET fully transitioned to TCP/IP, following its adoption as the U.S. Department of Defense's standard protocol in 1980. This protocol was designed to address the complexities of large-scale networking, ensuring both stability and data integrity, even in cases of packet loss or corruption. The protocol was structured in two layers: TCP managed the segmentation of large data blocks into smaller packets for transmission, while IP handled addressing and routing to ensure that packets reached their intended destination. The adoption of the TCP/IP system by computer networks solidified the distributed structure of the Internet, freeing it from centralized control. In its early days, in fact, each connected machine functioned as an independent node, contributing to the emergence of a fully decentralized framework. However, as institutions, universities, government agencies, and private enterprises, began interconnecting their systems, these individual machines coalesced into autonomous subnetworks – the so-called autonomous systems

(AS) – each managed under a distinct administrative domain. With TCP/IP providing a common language and the development of inter-network routing protocols (first the Exterior Gateway Protocol – EGP, and later, from 1989, the Border Gateway Protocol – BGP), these subnetworks wove together into a more structured and resilient web (Limonier et al. 2021). It is interesting to note, as reported by Blum (2012, 55), how rapidly the number of AS expanded: from 15 in 1982 to over 400 by 1986 (and as of 2025 exceeding 100.000 AS. See Regional Internet Registries Statistics, retrieved January 2025)).

As the 1980s unfolded, the rise of electronic mail (email) and bulletin boards ignited a surge in networking's popularity, extending beyond research and military. Meanwhile, the personal computer (PC) market was booming. Carr (2016, 50) writes that sales in the United States skyrocketed from just 40,000 units in 1975 to a staggering 6.6 million in 1985. Indeed, unlike the massive and expensive mainframes used by universities, government agencies and large corporations, PCs were far more affordable, making them an attractive option for businesses. This shift reshaped the focus of network technology developers, moving them away from institutional mainframes and towards desktop computers. As demand for PCs soared, private companies invested in commercial networking services that allowed users to connect their machines for file sharing and communication, whether within their offices or across national and global networks. It was during the 1980s, as this new telecommunications system expanded to the public, that the term "cyberspace" was first coined by science fiction writer William Gibson – the first to put into words the growing awareness that something entirely new was taking shape. This was not merely perceived as a technical evolution but the emergence of a different kind of reality. The perception of cyberspace quickly moved beyond the physical infrastructure of interconnected computer networks and the cables through which fragmented packets of information traveled. Instead, fascination shifted to the abstract realm of bits, drawn into the *mise en abyme* of the monochrome green screen of the monitors. It was an awareness that no longer fixated on the tangible mechanics of networking – that represented the crown jewel of American technology, which, along with other breakthroughs in innovation and science, served as a redemption for its prestige and technical capability against its Soviet rival – but instead began to imagine a new world, a virtual, untethered, and completely disjoint form the physical one.

In his "Neuromancer", Gibson (1989, 128), described cyberspace as:

A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding [...].

Giving the first definition of this realm, he referred to what another scholar (Garvey 2021) – drawing a parallel with the human body and its dualistic vision, that is, mind and body – would later describe as «the mind of cyberspace». According to Garvey (2021), cyberspace can be understood through a dualistic perspective, much like the human being, composed of both a body and a mind. The body is represented by its physical infrastructure: the hardware that stores information, the cables and networks that transmit data, and the devices – whether analog or digital – that facilitate communication. Just as the human body comprises organs, veins, and the biological systems that sustain it, cyberspace relies on a structured system of physical components that allow for the transmission and storage of information. The mind of cyberspace, on the other hand, emerges from the organization of this physical infrastructure into meaningful patterns. While, at a fundamental level, data consists of nothing more than electrical signals encoded as binary 0s and 1s, it is their structured arrangement that produces meaning and functionality within cyberspace. As Garvey (2021) explains:

Analogous to how the concept of the word 'concept' flowing to the author's mind while typing this at the moment is nothing more than just blood and electrical signals flowing through the brain and being transmitted to fingers to move in specific ways to strike certain letters on the keyboard to create the word 'concept,' the brain's organization of this information, namely the electrical signals, is what gives the word 'concept' meaning.

In this way, the mind of cyberspace is not merely the sum of its physical components, but rather the way information is structured, categorized, and made intelligible through ontologies, taxonomies, and conceptual frameworks. Just as human cognition arises from the organization of neural activity rather than from individual neurons, cyberspace's cognitive dimension is embedded in the way data is processed, classified, and interconnected. This intangible and abstract vision of cyberspace, detached from any spatial implications or technical connotations, has influenced numerous authors in their depiction of this reality. Similarly, in fact, Bruce Sterling in his "The Hacker Crackdown" (1992) defined it as: «the place between the phones. The indefinite place out there, where the two of you, two human beings, actually meet and communicate». The security computer analyst Winn Schwartau (1994) writes something similar in his "Information Warfare: Chaos on the Electronic Superhighway", defining cyberspace as:

> That intangible place between computers where information momentarily exists on its route from one end of the global network to the other... the ethereal reality, an infinity of electrons speeding down copper or glass fibers at the speed of light... Cyberspace is borderless... [but also] think of

> cyberspace as being divided into groups of local or regional cyberspace—hundreds and millions of smaller cyberspaces all over the world.

Naturally, this is not to suggest that these authors were unaware of the physical, material, and tangible dimension of cyberspace. Rather, the intention is to highlight the particular interest that emerged in exploring its more abstract and immaterial aspects, with inevitable consequences for how the governance of this space and its security were conceived. The geopolitical competition between the two superpowers of the Cold War was gradually giving way to a new era in international politics – a unique historical moment that shaped the worldview of many and, consequently, the general perception of cyberspace. The global explosion of cyberspace and the Internet, as Steed (2019, 27) puts it, «occurred at the height of the Western liberal triumph» (on this see also Fidler 2014) – bringing with it far-reaching implications for conceptions of space, territoriality, borders, politics, and geography. Here, we enter the true developmental phase of cyberspace, its expansion, evolution, governance, and security frameworks. This marks the beginning of cyberspace history in the liberal era, a period that, at first glance, can appear entirely apolitical and aspatial. Yet, beneath this surface, cyberspace was deeply entangled with the ideological and political currents of its time.

"It's the economy, stupid!" Cyberspace in the Flat World

The disappearance of the Soviet threat, although foreseeable in light of the initiative for a new détente aimed at overcoming the Cold War – articulated by Mikhail Gorbachev upon his appointment as General Secretary of the Communist Party of the Soviet Union in March 1985 – materialized with the fall of the Berlin Wall and culminated in the definitive dissolution of the USSR in 1991. This event marked the beginning of an entirely new phase for the international order, which was characterized by the undisputed primacy of the United States as the sole remaining superpower. The democratic-capitalist system emerged as the victorious model, perceived not only as the most successful but also as the most attractive and aspirational system for nations worldwide. The liberal order, built upon institutional pillars such as the Atlantic Alliance, the International Monetary Fund, the World Bank, and the General Agreement on Tariffs and Trade – later replaced by the World Trade Organization – was firmly anchored in American leadership. Having triumphed in the Cold War, this system now felt justified (and indeed convinced itself) in reaffirming and expanding its influence across the globe, unleashing its universalist and globalizing ambitions (See Barié 2013, Parsi 2018).

Certainly, the Clinton administration perfectly embodied this vision, reinforcing American global economic leadership by championing free markets and pursuing "enlargement" policies aimed at actively promoting democratization and human rights. Clinton's foreign and economic policies became closely intertwined in a symbiotic relationship (see, as his vision of democratic expansion through trade, the advancement of human rights, and the globalization of markets coalesced into a comprehensive ideological and economic "grand strategy" (Carr 2016, 55). The administration promoted a worldview centered on openness and interconnectedness through trade and technology, establishing a foreign policy doctrine that reflected a renewed approach to the post-Cold War international landscape, explicitly defining democracy and free markets as the foundational pillars of American values. Although Clinton entered the presidential race with little foreign policy experience, he successfully compensated by adopting many of the free-market slogans of his Republican rivals (Del Pero 2022 [2008], 407). These economic principles not only shaped his domestic agenda but also permeated his foreign policy approach. Prioritizing economic concerns over security issues, he encapsulated his vision in the now iconic slogan: «It's the economy, stupid!» – a phrase that came to symbolize the new presidential mindset. Moving away from the old Cold War doctrine of containment, the Clinton administration embraced a new vision of American internationalism: it was now the time for an «enlargement», in the words of Clinton's National Security Advisor, Anthony Lake (Del Pero 2022, 408). This strategy centered on globalization, the removal of trade barriers, the active promotion of human rights, and the easing of burdens and commitments inherited from the Cold War, including substantial reductions in military spending. The resources freed from these cuts were to be redirected toward advancing technological innovation and economic competitiveness. As Clinton himself argued:

> We need to sharply increase our national commitment to research and development [R&D]. Japan and Germany spend half again as much on civilian R&D as we do, and have the productivity growth rates to show for it. Every dollar we take out of military R&D in the post-Cold War era should go to R&D for commercial technologies, until civilian R&D can match and eventually surpass our Cold War military R&D commitment […] We should create a civilian research and development agency to support research in the few dozen strategic technologies that scientists have already identified as the basis for launching new growth industries over the next two decades, and revitalizing traditional ones. The civilian DARPA will coordinate R&D to help companies develop innovative technologies and bring new products to market. And without inhibiting the competition that drives innovation, we will encourage and promote collaborative efforts among firms and with research institutes for commercial development just as we have done with defense technologies for 40 years (Clinton 1992).

This vision reflected a clear shift from military preeminence to economic leadership, positioning technological progress and commercial innovation as the new pillars of American global influence. This strategy was not meant to be confined within domestic borders but rather embodied a universal vocation – a vision that sought to encompass the entire world within a single, integrated economic and technological space. As Clinton articulated in his 1993 address to the United Nations, «From beyond nations, economic and technological forces all over the globe are compelling the world towards integration. These forces are fueling a welcome explosion of entrepreneurship and political liberalization» (Clinton 1993). This conviction – that globalization, fueled by technological growth was an unstoppable force driving economic expansion and liberalism – was not limited to the Clinton administration but permeated various levels of American society, from academia to government institutions. The United States, in those years, fully embraced its global identity, seeing itself at the center of a new interconnected world where economic and technological leadership defined power. The Clinton era coincided with the boom of the so-called *New Economy*, a phase of rapid economic growth driven by the rise of the internet and digital services. These years saw the revolutionary expansion of online business models, the emergence of major technology corporations, and the exponential growth of companies like IBM and Apple in the hardware and software sector. At the same time, the rise of internet-based enterprises such as Google and Amazon reshaped markets, laying the foundations for the digital economy that would define the decades to come (Borgognone 2018 [2013], 279).

This transformation also produced a series of powerful narratives about the new global order – myths that were enthusiastically embraced and theorized also within academic circles. Scholars and commentators sought to define and frame this historic shift, often encapsulating it in striking titles that captured the excitement and momentum of the time, reinforcing the idea that technology, markets, and liberalism were the driving forces of the future. Notably, *The End of History* (Fukuyama 1989) proclaimed the definitive triumph of liberal democracy, while *The End of Geography* (O'Brien 1992) theorized a world where economic and financial flows transcended physical borders. Similarly, *The Death of Distance* (Cairncross 2000) captured the idea that advancements in communication technology had rendered geographical constraints irrelevant, and *The World Is Flat* (Friedman 2007) reinforced the vision of an increasingly interconnected and leveled global playing field. While the notions of "the end of history", "the end of geography", and "a flat world" certainly reflected relevant aspects of globalization – capturing how politics and space and technology were conceived at the time – these notions, though today subject to irony, were emblematic of a widely shared common-sense and worldview. They framed globalization as an irreversible process tied to democratic liberalism, shaping a common understanding of the transformations underway and raising necessary

questions that, at the time, had to be addressed. Certainly, the technological and political changes unfolding during those years needed to be understood, and adequate conceptual tools were required to grasp their full implications. It must also be acknowledged, however, that the analyses put forward by these authors were not as simplistic or naïve as they might seem when framed in this discussion. Their work reflected serious attempts to grasp the profound shifts taking place, and while some of their conclusions may today appear overly optimistic, they certainly offered valuable insights. At the same time, however, they contributed to a profound and general misreading of power relations in the international system. They fueled the illusion that states had lost their centrality, that territoriality had been definitively erased by technological advancements, and that politics could be substituted with the economy and the digital interconnection would create a "global village", effectively making the world "flat".

It is no coincidence that, by the early 1990s, there was a growing sense that geopolitics had been declared dead (Ó Tuathail, 1998), prompting a reconsideration of the very categories of geography and politics. Precisely from the recognition of the epochal change brought about by the end of the Cold War, traditional geopolitical considerations seemed to lose their significance. The frameworks that had long defined international relations, rooted in territorial divisions and strategic rivalries, appeared increasingly inadequate in explaining a world reshaped by economic globalization, technological advancements, and the rise of new forms of connectivity. This shift challenged established geopolitical thinking, calling for a reevaluation of the spatial and political dynamics that structured global affairs. As Ó Tuathail (1998, 2) puts it – in the first chapter of a volume dedicated to the project of founding new "critical geopolitics" – their endeavor of reviving geopolitics was «not dedicated to resurrecting traditional themes of geopolitics» but rather an attempt to analyze the geographical representations and practices that actively contributed to shaping the spaces of global politics (Agnew, 1998). This was the lens through which cyberspace was viewed, the perspective that enabled its expansion – one driven by market logic, with politics pushed to the sidelines, left to observe with the near-certainty that, sooner or later, it would fade away, making room for something else. Within this framework, cyberspace was imagined as a realm that transcended territorial constraints, a «space of the mind» (Barlow 1996) – as some libertarians envisioned it – conceived as an untouchable domain, beyond the reach of states and their sovereignty. It was a space of individualism, of private actors, of the singular over the collective. Even Karl Schlögel, an author certainly not indifferent to the enduring relevance of geography, in his volume *In Space We Read Time* (2016 [2003]), comes to the conclusion that cyberspace should not be viewed merely as an infrastructure but rather as a territory fundamentally disconnected from the physical world. He refers to it as *«Cyberia»*, describing it as «a territory constituted and made cohesive by digital information.

It does not end at the borders of the nation-state, and in fact poses a fundamental challenge to its sovereignty. It is connected to the entire world and thus transcends the limitation of local commitments. Cyberia is what the nation-state once was: an imagined community, the digital nation». In many ways, cyberspace embodied all the prevailing myths of its time: it transcended history, politics, space, and distance. As Mosco (2004, 2-3) observed, «cyberspace embody and drive important myths about our time. Powered by computer communication, we would, according to the myths, experience an epochal transformation in human experience that would transcend time (the end of history), space (the end of geography), and power (the end of politics)». This perspective was evident even in the early definitions of cyberspace, which, as we have seen, focused primarily on its immaterial aspects – those that rendered it an a-geographical and a-political reality. Even its very name (on this, see Scholte, 2007) was coined to distance itself from the materiality of the term Internet, which referred merely to the physical interconnection of networks. Here, that physicality was deliberately left behind; even bits themselves – electrons in essence – lost their physical connotation, transforming cyberspace into a realm of "pure spirit", a place where humanity could unite under the banner of freedom. This romanticized vision of cyberspace persisted for a long time (see for instance Obama's International Cyberstrategy of 2011, and Fidler 2014), carried forward by the momentum of a liberal (at times libertarian) mentality, ultimately shaping a set of policies that guided its technical development. The principles of deregulation and privatization came to define its governance, fully embracing an economic-driven logic that ultimately "betrayed" its original strategic-military conception in favor of market imperatives.

It was, in essence, a decision of the Clinton administration, which, as mentioned, stood as the ultimate emblem of liberal triumph, that led to the governance of the internet being treated «as a matter for the private sector» (Steed 2019, 29). Viewing this emerging reality through a liberal lens and perceiving no political enemy on the horizon – only criminal threats – the administration allowed cyberspace to experience what Steed (2019, 31) describes as an «apolitical honeymoon». Starting in the mid-1990s, the Clinton-Gore duo developed a series of policies intended to manage the transition of the internet from a network primarily funded and operated by the federal government to one that was open, accessible, privately owned, and integrated into commercial activities. However, this objective was not achieved without resistance, as the Clinton administration initially faced opposition from Congress, which was wary of allowing private companies to profit from a project funded by taxpayers (Carr 2016, 57). At the time, the internet was operated under the oversight of the National Science Foundation (NSF), which according to the US government had to only have a temporary role, before transferring control to private stakeholders. Yet, to make commercialization politically viable, the privatization of the internet's infrastructure had to come first. The NSF gradually permitted

commercial operators to establish their own networks, which could interconnect with the NSF backbone while relying on privately funded infrastructure. Additionally, the NSF outsourced internet services to the private sector, fostering the development of Internet Service Providers (ISPs). By April 1995, this strategy culminated in the decommissioning of the NSF backbone, effectively transferring control of the internet into private hands (see Mullally 2024).

This shift toward privatization was further reinforced by the Telecommunications Act of 1996 (Congress 1996) which marked a crucial turning point in the deregulation of digital and communications infrastructure in the United States. Following the Clinton administration's commitment to a market-driven approach to connectivity, the Act was designed to promote competition and investment, breaking down regulatory barriers between previously separate telecommunications sectors. It allowed telephone, cable, and internet service providers to enter each other's markets, accelerating the deployment of broadband infrastructure and reshaping the geography of global connectivity, particularly through its impact on submarine cable networks (see Starosielski 2015, 45-63). Until then, the global submarine cable infrastructure – probably the most important of the physical components of transmission, the very element that truly makes cyberspace global – had largely followed the routes established by historic telegraph and coaxial cables, maintaining a relatively stable spatial distribution for over a century that reflected a political and strategic logic rather than commercial considerations (on this see Kennedy 1971; Starosielski 2015, 38-44)[9]. However, as deregulation unleashed a wave of private investment in telecommunications, the construction of new submarine cables increased dramatically in the late 1990s, transforming the topography of global communications and leading to what Starosielski (2015, 48) describes as a «global boom in cable laying».

As the internet expanded commercially, governance complexities emerged, particularly concerning the management of domain names – the unique addresses that identify websites and enable users to access them through a structured naming system (e.g., .com, .org, .gov). The existing informal mechanisms, which had been suitable for a smaller, non-commercial internet, struggled to scale with rapid global growth. In response (on this see Steed 2019, 21-30), the U.S. government facilitated the creation of the Internet Corporation for Assigned Names and Numbers (ICANN) in 1998, establishing a private, non-profit organization responsible for managing the internet's system of unique identifiers, including domain names, IP addresses, and protocol parameters. Alongside ICANN, other key

[9] The history of submarine cables, their relevance, and the logic of their different topographies will be expanded in the second chapter of this dissertation.

organizations emerged during the ‘90s as part of the multi-stakeholder model that would define internet governance. The Internet Society (ISOC), founded in 1992, played a crucial role in promoting the open development and use of the internet. The Internet Engineering Task Force (IETF), under the oversight of the Internet Architecture Board (IAB), was responsible for setting technical standards and ensuring interoperability. The World Wide Web Consortium (W3C), established in 1994, developed protocols and standards for web functionality. Additionally, regional Internet registries (RIRs) took on the task of managing the allocation of IP addresses worldwide, preventing fragmentation in an increasingly global network.

Whether the creation of ICANN was primarily motivated, as Carr (2016) suggests, by the strategic objective of securing U.S. dominance over the digital sphere, or whether it stemmed from the genuine need to foster order on an increasingly fragmented and unregulated system (Steed 2019) remains a matter of debate. More likely, both considerations played a role. However, as Raustiala (2017) highlights, that the latter interpretation gains credibility when considering that in 2016 the Obama administration formally relinquished U.S. government oversight of ICANN, and the decision was intended to «protect the fundamental features of the Internet nearly everyone cares about most: its openness, diversity, and fundamental resilience» (Raustiala 2017). Certainly, American interests were safeguarded during the definition of the Internet governance, or at the very least, there was a deep-rooted belief in the American leadership at the time that promoting a multi-stakeholder governance model aligned with U.S. strategic objectives. This approach was fully consistent with the American goal in reducing state intervention and costs. The aim in fact, was to enable this emerging reality to operate with a degree of autonomy from direct U.S. control, based on the firm conviction that, guided by market forces and the principles of supply and demand, cyberspace – the ultimate liberal domain – would naturally foster the global diffusion of liberal-democratic values, without necessitating direct American control.

This conviction is evident in the words and beliefs of Vice President Al Gore, who, in 1994, clearly articulated this vision. Although it was widely acknowledged that the Internet was fundamentally an American creation, Gore, during his speech at the International Telecommunication Union (ITU) conference in Buenos Aires in March 1994, advocated for a broader, more inclusive perspective – one that, while advancing American interests, also aspired to something greater. He declared:

> Let us build a global community in which the people of neighboring countries view each other not as potential enemies, but as potential partners, as members of the same family in the vast, increasingly interconnected human family. […] The GII will not only be a metaphor for a functioning democracy, it will in fact promote the functioning of

> democracy by greatly enhancing the participation of citizens in decision-making. And it will greatly promote the ability of nations to cooperate with each other. I see a new Athenian Age of democracy forged in the fora the GII will create.

This was the American vision of globalization – the belief that even potential enemies would, once economically interconnected and exposed to this reality capable of embracing the entire globe, see all tensions and divisions disappear, at least gradually. Through instantaneous communications, the sharing of values, and the common education and global transmission of this knowledge, the world would smooth out all its rough edges and irregularities. This space – created for the human family – belonged to everyone. Indeed, Gore affirmed that «The Global Information Infrastructure will help educate our children and allow us to exchange ideas within a community and among nations. It will be a means by which families and friends will transcend the barriers of time and distance».

It must be noted, of course, that neither Clinton nor Gore were so naive as to overlook the potential risks and challenges involved in achieving these objectively utopian goals. In the same speech, Gore himself acknowledged the difficulties, emphasizing: «In too many parts of the world, political unrest makes it difficult or impossible to maintain existing infrastructure, let alone lay new wire or deploy new capacity. How can we work together to overcome these hurdles». However, once again, the proposed solution laid in cooperation, leveraging the very interconnection of these systems as a means to bridge global divides. As Gore stated: «First, we can use the Global Information Infrastructure for technical collaboration between industrialized nations and developing countries». On another occasion, as Carr (2016, 62) noted, Clinton showed to be well aware of the potential risks that Americans faced in making this interconnection so pervasive:

> Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States. Our economy is increasingly reliant upon interdependent and cyber-supported infrastructures and non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.

However, maintaining his optimistic outlook, Clinton believed that the solution could this time come from the market. Given that the infrastructure was now mostly in private hands, he was convinced that market-driven incentives should be the primary mechanism for addressing cybersecurity challenges. Moreover, he argued that the best way to involve the private sector in protecting national infrastructure was through voluntary participation, rather than state-imposed regulations. These two principles – the market as the most effective tool for ensuring national cybersecurity and the voluntary

engagement of private actors – became the cornerstone of U.S. cybersecurity strategies for a long time (Carr, 2016).

During the Clinton presidency, the United States embraced the idea of relinquishing control over Internet governance, presenting it as a gift to the human family rather than a mere instrument of power. This, understood in terms of hard power, cyberspace was nevertheless the tool best suited to act as a leveling and homogenizing force, capable of fostering pluralization and democratization of information. This was achieved through the establishment of norms and standards, public diplomacy campaigns to sway opinion, and the provision of infrastructure and technology to support human rights activists. In short, it was an apparently neutral instrument, yet one inherently capable of influencing and generating attraction toward the Western and American world. Thus, cyberspace became the quintessential vehicle for projecting American soft power (Nye 2010, 9).

The vision was for cyberspace to develop in an apolitical and neutral way – an extension of the liberal belief that free markets and open exchanges would naturally lead to global progress, an idea that, in the author's view, is clearly far from being truly apolitical. However, this borderless and unregulated vision of cyberspace did not pass the test of time. Several factors, in fact, contributed to this gradual shift. First, the changing international balance of power, marked by the emergence of a multipolar world order and the gradual erosion of U.S. hegemony (Ikenberry 2018), or at least its declining willingness to fully commit to maintaining its global hegemony. Secondly, cyberspace, once the "home for the minds" of all individuals, gradually transformed into a contested space where security concerns could no longer be overlooked. Over time, a range of threats emerged, shaping the strategic landscape of the digital realm. Among these, cyber-enabled hybrid military operations became particularly significant, as states and non-state actors increasingly leveraged cyberspace for strategic and tactical advantage. At the same time, cybercrime – though often considered a separate phenomenon – contributed to broader security challenges, testing the resilience of societies and forcing governments to reconsider their approach to global digital governance and their defense (Fidler 2014; Steed 2019). For Western nations, in particular, the growing threat of cybercrime raised urgent questions about how to protect hyper-connected societies from attacks. At the same time, they were forced to recognize that even in this seemingly virtual realm, political adversaries were asserting their presence. Meanwhile, authoritarian states like Russia and China saw the Internet as a dangerous tool of political mobilization used possibly to threatens the stability of their regimes, particularly so, in light of the Arab Spring and the Color Revolutions (on Russian perception on this see Stefanachi 2024). Ultimately, the ideal of a borderless, free Internet collided with geopolitical reality. As the

world evolved, successive U.S. administrations had to acknowledge that history had not ended, and that geography and power politics continued to shape even the digital world.

The Shift to a Contested World and New Forms of Cyberpower

The faith in the market and the promise of global interconnection, seen as the foundation of stability and progress, gradually gave way to a more sobering realization – that this very interdependence could be weaponized, posing serious risks to societies. The idea that economic and technological interconnectedness would naturally lead to security and cooperation was replaced by a growing awareness that vulnerabilities were deeply embedded within these networks and could be exploited by adversaries. As Farrell and Newman (2019) argue, the liberal vision of a flat, decentralized world has proven deeply flawed. The expectation that interconnectivity would create a truly ubiquitous and neutral space, taking societies "beyond history", has not materialized, at least not in the way liberal rhetoric once suggested. In reality, network structures have reinforced, rather than erased, power imbalances. Instead of fostering diffuse cooperation and decentralized influence, they have led to a concentration of power within specific nodes, creating persistent asymmetries, in the words of Farrel and Newman (2019): «Key global economic networks – like many other complex phenomena – tend to generate ever more asymmetric topologies in which exchange becomes centralized, flowing through a few specific intermediaries […] have converged toward "hub and spoke" systems, with important consequences for power relations». While the technical architecture of cyberspace was designed to be resilient and distributed, in practice it has developed hierarchical structures with centers of control and peripheral areas that connected to the hubs by far less paths thus becoming far less influential. Some nodes have become critical chokepoints, shaping the flow of information and economic exchanges, further reinforcing global inequalities and dependencies. Thus, rather than dissolving traditional power structures, cyberspace has become a new battleground for influence, where connectivity itself is strategically leveraged by those who dominate key points in the network.

This shift in perception has been particularly evident in the United States, which moved from a sense of invulnerability and from the peak of security optimism to a state of pervasive insecurity (Colombo 2022). The post-Cold War euphoria, marked by the belief that liberal values and global markets would ensure long-term stability for their place in the international arena, began to erode as political tensions (re)emerged in new, and sometimes unexpected, ways. This transformation became evident in cyberspace too. The very interconnectivity that had once symbolized progress increasingly came to be seen as a potential vector of attack, particularly for Western countries, where critical infrastructure, economies, and financial markets were deeply embedded in digital networks. As the illusions of liberal euphoria gradually faded, policymakers and strategists began to anticipate worst-case

scenarios in which cyber threats could escalate into catastrophic disruptions; see, among others, the myth of the fear of a "Cyber Pearl Harbor", as foreshadowed in 2012 by then-U.S. Secretary of Defense Leon Panetta during his speech at the Business Executives for National Security Conference.

From the early 21st century onward, the discourse on cybersecurity underwent an irreversible shift – from a techno-optimistic vision of digital empowerment to one dominated by concerns over risk, vulnerability, and the pressing need for national defense in cyberspace. If this was the primary concern for the Western world, for the so-called revisionist powers instead – Russia and China – cyberspace was never a neutral space of global interconnectivity but rather an infrastructure deeply influenced by the United States, one they increasingly viewed as intrusive and potentially dangerous for the stability of their regimes. Their skepticism only grew in the light of the Arabs Springs – although contributions of social media made to these revolutions remains debated – these captured the belief that internet-enabled communications threaten authoritarian rulers. This impression grew even more after the Snowden revelations in 2013, confirming their worst fear: the internet was not simply a tool for open communication and commerce but also a domain of influence, surveillance and control, dominated by Western actors. In response, both Russia and China took decisive steps to detach themselves from what they perceived as an "American internet". Putin, as Klimburg (2017) notes, went so far as to call the entire internet nothing more than a «CIA project». This perspective fueled efforts to reshape their digital ecosystems in ways that prioritized state sovereignty and state control. For instance, Russia progressively moved toward its concept of a sovereign Runet (Russian Internet), tightening control over domestic internet infrastructure, forcing data localization, and creating mechanisms to isolate its segment of the internet from the global web (Limonier 2018). Meanwhile, China, which had already been refining its digital governance model since the early 2000s, intensified its efforts in pursuit of cyber sovereignty (Balestrieri & Balestrieri 2019; Hillman 2021; Balestrieri & Balestrieri 2024, Topor 2024). This ambition was driven by the desire to shield its "information space" from unwanted foreign influence and to reshape Internet governance by shifting from a multistakeholder model to a state-centric one. China sought to assert exclusive state control over its national digital infrastructure, reinforcing the notion that cyberspace should be governed primarily by sovereign states rather than by international bodies or private entities (Nagelhus Schia & Gjesvik, 2017).

It is worth highlighting, that within one of the central debates in the literature on cyberspace and cyberpower – namely, whether cyber technology constitutes a «weapon of the strong» or a «weapon of the weak» (Dossi 2018) – the Chinese perspective stands in stark contrast to the American or Western viewpoint. This difference in perspectives is central to understanding how the perception of

this space has been viewed with deep suspicion by China since its inception, while on the other hand, it clearly demonstrates how the American viewpoint is a product of an increasingly anxious perspective, born from a gradual sense of being under attack and vulnerable, even to weaker actors. This debate, as discussed by Dossi (2018), revolves around the contrasting views on cyberwarfare. The mainstream perspective perceives cyberspace as a "weapon of the weak," arguing that the low barriers to entry in the cyber domain enable weaker actors to challenge more powerful adversaries. It is assumed that cyber technology is inexpensive, allowing military objectives to be achieved at a lower cost. However, a smaller group of scholars disagrees, contending that cyberwarfare serves as a force multiplier, reinforcing the power of stronger actors. They argue that while basic hardware and training might suffice for amateur attacks, significant military operations with political goals require substantial investment in research and development. Furthermore, these scholars assert that cyberwarfare is most effective when integrated with traditional forms of warfare. While some believe cyberwarfare can achieve strategic aims independently, others, including Gartzke (2013), argue that traditional military tools are necessary to translate virtual advantages into real-world political outcomes. Very interestingly, Dossi (2018) in his work traces this debate through the Chinese and American perspectives, observing how in China the prevailing idea is that the new domain is largely dominated by technologically advanced powers, particularly the US, «Several articles insist on a so-called US "internet hegemony" (*wangluo baquan*), meaning that the US "uses its technological advantage to obstruct, restrict or prevent other countries from obtaining and using information, or even take advantage of monopolized information technology to control other countries' sources and flows of information, in order to promote its own economic, political or military interests" (Wu 2014, p. 55)» (Dossi 2018). Thus, in the Chinese discourse, cyberspace is seen as a domain where the United States exerts hegemony across several dimensions. This includes technological dominance, as the US controls key technologies, granting it significant influence over the political, economic, and military institutions of developing countries. Additionally, the US is perceived to control internet governance, overseeing the institutions responsible for critical administrative functions. Cultural hegemony is also a key aspect, with the US not only managing the internet's technical infrastructure but also shaping the cultural content it transmits, resulting in a one-way flow of information from developed to developing nations. Finally, the US's military hegemony in cyberspace is evident in its establishment of cyber forces for offensive operations, further reinforcing its dominance in this domain. On the other hand, starting from the second Obama administration, the US began to perceive cyberspace as a source of vulnerability, as it found itself at the center of an interconnected world that had become increasingly hostile. This environment was seen as one that empowered smaller actors at the expense of American security and power.

All these factors fundamentally reshaped the way cyberspace was perceived during the first two decades of this century, marking a stark departure from the optimistic vision of the 1990s. Once imagined as a boundless realm that erased distances and leveled differences, it gradually transformed into a domain of sovereignty, borders, and control. No longer the space of cooperation and the "human family", it became a contested arena where clear enemies can now be identified. Far from the immaterial and borderless space it was once thought to be, cyberspace proved to be increasingly subject to the pull of territoriality. Its physical infrastructure remained tied to geography, exposed to environmental constraints and the authority of states exerting control over their digital domains. What was once seen as an open, neutral network evolved into a strategic battleground, where nations sought to assert their digital sovereignty and secure their place in an increasingly fragmented and securitized cyberspace.

Now, as this research examines the evolving perceptions of geography, space, security, and cyberspace, now it will specifically analyze the transformation of U.S. cyber strategy from 2000 to the present. This shift will be traced in relation to emerging threats, geopolitical competition, and changing security perceptions, providing an insight into how the U.S. has adapted to an increasingly contested landscape. The United States represents a particularly compelling case study for several reasons. First, it offers the most extensive and accessible collection of primary sources, policy documents, and scholarly analyses, allowing for a rigorous and empirically grounded investigation of cyber policy development. More significantly, the U.S. experience uniquely illustrates the evolution of cyberspace from a tool of soft power to a space increasingly defined by strategic vulnerabilities and national security imperatives. Unlike China and Russia, which have approached cyberspace governance with inherent skepticism toward the open internet, the United States has faced the complex challenge of redefining its role in cyberspace while still upholding its commitment to an interconnected digital free order. This tension, as we will see, has profoundly shaped the trajectory of U.S. cybersecurity policies and strategic posture. Furthermore, the evolution of American cyber strategy serves as an image of broader shifts in the U.S. grand strategy, reflecting the transition from post-Cold War optimism and unchallenged hegemony to a new era of strategic competition – most notably with China. As cyberspace has become a key battleground for geopolitical influence, analyzing U.S. cyber strategy is essential to understanding the evolving dynamics of power, sovereignty, and security.

Since the end of the 1990s, Western rhetoric – that of the United States in particular – began to shift. As argued by Colombo (2022), this change may have been inherently tied to liberal ideology itself, which tends to view the world through utopian lenses, envisioning a seamless and harmonious global

order and thus perceiving any small fracture as an existential threat. Over time, in fact, the prevailing narrative of security and confidence in a world governed by economic interdependence, technological progress, and governance models rooted in international public and private organizations started to weaken. A first subtle crack in this idealized vision did not initially stem from external geopolitical shifts but rather from an emerging internal distrust – an underlying anxiety about the very technology that had become increasingly pervasive: the Year2000 Bug (Y2K). Also known as the "Millennium Bug", this issue arose from a programming shortcut in early computer systems, which recorded years using only the last two digits (e.g., "99" for 1999). As the year 2000 approached, concerns emerged that computers would interpret "00" as 1900 rather than 2000, potentially causing widespread failures in financial systems, infrastructure, and critical services (See Smith et al. 1997). The alarm surrounding Y2K was widespread, with some predicting catastrophic consequences, including the collapse of banking systems, power grids, and even military infrastructure (Zachary 2019). Private industries invested billions in preventive measures, and while the feared global breakdown never materialized – partly due to extensive remediation efforts – the panic itself was revealing. It demonstrated a growing unease with the very digital infrastructure that had, until then, been seen primarily as a tool of progress and global integration. Moreover, while it is true that a great deal of investments were made by private entities – given that the network and its systems were privately owned – governments also had to intervene to coordinate efforts and guarantee the implementation of certain minimum preventive measures due to the scale and pervasiveness of interconnected systems. As Carr (2016, 65) notes «Calls for government intervention generate debates about the merits of adhering to the liberal value of limited government as opposed to the benefits of a 'strong, central hand' in shaping Internet technology». In 1998, the United States government addressed the Y2K challenge by enacting the *Year 2000 Information and Readiness Disclosure Act*, which facilitated collaboration with the private sector to ensure preparedness while also setting limits on certain corporate liabilities. The Act expressed significant concern over the potential consequences of the issue, stating that «the problem described [...] and resulting failures could incapacitate systems that are essential to the functioning of markets, commerce, consumer products, utilities, government, and safety and defense systems, in the United States and throughout the world» (Act 1998). Though the Y2K crisis did not produce the warned catastrophic damage, it marked an early moment of distrust and suspicion toward this parallel, increasingly essential infrastructure. It suggested that, despite widespread optimism about cyberspace and digital globalization, technological interdependence also carried unforeseen vulnerabilities even far beyond the ethereal world of cyberspace, setting the stage for deeper anxieties in the years to come.

Naturally, what profoundly altered the perception inherited from the 1990s, creating a lasting sense of fear that has persisted almost uninterrupted to this day has been the terrorist attacks of September 11, 2001. The world had indeed become smaller, and the United States could no longer rely on geographic isolation to shield itself from history: they had been struck at the heart of their own homeland. In June 2002, a few months after the attacks, President Bush proposed separating the White House Office of Homeland Security and transforming it into an independent department, the Department of Homeland Security (DHS), which was officially established in September of the same year. This restructuring marked the most significant transformation of the U.S. government in over half a century, uniting 22 federal entities under a single cabinet-level department dedicated to homeland security and among the responsibilities of this new department was also the securitization of cyberspace:

The consequences of an attack on our cyber infrastructure can cascade across many sectors, causing widespread disruption of essential services, damaging our economy, and imperiling public safety. The speed, virulence, and maliciousness of cyber-attacks have increased dramatically in recent years. Accordingly, the Department of Homeland Security would place an especially high priority on protecting our cyber infrastructure from terrorist attack (Bush 2002)

In 2003, the Bush administration released another key document on cybersecurity, the National Strategy to Secure Cyberspace, which served as an implementing component of the National Strategy for Homeland Security of 2002. This document framed its rationale – its case for action – around the events of 9/11. As stated in the strategy:

The terrorist attacks against the United States that took place on September 11, 2001, had a profound impact on our Nation. The federal government and society as a whole have been forced to reexamine conceptions of security […] In the last century, geographic isolation helped protect the United States from a direct physical invasion. In cyberspace national boundaries have little meaning. Information flows continuously and seamlessly across political, ethnic, and religious divides. Even the infrastructure that makes up cyberspace – software and hardware – is global in its design and development. Because of the global nature of cyberspace, the vulnerabilities that exist are open to the world and available to anyone, anywhere, with sufficient capability to exploit them. (Bush 2003)

Nevertheless, despite the clear shift in threat perception and the growing concern surrounding cyberspace under the Bush administration, a degree of continuity with the Clinton-Gore approach in addressing cyberspace remains evident, particularly in the emphasis placed on the role of the private sector. While the administration acknowledged the undeniable risks posed by this domain, it still

upheld the idea that «the private sector is best equipped and structured to respond to an evolving cyber threat [..] Public-private engagement is a key component of our Strategy to secure cyberspace» (Bush 2003). By delegating security in this space almost entirely to private entities, U.S. policymakers demonstrated a profound faith in market dynamics, operating under the assumption that by simply increasing the demand for security, the market would respond accordingly, with the most effective providers naturally emerging through competition. This logic – akin to the broader neoliberal belief in self-regulating mechanisms – was fundamentally premised on the idea that economic incentives alone would drive the necessary investments and innovations to ensure cybersecurity. However, this assumption would soon come under increasing strain, first with the 2008 financial crisis, which exposed the vulnerabilities of unregulated market logic, and later, as state-based threats began to materialize in the cyber arena. The latter, in particular, would accelerate the entry of the federal government into this space, marking a shift from the ideal of an autonomous, market-driven cyberspace to one where state intervention became not only necessary but inevitable. At the time however, the primary threats identified in the strategy, given its case for action, remained international terrorism and transnational cybercrime. Consequently, significant emphasis was placed on international cooperation, particularly through existing international organizations, to establish points of contact and foster coordination in response to these evolving challenges. Given the inextricable interconnection between states in cyberspace, the strategy underscored the necessity of collaborative efforts to enhance cybersecurity resilience. Notably, it aimed to build upon the common experience of the Y2K crisis, where the absence of a centralized coordination mechanism had highlighted the need for structured international cooperation in addressing large-scale cyber threats (Bush 2003). There was, therefore, no perception of an enemy within the international system; rather, the threats were represented as global adversaries – criminal actors whose actions, in a way, further united the international community in the face of a common menace.

In the following years, reports of cyberattacks targeting both public and private entities continued to rise, heightening concerns over threats emanating from cyberspace. This growing unease reached a turning point in April 2007 with what was widely considered the first publicly acknowledged instance of a state-to-state cyberattack the one on Russia against Estonia – though the precise origins of the attack remain uncertain and Russian government has consistently denied any direct involvement. Following a diplomatic dispute between the two countries, Estonia's critical infrastructure came under an extensive and sustained Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks (Ottis 2007). The attack, involving over a million computers worldwide, targeted key national institutions, including the websites of the Estonian president and parliament, three of the country's six major news services, two of its largest banks, and several telecommunications firms. To mitigate

the impact of the attack, Estonia was compelled to temporarily disconnect from most of its foreign internet traffic, as most of the malicious activity originated from outside its borders (Landler and Markoff, 2007).

Figure 2 - Estonia Connectivity Map (ITU) Retrieved on February 2nd, 2025.

It is highly significant to note, especially considering the objectives of this study, that for the first time in the history of cyberspace, a state adversary was identified, so cyberspace can be use as an instrument of power in its own – one that compelled Estonia to cut itself off from the Internet within its own borders. This marked the unexpected emergence of power action, "hard" cyberpower (Nye 2010) compared to the idea of cyberspace as the space of persuasion and soft power. Territorial boundaries therefore became central in the power dynamic in the cyberworld, and it was possibly the first instance in which the significance of territoriality and the ability to exert physical control over critical infrastructure began to be fully recognized.

The emergence of state-based threats in cyberspace and the potential militarization of this domain led the North Atlantic Treaty Organization (NATO) to convene a meeting of foreign ministers to discuss a more appropriate response to the growing problem of cyber aggression. A direct outcome of this deliberation, following an Estonian proposal, was the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in May 2008. At the invitation of the Tallinn-based CCDCOE, a group of international experts published in 2013 the Tallinn Manual on the International

Law Applicable to Cyber Warfare. Although this document did not represent the official position of NATO, the CCDCOE, or any state, it remains a crucial resource for understanding the profound shift in how cyberspace was conceptualized. Once imagined as the epitome of a "flat world", it increasingly came to be viewed through the more traditional lens of interstate relations, those that centered on sovereignty, territory, borders. For the first time, the expert group contributing to this work explicitly recognized the principle of sovereignty in cyberspace:

Rule 1 – Sovereignty A State may exercise control over cyber infrastructure and activities within its sovereign territory […] no State may claim sovereignty over cyberspace per se, States may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure […] cyber infrastructure situated in the land territory, internal waters, territorial sea (including its bed and subsoil), archipelagic waters, or national airspace is subject to the sovereignty of the territorial State.

A far more tangible and material world begins to take shape – one that is now fully political, where boundaries are clearly delineated, and where friends and enemies can be identified with precision. This is not to suggest that the identity of the actor responsible for cyberattacks can be definitively proven. On the contrary, most state-based cyber operations remain concealed under a veil of plausible deniability, often employing proxies. This ambiguity creates significant challenges in formulating countermeasures or establishing a credible deterrence strategy (On this, see: Lindsay 2015; Baliga et al. 2020; Brown & Fazal 2021)[10]. The central issue of interest to this analysis lies in the ability to distinguish and draw clear boundaries between an inside and an outside – a Schmittian "furrow in the earth" – between us and them, between friend and enemy, even in geographical terms, that can appear by analyzing the origin and distribution of the attack.

The shift from the previous liberal view of cyberspace to this new "geopolitical reality", as noted by Lonergan and Schneider (2023), is observable also in the transition between the first U.S. Defense Cyber Strategy of 2011 and the second in 2015, both issued during Obama's presidency. The Department of Defense (DoD) released its inaugural cyber strategy in July 2011, following the Obama administration's International Cyberspace Strategy of the same year. This earlier document conveyed a sense of optimism regarding the role of cyberspace and the Internet in advancing globally human rights, promoting democracy, and fostering economic opportunities. This perspective was further

[10] It must be noted however, there is recent and ongoing debate about the necessity and effectiveness of plausible deniability in cyber operations. As Canfil (2022) argues, "usual suspects" who anticipate being blamed regardless of their actual involvement may have fewer incentives to rely on proxies.

reinforced by the Arab Spring and the widespread belief that social media played a crucial role in empowering democratic movements. As stated in the strategy:

> We encourage people all over the world to use digital media to express opinions, share information, monitor elections, expose corruption, and organize social and political movements, and denounce those who harass, unfairly arrest, threaten, or commit violent acts against the people who use these technologies (Obama 2011).

In line with this vision, the DoD strategy defined its ultimate objective as the establishment of a free, open, interoperable, reliable, and secure cyberspace – an ideal portrayed as a universally beneficial goal. The preferred approach to achieving this was primarily through non-military means, emphasizing diplomacy, international cooperation, and the promotion of norms, which were regarded as equally, if not more, significant than law enforcement or military capabilities. Moreover, the 2011 strategy did not explicitly identify enemies and remained primarily focused on non-state actors and insider threats rather than any specific nation-state. It was also ambiguous regarding how the U.S. military planned to address threats originating from cyberspace, reflecting broader uncertainty about the military's role in this domain.

The evolving international landscape has heightened perceptions of the decline of Western centrality and contributed to an increasing sense of insecurity. A particularly significant event in this regard was the annexation of Crimea and the ongoing conflict over Donbas, which has been fiercely contested since 2014. Once again, this episode underscored the crucial role of borders and territorial control – not only in the physical realm but also in the digital domain. Controlling cyberspace and information flows became a strategic objective, as demonstrated by one of Russia's earliest actions in the crisis. On February 28, 2014, a Russian commando unit seized the building and equipment of the Ukrainian telecommunications company Ukrtelekom, severing its cables that connected Crimea to mainland Ukraine and effectively disconnecting much of the peninsula from the Ukrainian Network Internet and in the subsequent months rushed to connect Crimea to the Russian network (Douzet et al. 2020).

Russian hacktivism, the emerging cyber threat from Iran and North Korea, and China's growing assertiveness in cyberspace – particularly its focus on sovereign cyber infrastructure (see Steed 2019, 65-76) – have led the U.S. administration to adopt a more realist stance. This shift marks a departure from liberal idealism toward a strategy that explicitly acknowledges, for the first time, the presence of state enemies in cyberspace that are explicitly named. It reflects a recognition that this contested domain is no longer an abstract, borderless space but one where geopolitical rivalries and strategic competition are increasingly shaping the landscape:

From 2013-2015, the Director of National Intelligence named the cyber threat as the number one strategic threat to the United States, placing it ahead of terrorism for the first time since the attacks of September 11, 2001 […] Potential adversaries have invested significantly in cyber as it provides them with a viable, plausibly deniable capability to target the U.S. homeland and damage U.S. interests. Russia and China have developed advanced cyber capabilities and strategies. Russian actors are stealthy in their cyber tradecraft and their intentions are sometimes difficult to discern. China steals intellectual property (IP) from global businesses to benefit Chinese companies and undercut U.S. competitiveness. While Iran and North Korea have less developed cyber capabilities, they have displayed an overt level of hostile intent towards the United States and U.S. interests in cyberspace (Obama 2015).

Nonetheless, the government's possible responses to these cyber incidents centered mostly on economic, diplomatic and legal activities, and the Pentagon was set to play a limited role in the policy responses to those incidents, in fact it was primarily placed in a reserve and deter posture.

With Donald Trump's arrival at the White House, the perception of external threats became even more entrenched. However, as can be seen from the evolution of U.S. cyber strategies, this did not signify a complete break from the previous model, but rather an adaptation, shaped by the administration's particular approach and rhetoric. This shift is clearly reflected in the 2017 National Security Strategy, which formally declared the end of the liberal illusion. Cyberspace and technological interconnectivity were no longer viewed through the lens of a "flat world"; instead, the document acknowledged that international threats were not mitigated by digital globalization but rather amplified by it:

> We face simultaneous threats from different actors across multiple arenas – all accelerated by technology […] We assumed that our military superiority was guaranteed and that a democratic peace was inevitable. We believed that liberal-democratic enlargement and inclusion would fundamentally alter the nature of international relations […]as threats to our national security increased, the United States dramatically cut the size of our military [and this] contributed to the erosion of America's military dominance during a time of increasing threats [all this while] China and Russia began to reassert their influence regionally and globally (Trump 2017).

Furthermore, in line with the perceived threat landscape, the 2018 DoD Cyber Strategy identified the necessity for a new role for the government in securing cyberspace – moving away from the previous model that prioritized private sector leadership in cybersecurity. While earlier approaches, particularly under the Clinton and Bush administrations, emphasized market-driven solutions and voluntary public-private collaboration, the 2018 strategy marked a decisive shift toward a more

proactive and interventionist stance. The strategy underscored that cyber threats had evolved beyond what the private sector could effectively handle alone, requiring greater government involvement in deterrence, active defense, and counter-cyber operations: «The United States Government will work with private and public sector entities to promote understanding of cybersecurity risk so they make more informed risk-management decisions, invest in appropriate security measures, and realize benefits from those investments» (Trump 2018). This shift marks a definitive move away from the notion of cyberspace as an apolitical, neutral domain of individuals and instead positions it as a fully political arena where power, sovereignty, and strategic considerations dictate policy choices. As the previous strategy, it explicitly acknowledged that cyberspace is now a contested domain, where adversarial states can indeed leverage cyber capabilities to undermine U.S. national security, economic interests, and critical infrastructure. As a result, the Pentagon adopted now a more forward-leaning posture, encapsulated in the concept of "Defend Forward" – which called for preemptive cyber operations to disrupt malicious activities before they could reach U.S. networks. This strategy marked a break from the traditional reactive approach that largely focused on network defense and post-incident response, emphasizing instead the need to engage adversaries in cyberspace proactively. In this sense, the 2018 DoD Cyber Strategy represented a key turning point in U.S. cyber policy, transitioning from a decentralized, model of cybersecurity governance toward a more centralized, state-directed approach, and assertive approach (Lonergan 2023).

The 2023 National Cybersecurity Strategy under the Biden administration largely continues the trajectory set by the 2018 National Cyber Strategy of the Trump administration, reinforcing the securitization of cyberspace and the perception of an increasingly contested digital domain. While the language differs – Biden's strategy frames cybersecurity within a broader vision of democratic resilience, while Trump's emphasized national strength and deterrence – the underlying approach remains consistent with that of its predecessor. If anything, the Biden administration goes even further in expanding the federal government's role in cybersecurity, moving beyond Trump's emphasis on public-private partnerships by asserting stronger state intervention and regulatory oversight over critical infrastructure and supply chains:

Government's role is to protect its own systems; to ensure private entities, particularly critical infrastructure, are protecting their systems; and to carry out core governmental functions such as engaging in diplomacy, collecting intelligence, imposing economic costs, enforcing the law, and, conducting disruptive actions to counter cyber threats. Together, industry and government must drive effective and equitable collaboration to correct market failures, minimize the harms from cyber incidents to society's most vulnerable, and defend our shared digital ecosystem. (Biden 2023)

All U.S. administrations have demonstrated remarkable continuity in their evolving approach to cyberspace, shifting from the liberal dream of an open, self-regulating domain to a vision of siege, where threats emanate from every direction. This securitization of cyberspace – the perception of a contested space filled with enemies – mirrors the broader transformation of the international system in which the United States has operated since 2001. The first two decades of this century were marked by a sustained challenge to the moral, political, and military legitimacy of American supremacy. The years that were expected to witness the uninterrupted expansion of the liberal-democratic model instead saw it under attack and increasingly questioned, both externally and from within. Unsurprisingly, cyberspace – once envisioned as the embodiment of a boundless and depoliticized sphere – was drawn into this turbulence. A growing loss of faith in market-driven logic and its ability to autonomously regulate both the economy and security concerns led to the reassertion of sovereignty and the return of politics as the defining force in cyberspace governance. No longer merely an instrument of soft power and ideological influence, cyberspace has increasingly become a domain of coercion, a realm where uncertainty and hostilities unfold, reinforcing its role as a medium of "hard power", capable of exerting strategic pressure and shaping geopolitical realities.

Alongside the rediscovery of state enemies in the international arena, another significant trend, particularly since the 2010s, has been the reemergence of territoriality and borders – elements that, during the era of liberal optimism, were assumed to have been definitively settled but have instead been increasingly contested, first gradually and then with escalating intensity. The most obvious reference here is the Russia-Ukraine conflict, but similar dynamics can be observed in China's maritime and terrestrial disputes, Iran's claims over Shia communities in Iraq, Bahrain, Syria, Yemen, and Lebanon, and Turkey's political-military protectorate over northern Iraq and northern Syria (see for instance Mankoff 2022). These cases illustrate how recent years have been marked by a forceful return of territoriality as a central feature of global politics. Consequently, this renewed focus on borders has spilled over into cyberspace, where territoriality, sovereignty, and control over digital infrastructures have become increasingly relevant. This shift was first observed in the Estonian case in 2007 and later, more dramatically, in the Ukrainian crisis. Alongside this return of territoriality, another crucial dimension of sovereignty has gained prominence: data sovereignty. As states increasingly view data as a strategic resource, questions over who controls data, where it is stored, and how it is governed have become central concerns. Thus, the demand for a new global governance of cyberspace, which, as seen in the Tallinn Manual, establishes cyber sovereignty as a fundamental principle. At the core of this sovereignty lies the reassertion of control over data – a shift that reflects the increasing recognition that data, often perceived as intangible entities floating in the so-called "cloud", are in fact a strategic asset central to national security and economic autonomy. However,

this sovereignty is not merely an abstract legal or political concept; rather, it has a tangible, material dimension. Fundamentally, when discussing data sovereignty, we are referring to the boom of data localization laws and this localization basically consists in «the act of storing data on a device that is physically located within the country where the data was created» (Steed 2019, 70). In essence, it means the extension of territorial sovereignty and national legal jurisdiction to the infrastructure and to the data inside. This shift underscores a crucial evolution in the conceptualization of cyberspace: no longer merely a realm of free-flowing, unregulated information, but rather a domain increasingly subject to the same principles of territoriality, control, and governance that have historically defined state power in the physical world. The rise of digital sovereignty and data localization laws reflects a global shift toward reclaiming control over cyberspace, driven by geopolitical tensions and security concerns. While Russia and China have implemented stringent regulations mandating that data related to their citizens be stored within national borders (see Burgman 2016; Lyall 2017), this trend is not confined to authoritarian regimes. Democracies in Asia (See Steed 2019, 71-76), like India, Vietnam, in Europe the UK, and even the European Union are on a «emerging quest for 'digital sovereignty'» (Madiega 2020, see also Svantesson 2020).

It is therefore essential to move away from the immaterial vision of cyberspace as the great destroyer of distances and the leveler of places – the homogenizing space of the world, Cyberia. Today, it becomes impossible to conceive it without acknowledging its underlying foundation of physical networks, still subject to the constraints of location, the forces of nature, the magnetic force of territoriality, and the control exerted by political actors over geographic space. Thus, while previous reflections – important as they are conceptualizing a new space – have highlighted an aspatial and apolitical social reality of cyberspace, conceived as a metaphor or a construct of human minds, they must necessarily be expanded and completed. This becomes necessary because, as Betz and Stevens (2011) argue, «[defining cyberspace] is not trivial. What we decide to include or exclude from cyberspace has significant implications for the operation of power, as it determines the purview of cyberspace strategies and operations of cyber-power». Given the changes in the international landscape and the evolving perception of these transformations, and considering how they have been reflected in cyberspace, it is more necessary than ever to adopt a model that explicitly incorporates the presence of infrastructure, its materiality, and its geographical dimension in its definition. Possibly, the most sophisticated description of the inclusive model is provided by Libicki (2009): «One way to understand cyberspace in general, and cyberattacks in particular, is to view it as consisting of three layers: the physical layer, a syntactic layer sitting above the physical, and a semantic layer sitting on top». According to this model, the perspective focuses on the fact that information systems are built on a physical layer of hardware, and removing this layer causes the

system to disappear. Then, we have the syntactic or logical layer, that includes the instructions and protocols for machine interactions, such as device recognition, packet framing, and database manipulation; and finally, on top, there is the semantic layer, that contains the information stored within the machines. A definition that encompasses the material aspects of cyberspace, their geographical positioning, and their control by territorial entities such as states provides a crucial framework for understanding how the concept of cyber-power has evolved. Initially endowed with an innate predisposition toward soft power, cyberspace has increasingly become an arena for the exercise of hard power, where states and actors can coerce and influence adversaries not only through information and narrative control but also through tangible means. This includes the ability to physically disrupt or destroy critical infrastructure, seize control of networks for intelligence operations, and execute denial-of-service attacks, demonstrating that cyber-power is no longer confined to the realm of persuasion but has become a strategic instrument of compulsion and dominance.

The resurgence of enemies, borders, territoriality, and geography has been accompanied by the natural return of focus on infrastructure and its physical placement. While technology undoubtedly reshapes how we perceive geographical realities, it is the framework through which we analyze this interaction that determines our understanding. Today, that framework is shaped by a pervasive sense of global insecurity and enmity, brought to the recognition that interconnectivity itself can be a vulnerability. In this context, boundaries are redrawn, threats are reassessed, and previously neutral spaces become arenas of competition. As the distinction between enemies and friends becomes more pronounced and geography continues to demonstrate its enduring relevance in contemporary concepts of security and power, geopolitics – once considered obsolete due to the leveling forces of globalization – re-emerges as a fundamental tool, with its own analytical instruments, for understanding reality even within the virtual space.

Conclusions

Tracing the evolution of cyberspace from its origins to the present, particularly examining how it has been conceptualized by successive U.S. administrations – given the role of the United States in constructing this reality and imprinting a framework that has significantly shaped its development – this review has aimed – while steering clear of debates on cyberwarfare and hybrid warfare, greatly discussed topic in this field – to outline the shifting perceptions and technical realities that have shaped this domain.

The evolution of cyberspace from a frontier of unbounded liberalism to a contested and securitized domain is emblematic of broader transformations in the international order. Initially conceived as a space of openness and interconnectivity, largely governed by market dynamics and driven by the ideological optimism of globalization, cyberspace has instead followed a trajectory of progressive securitization and reterritorialization. States have reasserted control over digital infrastructures, data flows, and network architectures, bringing cyberspace increasingly under the logic of sovereignty, territoriality, and strategic competition. Once imagined as a de-territorialized realm where the constraints of geography and power politics had little relevance, it has now become clear that cyberspace remains deeply embedded in material infrastructures, legal jurisdictions, and geopolitical rivalries. This shift has been driven not only by the rise of state-based cyber threats but also by a broader realization that interconnectivity itself can be weaponized, that global digital dependencies create vulnerabilities, and that the assumption of an autonomous, self-regulating cyberspace was ultimately untenable. The proliferation of data localization laws, the fragmentation of digital governance, and the growing emphasis on cyber sovereignty reflect this changing reality, as both democratic and authoritarian regimes seek to control the flows of information within their borders and to insulate their critical infrastructures from external interference.

The same technological architecture that once promised to erode traditional notions of space and distance now reveals itself as profoundly shaped by them. The resurgence of geography in cyberspace is not merely a conceptual evolution but a strategic necessity, as control over digital infrastructures and data flows increasingly translates into political leverage and power. This realization underscores the need for a more rigorous study of the relationship between infrastructure and geographic positioning, between infrastructure and topography. It calls for greater attention to the paths of submarine cables crisscrossing the oceans, to the territorial control of data centers and their strategic placement, and even to the ways in which atmospheric elements introduce friction into the management and security of these structures. On these foundations comes the rationale behind this study – a work that seeks to reinstate geography and geopolitics at the heart of cyberspace analysis, shedding light on the spatial dimensions that shape digital power and influence in the contemporary world.

Bibliography

Abbate, J. (2000). Inventing the Internet. MIT Press.

Agnew, J. (1998). Geopolitics: Re-visioning world politics (1st ed.). Routledge.

Babb, S. (2013). The Washington Consensus as transnational policy paradigm: Its origins, trajectory, and likely successor. Review of International Political Economy, 20(2), 268–297.

Balestrieri, F., & Balestrieri, L. (2019). Guerra digitale – Il 5G e lo scontro tra Stati Uniti e Cina per il dominio tecnologico. LUISS University Press.

Balestrieri, F., & Balestrieri, M. (2024). Tecnologie dell'impero: AI, quantum computing, 6G e la nuova geopolitica del potere. LUISS University Press.

Baran, P. (1964). On distributed communications networks. IEEE Transactions on Communications Systems, 12(1), 1-9.

Barié, O. (2013). Dalla guerra fredda alla grande crisi: Il nuovo mondo delle relazioni internazionali. Il Mulino.

Barlow, J. P. (1996, February 8). A declaration of the independence of cyberspace. Electronic Frontier Foundation. Reprinted from Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Betz, D. J., & Stevens, T. (2011). Cyberspace and the State – Towards a strategy for cyber-power. The International Institute for Strategic Studies, Routledge.

Biden, J. (2023). National Cybersecurity Strategy. DC: U.S. Department of Defense.

Blum, A. (2012). Tubes: A journey to the center of the Internet. Ecco Pr – Harper Collins Publisher.

Bolt Beranek and Newman (BBN).. Packet switching. Encyclopædia Britannica.

Bordonaro F. (2018). La geopolitica anglosassone. Delle origini ai nostri giorni. Guerini scientifica.

Borgognone, G. (2013). Storia degli Stati Uniti: La democrazia americana dalla fondazione all'era globale. Feltrinelli.

Brown, J. M., & Fazal, T. M. (2021). "#SorryNotSorry: why states neither confirm nor deny responsibility for cyber operations." European Journal of International Security, 6, 1–17.

Brown, J. M., & Fazal, T. M. (2021). # SorryNotSorry: Why states neither confirm nor deny responsibility for cyber operations. European Journal of International Security, 6(4), 401-417.

Bumiller, E., & Shanker, T. (2012). Panetta warns of dire threat of cyberattack on U.S. The New York Times.

Burgman, P. R., Jr. (2016). "Securing Cyberspace: China Leading the Way in Cyber Sovereignty", The Diplomat (18 May 2016).

Bush, G. W. (2002). National strategy for homeland security. Washington, DC: White House.

Bush, G. W. (2003). The national strategy to secure cyberspace. Washington, DC: White House.

Cairncross, F. (2001). The death of distance: How the communications revolution is changing our lives. Harvard Business Press.

Canfil, J. K. (2022). The illogic of plausible deniability: why proxy conflict in cyberspace may no longer pay. Journal of Cybersecurity, Volume 8, Issue 1, tyac007.

Carr, M. (2016). US power and the internet in international relations: The irony of the information age. Springer.

Clinton, B. (1992, April 16). The economy: Speech - Philadelphia, PA. Wharton School of Business, University of Pennsylvania.

Clinton, B. (1993, September 27). Address by President Bill Clinton to the UN General Assembly.

Clinton, W. J., & Gore, A. (1997). A framework for global electronic commerce. The White House.

Colombo, A. (2022). Il governo mondiale dell'emergenza: Dall'apoteosi della sicurezza all'epidemia dell'insicurezza. Raffaello Cortina Editore.

Colombo, A. (2025). Il suicidio della pace. Perché l'ordine internazionale liberale ha fallito. Raffaello Cortina Editore.

Congress, U.S. (1996). Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56.

Del Pero, M. (2017). Libertà e impero: Gli Stati Uniti e il mondo 1776-2016 (2nd ed.). Laterza.

Department of Defense (2011). Department of Defense Strategy for Operating in Cyberspace. Washington, DC: U.S. Department of Defense.

Di Nolfo, E. (2015). Storia delle relazioni internazionali. Gli anni della guerra fredda 1946-1990 (Vol. 2). Laterza.

Dossi, S. (2018). Confronting China's cyberwarfare capabilities: A "weapon of the weak" or a force multiplier? In M. Clementi, M. Dian, & B. Pisciotta (Eds.), *US foreign policy in a challenging world: Building order on shifting foundations*. Springer International Publishing.

Douzet, F., Salamatian, L., Salamatian, K., Pétiniaud, L., Limonier, K., & Alchus, T. (2020). Measuring the fragmentation of the Internet: The case of the Border Gateway Protocol (BGP) during the Ukrainian crisis. In 2020 12th International Conference on Cyber Conflict: 20/20 Vision: The Next Decade. NATO CCDCOE Publications.

Farrell, H., & Newman, A. (2019). Underground Empire: How America Weaponized the World Economy. Allen Lane, Penguin Books.

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. International Security, 44(1), 42-79. https://doi.org/10.1162/ISEC_a_00351

Fidler, D. P. (2014). Le cyberspace, c'est moi?: Authoritarian leaders, the Internet, and international politics. Seton Hall Journal of Diplomacy and International Relations, 15, 7–22.

Fidler, D. P. (2021). From the Arab Spring to the American Winter: Cyberspace and Democracy After the Insurrection, Council on Foreign Relations.

Friedman, T. L. (2007). The world is flat: The globalized world in the twenty-first century (2nd rev. ed.). Penguin UK.

Fukuyama, F. (1989). The End of History? The National Interest.

Galli, C., & Parsi, V. E. (2011). Editoriale. Spazi geografici e spazi politici: La geopolitica, ieri e oggi. Filosofia Politica, 25(1), 3–10.

Garvey, M. (2021). A philosophical examination on the definition of cyberspace. In Cyber Security and Supply Chain Management.

Gartzke, E. (2013). The myth of cyberwar – Bringing war in cyberspace back down to earth. *International Security, 38*(2).

Gibson, W. (1989). Neuromancer. Orion.

Goldsmith, J. (1998). The internet and the abiding significance of territorial sovereignty. Indiana Journal of Global Legal Studies, 5(2).

Gore, A. (1994, March 21). Inauguration of the first World Telecommunication Development Conference (WTDC-94): Remarks prepared for delivery. World Telecommunication Development Conference, Buenos Aires, Argentina.

Gore, C. (2000). The rise and fall of the Washington Consensus as a paradigm for developing countries. World Development, 28(5), 789–804.

Hardy, I. T. (1994). The proper legal regime for 'cyberspace'. University of Pittsburgh Law Review, 55(4).

Hillman, J. E. (2021). Securing the subsea network – A primer for policymakers. CSIS (Center for Strategic & International Studies).

Ikenberry, G. J. (2018). The end of liberal international order? International Affairs, 94(1), 7–23.

Isaacson, W. (2015). The Innovators: How a Group of Hackers, Geniuses, and Geeks Created the Digital Revolution. Simon & Schuster.

Johnson, D. R., & Post, D. (1996). Law and borders: The rise of law in cyberspace. Stanford Law Review, 48(5).

Kennedy, P. M. (1971). Imperial Cable Communications and Strategy, 1870–1914. In The War Plans of the Great Powers (RLE The First World War) (1st ed.). Routledge.

Klimburg, A. (2017). The Darkening Web: The War for Cyberspace. Penguin Press.

Kuehl, D. T. (2011). From cyberspace to cyberpower: Defining the problem. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), Cyberpower and national security (pp. 24-42). National Defense University Press.

Landler, M., & Markoff, J. (2007, May 29). Digital fears emerge after data siege in Estonia. The New York Times.

Limonier, K. (2018). Ru.net : Géopolitique du cyberespace russophone. L'Inventaire.

Limonier, K., Douzet, F., Petiniaud, L., Salamatian, L., & Salamatian, K. (2021). Mapping the routes of the Internet for geopolitics: The case of Eastern Ukraine. First Monday.

Lindsay, J. R. (2015). "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack." Journal of Cybersecurity, 1(1), 53–67.

Loeb, Z. (2019, December 30). "The lessons of Y2K, 20 years later". The Washington Post.

Lonergan, E. D., & Schneider, J. (2023). The power of beliefs in US cyber strategy: The evolving role of deterrence, norms, and escalation. Journal of Cybersecurity, 2023, 1–10.

Lonergan, E. D., Lonergan, S. W., & Schneider, J. (2022, April 4). Reviewing US cyber posture: An analysis. Saltzman Institute of War and Peace Studies, Columbia University.

Mackinder, H. J. (1904). The geographical pivot of history. The Geographical Journal, 23(4), 421–437.

Madiega, T. (2020). Digital sovereignty for Europe (PE 651.992 - July 2020). European Parliamentary Research Service.

Mahan, A. T. (1890). The influence of sea power upon history, 1660–1783 (15th ed.). Little, Brown, and Company. (Original work published 1890).

Mahan, A. T. (1897). The interest of America in sea power, present and future. Little, Brown.

Mankoff, J. (2022). The War in Ukraine and Eurasia's New Imperial Moment. The Washington Quarterly, 45(2), 127–147.

Maurer, J. H. (2023). Alfred Thayer Mahan and the strategy of sea power. In H. Brands (Ed.), The new makers of modern strategy: From the ancient world to the digital age (pp. 445–465). Princeton University Press.

Mosco, V. (2004). The Digital Sublime: Myth, Power, and Cyberspace. MIT Press.

Mueller, M. L. (2019). Against sovereignty in cyberspace. International Studies Review, 0, 1–23.

Mullally, L. (2024). The actually existing internet: The disappearing internet (1991–2010). Autonomy Institute.

Nagelhus Schia, N., & Gjesvik, L. (2017). China's cyber sovereignty. Norsk Utenrikspolitisk Institutt (NUPI).

Nick Lyall, "Cyber Sovereignty: The Sino-Russian Authoritarian Model", Foreign Brief (15 September 2017).

Nye, J. S. Jr. (1990). Soft power. Foreign Policy, (80), 153-171.

Nye, J. S. Jr. (2010). Cyber Power. Belfer Center for Science and International Affairs, Harvard Kennedy School.

O'Brien, R. (1992). Global financial integration: The end of geography. Council on Foreign Relations.

Obama, B. H. (2011). International strategy for cyberspace: Prosperity, security, and openness in a networked world. Washington, DC: The White House.

Obama, B. H. (2015). The Department of Defense Cyber Strategy. Washington, DC: The White House.

Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. Cooperative Cyber Defence Centre of Excellence.

Parsi, V. E. (2022). Titanic. Naufragio o cambio di rotta per l'ordine liberale. Il Mulino.

Paul R. Burgman, Jr., “Securing Cyberspace: China Leading the Way in Cyber Sovereignty”, The Diplomat (18 May 2016).

Raustiala, K. (2017, February 13). An internet whole and free: Why Washington was right to give up control. Foreign Affairs.

Schlögel, K. (2016). In Space We Read Time: On the History of Civilization and Geopolitics. (G. Jackson, Trans.). Bard Graduate Center.

Schmitt, C. (2013). Le categorie del «politico». Saggi di teoria politica (G. Miglio & P. Schiera, Eds.). Il Mulino.

Schmitt, M. N. (Ed.). (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press.

Schwartau, W. (1999). Information Warfare: Chaos on the Electronic Superhighway. Thunder's Mouth Press.

Smith, D. B., Müller, H. A., & Tilley, S. R. (1997). The Year 2000 problem: Issues and implications (CMU/SEI-97-TR-002, ESC-TR-97-002). Software Engineering Institute, Carnegie Mellon University.

Sprout, H. (1963). Geopolitical hypotheses in technological perspective. World Politics, 15(2), 187–212.

Sprout, H., & Sprout, M. (1979). The ecological perspective on human affairs: With special reference to international politics. Greenwood Press. (Original work published 1965).

Starosielski, N. (2015). The Undersea Network. Duke University Press.

Steed, D. (2019). The politics and technology of cyberspace. Routledge.

Stefanachi, C. (2015). Le trasformazioni dello spazio politico-geografico e la nuova mappa delle minacce e delle opportunità: Origini e temi della riflessione geopolitica americana. Storia del pensiero politico, 3(September–December).

Stefanachi, C. (2017). America invulnerabile e insicura: La politica estera degli Stati Uniti nella stagione dell'impegno globale: Una lettura geopolitica. Vita e Pensiero.

Sterling, B. (1992). The hacker crackdown: Law and disorder on the electronic frontier. Bantam Books.

Svantesson, D. J. B. (2020). Data localisation trends and challenges: Considerations for the review of the privacy guidelines (OECD Digital Economy Papers No. 301). Organisation for Economic Co-operation and Development.

Tarnoff, B. (2016, July 15). How the internet was invented. The Guardian.

Topor, L. (2024). Cyber Sovereignty: International Security, Mass Communication, and the Future of the Internet. Springer.

Trump, D. J. (2017). National security strategy of the United States of America. Washington, DC: The White House.

Trump, D. J. (2018). National cyber strategy of the United States of America. Washington, DC: The White House.

Turner, F. J. (1893). The significance of the frontier in American history. American Historical Association.

Chapter II - Geography and Cyberspace

Moving Beyond the Illusions

The world inherited from the 1990s has left us with the persistent illusion of cyberspace as a metaphorical realm – deterritorialized, self-regulating, and free from the constraints of geography or geopolitics. This vision, rooted in the liberal optimism of the post-Cold War era, imagined the digital sphere as a borderless space of interaction where flows of information would transcend states, sovereignty, and power politics. As the historical reconstruction developed in Chapter I has shown, this imaginary gradually eroded, yet it would be misleading to conclude that the "post-territorial" vision is therefore irrelevant to the present analysis. Even if the strongest versions of the 1990s "flat world" thesis have largely receded, the paradigm was extremely consequential for a sufficiently long period to shape institutional expectations, policy vocabularies, and create analytical blind spots, normalizing the tendency to treat digital connectivity as detached from infrastructure and jurisdiction, thus naturalizing the neglect of material and spatial constraint. Moreover, important residues of the post-territorial imaginary persist in contemporary discourse and policy practice, not as a coherent doctrine but as a durable grammar through which cyberspace is still frequently described.

For instance, in the fields of cybersecurity and cybercrime, cyberspace is often framed as a "borderless" environment in which threats circulate independently of geography. The same is true for internet governance debates: the normative vocabulary of an open, global, interoperable internet continues to structure policy discussions, frequently treating territorial fragmentation as a risk to be avoided – and even as something highly unlikely, given – according to some (see, for instance, Mueller 2017) – the obsolescence of state-centric assumptions. In the political economy of the digital sphere, trade agendas and policy discourse often treat cross-border data flows as the lifeblood of the contemporary economy, with localization framed as a deviation from an assumed baseline of frictionless circulation. These strands do not amount to a simple revival of 1990s cyber-utopianism. Rather, they coexist − often uneasily − with the growing reassertion of jurisdiction, infrastructure control, and geopolitical bloc formation. It is precisely this tension between the enduring language of borderless connectivity and the material-geopolitical constraints of digital infrastructures that motivates the chapter's focus: moving beyond metaphor to examine how geography conditions

cyberspace's physical architecture, and how that architecture produces patterned hierarchies, dependencies, and vulnerabilities.

Even today, many liberal democracies continue to operate within this inherited framework, treating cyberspace as an abstract domain governed primarily by technical standards, market logic, and transnational cooperation. However, this metaphorical understanding of the virtual domain – what Murray (2006, 47), in his *Geographies of Globalization*, described as a space that does not refer to any territorial unit created by the Internet – has proven, as shown in the first chapter, increasingly untenable. The belief that the digital sphere could be divorced from physical space has given way to the need of a more grounded understanding of cyberspace as a domain inseparable from material infrastructures, legal jurisdictions, and geopolitical rivalries. Rather than the "demise of geography", the digital turn has brought geography back in through the back door. This dissertation departs from the conception of cyberspace as a metaphor and instead reasserts space, first in its geographical dimension, then in its political form, as a key analytical category for understanding the contemporary dynamics of cyberspace. If the first chapter sought to reconstruct the historical, political, and cultural foundations that allowed a certain conception of cyberspace to emerge and consolidate, this section takes a step further. In fact, before engaging directly with the geographical dimension of cyberspace, we will briefly examine the specific illusions, and the contradictions that are embedded in the dominant liberal representation of the digital domain.

As Morgus and Sherman (2018) noted, liberal-democratic governments, with the United States at the forefront, have long promoted an idealized version of the internet, defined by five guiding principles: freedom, openness, interoperability, security, and resilience. These principles, though rarely precisely defined, have come to represent the normative core of the liberal-democratic policy community. Since the early 2000s, they have been consistently reaffirmed in key strategy documents, such as the U.S. 2018 Department of Homeland Security's Cybersecurity Strategy and the U.K.'s 2016 cybersecurity plan as well as, for example, in the international digital agendas of France (2017) and Canada (2018). The internet, in this view, is imagined as a universal, self-regulating infrastructure, inherently aligned with liberal democratic values and resistant to state control. This vision, however, is increasingly at odds with the material, legal, and political realities of the contemporary internet. As Morgus and Sherman (2018, 14) point out, and in alignment with what we discussed in the previous chapter, countries such as China, Russia, and Iran have actively rejected the liberal model, building alternative frameworks rooted in state sovereignty, control, and strategic infrastructure development. More crucially – and more interestingly – even liberal democracies have begun to contradict their own ideals: the repeal of net neutrality protections in the U.S., the growing centralization of control in the

hands of private actors, and the reassertion of national jurisdiction over data flows all reveal deep inconsistencies within the liberal paradigm itself.

These contradictions are not marginal, but structural. While liberal-democratic governments continue to promote the idea of a free, open, and decentralized internet, their practices often tell a different story. The reliance on a handful of powerful technology companies to mediate access, regulate content, and manage critical infrastructure has produced a *de facto* centralization that undermines both openness and resilience. Content delivery networks, cloud service providers, and DNS operators have become *choke-points* through which vast amounts of traffic are routed, effectively transforming what was once conceived as a distributed network into a tightly managed and fragmented space. This tension becomes even more apparent when we consider how private actors – particularly major tech companies – can no longer be treated as neutral intermediaries. On the one hand they manage the core infrastructure of the internet, moderating speech at scale, and shaping access to information globally, while on the other, at the same time, their operational and political autonomy is profoundly constrained by the jurisdictions in which they are legally incorporated and economically embedded. In the United States this has led to a growing convergence between corporate governance and national interests. Companies such as Microsoft, Amazon, or Google are not only expected to comply with domestic regulations, but also to align themselves with national security priorities. This is particularly visible in areas like cloud infrastructure, data governance, and technological R&D. As acknowledged in the 2017 (White House) National Security Strategy, the United States government explicitly recognizes the strategic importance of the private sector, calling for closer coordination with national defense objectives:

> The U.S. Government will use private sector technical expertise and R&D capabilities more effectively. Private industry owns many of the technologies that the government relies upon for critical national security missions. The Department of Defense and other agencies will establish strategic partnerships with U.S. companies to help align private sector R&D resources to priority national security applications.

Moreover, the principle of interoperability – originally framed as a safeguard against fragmentation – has been selectively interpreted to serve commercial and strategic interests. Regulatory decisions, such as data localization requirements and restrictions on foreign platforms, are increasingly shaped not by universalist principles but by national economic agendas and security concerns. In this way, liberal states participate in the very dynamics of digital sovereignty and infrastructural nationalism that they rhetorically oppose when observed in authoritarian contexts. Even the increased commitment to cybersecurity often reinforces exclusionary or securitized approaches to internet

governance. The securitization of interconnectivity, meaning here the treatment of digital dependencies as strategic risks, has led many liberal democracies to adopt policies that echo the very control-based models they claim to reject. Initiatives aimed at securing "trusted" technology supply chains, banning foreign vendors, or imposing national control over routing infrastructures reflect an underlying convergence between liberal and authoritarian approaches to cyberspace governance. Ultimately, therefore, even the liberal model struggles to reconcile its idealized normative commitments with the geopolitical, infrastructural, and economic realities of the global internet. The vision of a neutral, open, and global cyberspace becomes increasingly difficult to sustain in a world where control over digital infrastructures, platforms, and standards has become a matter of national interest and international rivalry.

The contradiction between normative ideals and actual practices point to a deeper transformation in the spatial ontology of cyberspace. What was once conceived as a domain of frictionless flows, immune to the constraints of physical space and political authority, has increasingly come to resemble a fragmented and hierarchical landscape. This shift reflects not only a change in practices, but a conceptual realignment: from a de-territorialized imaginary of cyberspace to a re-territorialized digital order structured around spatial divisions, jurisdictional claims, and sovereign control. In this context, it is no longer possible to sustain the idea of cyberspace as an immaterial or metaphorical domain. On the contrary, digital infrastructures – cables, data centers, exchange points – are materially embedded, geographically situated, and politically governed. Their placement follows patterns shaped by distance, access, terrain, political alliances, and strategic imperatives. This growing entanglement between cyberspace and geography signals the return of spatial categories that liberal discourses had long displaced. Geography re-emerges here not simply as background, but as an active and structuring principle in the exercise of digital power. To capture this evolution, it is useful to turn to Carl Schmitt's conceptual terminology. Schmitt (1991 [1950]) famously argued that every legal and political order is grounded in a spatial configuration, what he called *nomos* – the division, appropriation, distribution, and delimitation of land. Applied to the digital realm, this insight suggests that the current phase of cyberspace is witnessing the emergence of a new *nomos*: one that moves from the idealized ideas of a free, open environment, deterritorialized flows, to the reassertion of spatial control as a condition for political authority. Where cyberspace was once framed through a thalassocratic imaginary, governed by circulation, openness, and the management of flows is now increasingly governed through terrestrial logics: border enforcement, infrastructural sovereignty, and spatial differentiation. While the invocation of a *nomos* of cyberspace offers a useful conceptual lens through which to interpret current transformations, it is important to acknowledge the limits of this analogy. At this stage, it would be premature to speak of a fully developed *nomos* in the Schmittian

sense. The digital domain remains a relatively recent field of strategic intervention for states, and the absence of stable, shared legal and institutional arrangements continues to constrain the consolidation of a coherent spatial order. Nonetheless, what is increasingly visible is the progressive entrance of states into cyberspace as sovereign actors – seeking to reshape a domain once imagined as fluid, deterritorialized, and self-regulating into a space structured by jurisdictional boundaries, infrastructural control, and geopolitical differentiation. The reference to *nomos* should therefore be read not as a claim about the existence of a mature and codified legal order, but as an indication of a broader trend: the reconfiguration of cyberspace from a non-territorial system of flows into a spatially grounded field of power, increasingly tied to geographic and political logics.

This shift in the spatial logic of cyberspace has not gone unnoticed in contemporary theoretical debates. Indeed, the re-emergence of territoriality as a structuring force in digital governance has been critically explored by several authors (among others see: Casini 2020; Munn 2023) – most notably Benjamin Bratton (2015) – who have returned to Schmitt's spatial concepts to interrogate the changing geographies of power in the age of planetary-scale computation.

As Benjamin Bratton compellingly reminds us in his volume *The Stack* (2015, 54), Carl Schmitt's political ontology begins with the primal incision of the plough into the earth – an act that, through its physical inscription, creates a line, a furrow, a claim: the spatial precondition for sovereignty and law. Sovereignty, for Schmitt, emerges from the act of grounding authority in space – *land taken and held*, defended, enclosed. The archetypal political gesture is not abstract jurisdiction but concrete occupation. Bratton mobilizes this Schmittian imagery to reflect on how planetary-scale computation reshapes this dynamic. In his reading, the infrastructure of global digital systems – cables snaking across oceans, data centers embedded in terrestrial grids, satellite constellations overhead – does not merely operate on top of territory but actively *produces* new spatialities, recomposing the ground it occupies by embedding jurisdiction, infrastructure, and governance into layered, dynamic systems (2015, 57). It should be acknowledged that Bratton (2015, 64) does not suggest that states have relinquished the ambition to inscribe digital space with sovereign control. On the contrary, he recognizes that several state actors – including Russia, China, Iran, and to a lesser extent the European Union –are explicitly attempting to reassert jurisdiction over cyberspace by establishing forms of digital territoriality. These include deep packet inspection systems, sovereign clouds, regional encryption standards, and policies mandating that data be stored and processed within national borders. Such initiatives aim to bring the informational layers of cyberspace back «inside the Westphalian loop» as Bratton (2015, 64) puts it, subjecting digital flows to the same legal and political optics that govern physical territory. In this sense, the logic of territorial sovereignty is being

reprogrammed into the infrastructures themselves. However, Bratton is skeptical that these efforts represent the dominant or inevitable direction of digital governance. He presents them as partial, reactive, and in many respects counterproductive, as gestures that may succeed in establishing zones of relative autonomy, but that ultimately remain at odds with the deeper logic of planetary computation. For Bratton, in fact, the nomos of the cloud is not easily tamed by the state; its spatial form is not linear or bounded but layered, recursive, and modular. Rather than restoring Schmittian territorial order, Bratton envisions a topology in which jurisdictional lines are rendered *flexible, reversible, programmable*. The sovereign decision is embedded not in the suspension of law over bounded land, but in the automated architectures of platforms, in the interfaces, protocols, and infrastructures that frame, route, and filter interactions. Territorial sovereignty, in this view, becomes but one among many competing logics shaping the space of the stack. Yet – and this is the core contention of the present work – such a diagnosis, however sophisticated, underestimates the extent to which the state's reassertion of territorial control is already materializing across multiple levels of the digital world. From India's data localization laws to Russia's "sovereign Internet", from China's Great Firewall to the growing European emphasis on digital strategic autonomy, states are not merely attempting to regulate cyberspace but to re-inscribe it as sovereign space. These moves are not simply theoretical or symbolic; they are infrastructural. They manifest in the physical siting of cables, landing points, and data centers, in the legal constraints placed on data flows, and in the increasing coupling of network topologies with national jurisdictions. What is emerging, then, is not a frictionless field of reversible networks but a digitally territorialized world composed of interlinked but politically bounded spaces, a plural landscape of sovereign digital enclaves with its centers, its territorial lines and its peripheries. If Bratton sees the territorialization of the cloud as one possible trajectory among many, this work suggests that it is fast becoming the central vector of cyber-geopolitical transformation. The soil, once again, is being ploughed. Only now, it is digital – and the furrows are lined with fiber. What is important to note here is that transition is not merely conceptual. It manifests concretely in a series of developments that will be addressed in depth in this and in the following chapter: from data localization laws and the physical exclusion of foreign vendors to the construction of national firewalls and the securitization of global chokepoints.

This broader reassertion of territorial logics in cyberspace necessitates a more focused inquiry into one specific spatial dimension: geography. That is, the concrete spatial substrate within which cyberspace takes shape, and to which it remains, in crucial ways, tethered. While the territorialization of the digital domain unfolds across multiple layers – legal, infrastructural, strategic – this chapter turns its attention to the material and spatial anchoring of cyberspace in geographic space.

Despite growing evidence to the contrary, the immaterial vision of cyberspace continues, albeit – as said − in a more reduced and diluted form, to persist in public discourse and among certain political actors, functioning as an intellectual frame through which the digital world is still imagined as stripped of its material underpinnings. This enduring metaphor in fact, is not merely a theoretical vestige, but continues to inform some institutional decisions and popular imaginaries alike. A striking example is the widely circulated 2023 interview with U.S. Vice President Kamala Harris, who explained cloud storage by stating: «It's on your laptop, and it's then therefore up here in this cloud, that exists above us, right? It's no longer in a physical place». While arguably a simplification for a general audience, such statements reinforce the image of cyberspace as a disembodied realm, seemingly detached from infrastructure, jurisdiction, or geography. Similar assumptions underlie more consequential policy decisions. For instance, in the lead-up to the Russian invasion of Ukraine, Amazon Web Services assisted the Ukrainian parliament in transferring critical data from local servers to the cloud (AWS, 2022). Many commentators (Tangalakis-Lippert 2022; Mitchell 2022; Mueller et al. 2023) heralded the operation as a textbook case of cyberspace's deterritorializing potential. Yet, this interpretation overlooks a crucial point: the cloud is not ethereal but it resides in physical data centres operated by corporations and situated in specific territories. Contrary to Tangalakis-Lippert's claim that «you can't take out the cloud with a cruise missile», a data centre *can* in fact be targeted. It is simply more difficult when geographically removed from the conflict zone or located in the sovereign territory of a NATO member state. In this case, AWS effectively granted Ukraine a form of "cyberstrategic depth" by relocating data to more secure geopolitical locations. But this move did not erase the relevance of geography, on the contrary, it underscored it.

Such examples highlight the analytical urgency of reclaiming materiality, spatiality, and territoriality as central dimensions in the study of cyberspace. As David Steed (2015) convincingly argues, the idea that cyberspace signals the "demise of geography" does not withstand empirical scrutiny. While certain layers of cyberspace may appear immaterial or virtual, they ultimately rely on a physical substratum composed of cables, servers, routers, satellites, and other hardware components. These infrastructures are not placeless: they are situated in specific geographical locations and embedded within legal, political, and strategic jurisdictions. In this sense, cyberspace is not exempt from spatial constraints – it is, on the contrary, materially grounded and territorially circumscribed. Numerous cases illustrate this interdependence between digital operations and geographical space. The Stuxnet operation, for instance – Steed (2015, 87) reminds us – revealed that even the most advanced cyberwarfare techniques must confront spatial and geopolitical constraints (on this see also Lindsay, 2013). The challenge of penetrating a so called "air-gapped" network – meaning a network that is physically disconnected from the Internet – was not merely technical but also physical and spatial.

Successfully infiltrating Iran's nuclear facilities required physical proximity, covert access, and operational reach within a tightly secured and authoritarian context. Geography, rather than being circumvented by digital means, re-emerged as a decisive variable. Moreover, the 2008 cyberattacks against Georgia offer another telling example. Despite the country's limited digital penetration at the time, its structural vulnerability lay in the geographical routing of its Internet traffic. Over half of Georgia's external connections passed through Russian infrastructure, while much of the remainder was routed via Turkey and Azerbaijan, countries whose networks were also partially dependent on Russian systems. This configuration granted Russia a strategic positional advantage and enabled various forms of digital interference rooted in the spatial architecture of cyberspace.

In the same vein, Steed (2015, 88) draws attention to the case of the UK's Tempora program – disclosed through the Snowden revelations – which enabled the interception of transatlantic communications by exploiting access to submarine cables landing on British soil. Without jurisdictional control over those landing stations, such surveillance capabilities would not have been possible – further illustrating how geopolitical positioning enables and constrains the projection of cyber power. While tapping cables underwater is technically complex and risky, Steed notes that interception is often more effectively conducted once the cables make landfall and their data is integrated into terrestrial networks. In this context, the United Kingdom's geographic location situated at a key "technical chokepoint" where Atlantic cables reach the European continent has proved strategically advantageous. This geographical condition, combined with long-standing intelligence-sharing partnerships – especially with the United States and other "Five Eyes" members (Australia, Canada, and New Zealand) – has made Britain a crucial node in global surveillance architectures. An additional and innovative case is that of Estonia's establishment of so-called "data embassies": sovereign data centres located abroad but fully under Estonian governmental control. These facilities serve as strategic backups for Estonia's e-government infrastructure and are designed to ensure digital continuity in case of crisis or occupation. As Kadlecová (2024) notes, the model explicitly reinforces territorial Westphalian sovereignty in digital form, securing the exclusion of external actors even when infrastructure is hosted beyond national borders.

All of these examples serve to illustrate a common insight: that space – particularly in its geographic and territorial articulations – remains an indispensable analytical category for understanding cyberspace. In light of this, the chapter aims to reorganize and systematize the debate around the physical infrastructure of cyberspace into a coherent analytical framework – since many of the insights currently available derive from scattered and heterogeneous sources. This chapter brings

renewed attention to the foundational layer of the digital domain – the material substrate that sustains global interconnection.

The chapter will therefore proceed in two main steps. First, it reconstructs the historical and technological trajectories of cyberspace infrastructures, focusing primarily on submarine cables, landing stations, and data centres as the key nodes of global digital connectivity. While the role of satellite infrastructure cannot be ignored, it will be addressed only in a secondary capacity, due to its distinct characteristics and operational logic. Through this focus, the chapter seeks to offer a grounded understanding of how physical infrastructure and geographic space co-constitute both the architecture and the politics of the digital realm. Second, drawing on a partially original dataset, the chapter provides a geographical and topological mapping of global cyber infrastructure through the use of Geographic Information Systems (GIS) and network analysis. The goal is to represent the material structure of cyberspace in concrete terms – tracing its development, identifying critical nodes, and assessing which political actors occupy central or peripheral positions within the global network. Particular attention is given to how geographic conditions permeate and shape the configuration of this infrastructure. This empirical section enables a detailed examination of how political and physical variables influence the spatial distribution of infrastructure nodes and routing paths, and how the resulting network topology mirrors broader geopolitical dynamics.

The guiding research question of this chapter is the following: *How do geographical factors influence the spatial distribution of cyberspace infrastructures?*

This inquiry will be pursued on both a historical and empirical level adopting a deliberately broad conception of geography and geographical factors. Following Colin Gray's (1996) insight, geography is understood not merely as the physical background of human activity, but as multi-dimensional field that includes physical, human, economic, political, cultural, strategic dimensions. While these domains are often treated separately, Gray emphasizes that any serious analysis of geopolitical power must consider them together, thus even when addressing cyberspace and cyberpower. Geography, though conceptually distinct from politics, strategy, or economics, exerts a formative influence on each, shaping not only the material conditions of action, but also the preferences, constraints, and imaginaries through which actors interpret and engage with the world. In the context of this chapter, geographical factors are thus taken to include terrain, location, distance, climate, natural hazards, as well as legal jurisdictions, infrastructural control, and broader patterns of international alignment.

This insights on geography's multi-dimensionality and its pervasive influence, is particularly pertinent today. Especially in light of the growing scientific consensus on climate change, it has

become increasingly evident that geography must no longer be understood as a fixed or immutable backdrop. Instead, geographical variables are now recognized as dynamic and transformative – subject to change and capable, in turn, of shaping the strategic behavior of political actors. Recent scholarship (Lavorio 2021; Gilli et al. 2024) reflects this shift by moving beyond the traditional view of geography as a passive stage for political action, and instead foregrounding its active role in producing new configurations of power, risk, and vulnerability. Let's be clear on this point: this is not a return to environmental determinism, but rather an acknowledgment that the physical environment constitutes the setting within which human action unfolds, and as such, it carries tangible implications for political and economic decision-making. The core intuition of this chapter is that this broad conceptualization of geography – as dynamic, contingent, and strategically relevant – must also be extended to the analysis of cyberspace.

The chapter unfolds in three main steps. It first outlines the methodological framework that underpins the analysis, clarifying the sources, techniques, and conceptual tools employed. It then turns to a historiographical reconstruction of submarine cable infrastructures, tracing their emergence, evolution, and geopolitical significance. Finally, it presents the empirical analysis of contemporary infrastructures, focusing on both submarine cables and data centers, in order to assess how geography continues to structure the architecture of cyberspace.

A New Methodological Approach to Cyber Infrastructure: Historical Reconstruction, Mapping and Network Analysis

The infrastructure underlying cyberspace consists of a vast and intricate network of physical components, ranging from submarine fiber-optic cables, terrestrial backbones, and data centers to internet exchange points (IXPs), satellites, routers, and servers. These devices and systems form the material substrate that enables the functioning of the global internet and digital communications. However, their distribution is highly uneven. The spatial arrangement of cyber infrastructure reflects asymmetries in technological capabilities, economic resources, and geopolitical positioning. Certain regions concentrate strategic assets such as cable landing points and hyperscale data centers, while others remain on the margins of global connectivity. These disparities are not merely technical, instead they have significant implications for political autonomy, economic development, and digital sovereignty. The material infrastructure of cyberspace traces fibre-optic routes across ocean floors, assigns strategic value to coastal landing points, occupies physical spaces through its hubs, and redefines national security priorities – effectively redrawing the maps of a new cyber geopolitics that

deeply influences economic decisions and political behaviour. This emergent topography importantly reconfigures the traditional notions of centre and periphery, at times reproducing their historical logic, at other times transforming the very meaning of spatial hierarchies. Peripheries today are still those regions that remain at the margins of internet infrastructure – disconnected or under-connected zones that lie outside the reach of robust digital networks. The decision to link these areas via a submarine cable, to locate a data centre, or to establish a satellite base is a strategic act – one that can significantly alter the political and economic trajectory of entire regions.

If traditionally scholars (for a more comprehensive discussion on this see: Kandera et al. 2004; Valigi 2018)[11] have assessed international power in terms of demographic size, access to natural resources, economic strength, and military capabilities, today – alongside those classical factors – one must add technological development and digital capacity as increasingly central components of power. Internet penetration, for instance, reaches nearly 100% of the population in some states, while in others – particularly in some areas of Africa and Asia – it remains below 25% (Digital Report 2024). These disparities are not merely technical, but deeply political: they shape access to global markets, information flows, and platforms of governance. The geography of infrastructure is, therefore, a geography of power.

Understanding the topography and the topology of the physical Network, and thus identifying its spatial distribution, locating its central nodes and peripheral zones, not only helps move beyond the

[11] It is, of course, acknowledged that measuring power in international relations involves significant conceptual and methodological difficulties, particularly regarding which factors are included or excluded. The literature offers divergent perspectives not only on *what* should be measured, but also on *whether* power can be meaningfully quantified at all. Even classic strategic authors such as Alfred Thayer Mahan at the end of the XIX century developed a sort of national power index by identifying six key determinants: geographical position, physical conformation, extent of territory, population size, national character, and the character of government (Mahan 1890). More recently, composite indices such as the Composite Index of National Capability (CINC), which aggregate demographic, industrial, and military variables, have been widely employed but are often criticized for their sensitivity to systemic fluctuations and for their inability to capture less tangible forms of power (Organski & Kugler, 1980; DiCicco & Levy, 1999; Gleditsch & Ward, 1999). Other scholars go further, questioning the very possibility of objectively measuring power, pointing to the non-fungibility of power resources and the central role of legitimacy and perception in shaping power relations (Guzzini, 2009). Still others conceptualize power as the stable combination of multiple factors at high levels, identifying territory, population, and economic weight as primary indicators, while treating others – such as military spending – as derivative variables, often linked to GDP (Valigi, 2018). The purpose of this statement is not to intervene in this ongoing theoretical debate, but rather to highlight how, over the past thirty years, digital infrastructures have come to play an increasingly important role in the (re)definition of power – reshaping strategic hierarchies and altering how influence and capability are projected in global space.

myth of disembodiment and keeps us at a distance from persistent illusions, but also allows us to (*re*)discover a geography marked by both continuity and transformation. It reveals old and new strategic chokepoints, areas that become attractive or vulnerable due to topographic, climatic, or political features, novel interconnections, and changing meanings in the absolute and relative positioning of states. This, in turn, reflects different strategies of power projection and digital entrenchment. Mapping these dynamics helps to elucidate how a state's position – both in absolute terms and relative – within global digital infrastructures shapes its capacity to exert power. Such positional advantage enables the projection of influence through infrastructure provision, the consolidation of spheres of digital interdependence, and the formation of new strategic alignments. In certain contexts, it may also underpin asymmetric dependencies that resemble neo-colonial relations (Balestrieri 2024), while simultaneously enhancing internal resilience and broadening the instruments available for geopolitical competition. States that serve, for example, as transit hubs for major submarine cables, or host large-scale data centers and cloud infrastructure, gain strategic importance that may amplify their geopolitical relevance. Conversely, territories excluded from core connectivity routes risk digital marginalization, increasing their technological dependence and vulnerability. Moreover, the physical placement of digital infrastructures increasingly intersects with military alliances, economic agreements, and geopolitical spheres of influence – shaping what some call a *geopolitics of connectivity* (Flint et al. 2019).

This study focuses primarily on two core components of cyberspace's physical infrastructure: namely, submarine cables and data centres, which constitute the main units of analysis in this chapter. Other elements such as terrestrial fibre-optic networks, Internet Exchange Points (IXPs), wireless towers, local access systems, and satellite infrastructure, while critical for ensuring full connectivity, are not treated as central objects of inquiry. This choice is due both to the uneven availability of reliable and homogeneous data and to the need to focus on those infrastructural elements that can be understood as digital chokepoints – meaning here strategic nodes whose disruption or control can have disproportionate effects on the functioning of the entire network.

Despite the widespread perception of the internet as a diffuse and decentralised system, digital connectivity remains deeply concentrated in physical terms. Data are stored and processed in a limited number of locations – the data centres – managed by a small group of providers with the capacity to deliver essential services at scale. At the same time, global data flows are channeled through narrow corridors: the submarine cables that crisscross the ocean floor and carry more than 95% of international internet traffic. These undersea "information highways" are not evenly distributed, and the points where they make landfall – the cable landing stations – become infrastructural bottlenecks

of global significance. In order for digital traffic to circulate globally, information must converge, flow through, and depend on these spatially concentrated paths and places. The persistence of chokepoints and concentration in global digital connectivity can be understood through two interrelated but analytically distinct dimensions: the technical-logical layer and the geographical-infrastructural one.

On the one hand, although the logical architecture of the internet is designed to enable distributed and flexible data transmission through the use of packet switching, this potential remains significantly constrained in practice. As discussed in the first chapter, packet switching is a method of data transmission that breaks information into discrete packets which, in theory, can travel along different paths through the network before being reassembled at their destination. However, actual routing behaviour is shaped by structural limitations and protocol-level choices that often reflect political, commercial, or administrative preferences rather than purely technical efficiency. The main protocol that governs data flows across autonomous systems – the Border Gateway Protocol (BGP), and particularly the external BGP (eBGP) – does not prioritise efficiency or redundancy. Instead, routing paths are shaped by political and commercial decisions made by network operators, such as peering agreements and transit arrangements (for a more in-depth analysis on BGP and its geopolitical implications see: Douzet et al. 2020; Sherman 2020; Limonier et al. 2021). As a result, international data traffic often converges on fixed routes and traverses the same physical links, reinforcing infrastructural dependencies.

On the other hand, geographical configurations further accentuate this centralisation. Landlocked countries or geographically isolated regions or islands are structurally dependent on neighbouring states or on a limited number of submarine cable connections. Where terrestrial connections dominate, as in the case of the landlocked countries, the lack of physical redundancy can expose entire nations to infrastructural fragility. A widely cited example is the 2011 incident in Georgia, where a 75-year-old woman in the village of Ksani accidentally severed a fibre-optic cable with a shovel. This cable, owned by the Georgian Railway Telecom, was one of only two linking Armenia to the global internet (Parfitt 2011; Lomsadze 2011). The damage resulted in a near-complete blackout of internet services across Armenia for several hours. While anecdotal, the episode reveals the extent to which entire nations may rely on a small number of physical routes for digital connectivity – especially in regions with limited infrastructure redundancy. Taken together, these logical, infrastructural and geographical dynamics reveal a persistent centralisation within global digital connectivity. They demonstrate that the circulation of data is not spatially neutral, but rather conditioned by chokepoints, commercial hierarchies, and geopolitical choices that define the spatial

logic of cyberspace. Thus, understanding their topography, distribution, and concentration is crucial to analysing how digital interconnection is shaped by, and in turn shapes, global power relations.

To investigate these dynamics more systematically, the chapter now turns to an in-depth analysis of the three key infrastructural components previously introduced: submarine cables, landing stations, and data centres. Each will be examined through a twofold approach that integrates a historical and technological reconstruction with an empirical spatial analysis conducted through Geographic Information Systems (GIS). This structure is designed to move beyond anecdotal accounts or purely descriptive mapping, and instead to uncover the enduring rationalities that underpin the spatial organization and political significance of digital infrastructure.

The historical component is essential not only as a matter of technical historiography, but because it reveals how global connectivity infrastructures have, from their inception, been shaped by strategic logics and spatial constraints. Moreover, this historical section will provide the analytical ground to assess the central hypothesis of this dissertation: that spatial and geographical factors are not merely contextual elements but play a constitutive role in shaping the conditions of control and distribution of cyber infrastructure, in particular in the first part will be tested on the submarine cable systems. Specifically, this influence operates along two interrelated dimensions: on the one hand, the ability to exert political authority over the territory where landing stations are located; on the other, the spatial configuration and dispersion of the cable routes themselves, which affect both their strategic resilience and the capacity to monitor or disrupt them.

The early submarine cable systems of the nineteenth and early twentieth centuries were developed in close conjunction with the imperial ambitions of the British Empire. These infrastructures were never neutral carriers of information: they were conceived, routed, and secured according to explicit military, commercial, and geopolitical considerations. Issues such as redundancy, cable vulnerability, and the ability to project power globally were already central to infrastructural planning and political debate more than a century ago. Remarkably, these decisions were deeply embedded in geographic reasoning – including assessments of terrain, maritime accessibility, control over chokepoints, and the strategic positioning of colonies and naval stations. The enduring relevance of geography is thus evident not only in the materiality of infrastructure, but also in the rationalities that have historically guided its deployment. What emerges is a clear historical continuity: the geopolitical dimensions of connectivity are not a recent development, but a structural and long-standing feature of global communications systems. As this chapter will show, contemporary concerns with chokepoints, infrastructure protection, and digital sovereignty resonate closely with these earlier configurations – not as analogies, but as recurrent expressions of the same spatial and strategic imperatives.

Alongside the historical and technological reconstruction, this chapter employs Geographic Information Systems to systematically examine the spatial configuration of cyberspace's critical infrastructures. GIS is a key tool for analysing political, environmental, and infrastructural issues, and plays an important role in political and social science research (Di Salvatore and Ruggeri 2021). Its capacity to visualise and analyse spatial patterns enables scholars to study a wide range of phenomena that are inherently spatial in nature. In political science, GIS has been employed to investigate electoral behaviour, mapping voting patterns in relation to demographic, economic, and territorial variables (Agnew and Shin 2025; Shin and Agnew 2011). It has also been used to examine patterns of social inequality, urban segregation, and access to public services, offering insights into how space mediates political inclusion and exclusion (Martínez 2009). In conflict studies, GIS has facilitated the spatial analysis of violence, displacement, and the geography of state and non-state control (Dawwas 2014; Stephenne et al. 2009). Moreover, research on migration has benefited from GIS-enabled tracking of mobility flows, refugee settlement patterns, and transnational networks (Mijani et al. 2021). In all these topics, GIS supports a more spatially grounded understanding of political processes, offering the ability to move from abstract models to context-specific, territorially embedded analyses. This brief overview of diverse applications is by no means exhaustive, but it aims to highlight the complexity and analytical validity of GIS as a tool within the social and political sciences. Designed to capture, store, manage, and manipulate spatial data, GIS enables the visualisation and analysis of diverse geographical variables – from zones of desertification and flood risk to patterns of infrastructural development and demographic distribution. As O'Reilly (2019, 25) argues, the rise of GIS technologies over the past three decades has significantly reshaped in particular the ways in which geopolitics is conceptualised and operationalised. By allowing the integration and layering of heterogeneous data, GIS provides a means to visualise and interrogate how political power is exercised across geographic space – ranging from local territorial claims to global conflict zones. In this sense, GIS contributes not only to the empirical mapping of spatial phenomena but also to a more nuanced understanding of how power, territory, and space interact in the construction of geopolitical order. As such, GIS has been employed in diverse contexts – from mapping human rights abuses (e.g. Amnesty International, Freedom House) to visualising areas of military deployment or political conflict (e.g. ACLED), or humanitarian operations under the United Nations. Crucially, these applications underscore that the value of GIS extends beyond technical cartography: it lies in its capacity to reveal the spatial dimensions of political and strategic dynamics – especially in a context where territorial configurations and digital infrastructures are increasingly interwoven.

GIS, in fact, serves not merely as a cartographic tool, but as an analytical framework capable of integrating and interrogating multiple spatial variables. Its very nature makes it particularly well-

suited for analyzing the spatial and geopolitical dimensions of cyberspace infrastructure, as it allows for the systematic examination of how physical geography, environmental constraints, jurisdictional boundaries, and infrastructural configurations intersect to shape patterns of digital connectivity and power. Through the construction of a multilayered dataset encompassing submarine cables, landing stations, and data centres, the analysis reveals how these infrastructures intersect with key geographical, environmental, and demographic factors. The use of GIS enables a more granular and empirically grounded approach to understanding the spatial distribution of cyberspace infrastructures. Unlike static maps or schematic visualisations, GIS, in fact, allows for the layering and cross-referencing of heterogeneous data sources, ranging from vector data on infrastructure nodes to raster data on environmental risk, and supports a variety of spatial operations, from proximity analysis to correlation testing or heatmapping. Thus, this analytical flexibility is particularly essential when addressing a domain as complex as cyberspace. In particular, the analysis conducted in this chapter involves overlaying critical infrastructure layers with a range of contextual variables, including average temperature, population density, natural hazard exposure, seabed characteristics, and national jurisdictional boundaries. These variables are not analysed in isolation, but examined in relation to one another – for instance, assessing whether data centres are disproportionately located in cooler climatic zones, whether landing stations cluster near key maritime chokepoints, or to what extent key submarine cable routes traverse regions that are exposed to significant natural hazards, such as seismic activity or extreme weather events, thereby increasing their physical vulnerability. While these correlations do not imply causality, they help surface spatial logics and potential vulnerabilities that would otherwise remain obscured. The inclusion of physical variables such as bathymetry and natural hazard zones allows for the identification of environmentally sensitive or high-risk locations within the infrastructure network, with implications for both resilience and strategic planning. Likewise, demographic layers such as population density help contextualise infrastructural investments in relation to demand, accessibility, and potential exposure. Jurisdictional overlays, finally, permit the mapping of control, enabling analysis of how infrastructures are embedded in state territory and sovereignty claims. More broadly, the application of GIS in this context serves to reinforce one of the chapter's central claims: that the infrastructures of cyberspace are not randomly distributed or purely technologically driven, but geographically constrained and spatially embedded. By making these patterns visible and analytically tractable, GIS provides a mean to systematically engage with the geography of digital power. It transforms cyberspace from an abstract domain of flows into a mapped terrain – one whose contours are shaped by environmental constraints, economic incentives, geopolitical priorities, and historical dependencies. In this way, GIS analysis contributes not only to mapping infrastructure, but to identifying patterns of strategic distribution, spatial

clustering, and infrastructural risk – all of which are key to understanding how geography continues to shape the political economy and geopolitics of cyberspace.

In addition to the spatial analysis conducted through GIS, this chapter also employs a network analysis of the submarine cable system, building on the same underlying dataset. While GIS enables the identification of spatial concentrations, overlaps, and vulnerabilities based on physical geography, network analysis allows us to shift perspective and model digital connectivity as a set of relational ties – that is, as a graph composed of nodes and edges. In this representation, each state is modelled as a node, and each submarine cable that connects two countries directly becomes an edge between them.

This abstraction is not meant to replace the geographical map, but rather to complement it by capturing the structural properties of interconnection beyond their spatial location. The rationale behind this analytical step is twofold. First, network analysis allows for a more precise and quantifiable understanding of how states are positioned within the architecture of global connectivity. While maps show where cables go, they do not reveal which countries occupy central positions in the overall topology of the system, nor which ones are peripheral or vulnerable to disconnection. By representing connectivity as a relational graph, it becomes possible to compute key centrality measures that shed light on which actors function as hubs, intermediaries, or influential nodes within the network. It must be noted here that centrality in network analysis is not a singular concept but a family of measures that each capture different aspects of a node's structural importance (on this for instance see: Borgatti et al. 2018, 174), and this is particularly relevant for this work. Broadly speaking, centrality refers to the position of a node within a network and the advantage or influence that accrues from that position. A node may be considered central because its removal would fragment the network, or because it connects otherwise distant parts of the system. For instance, degree centrality captures the number of direct links a node has, suggesting its capacity for immediate interaction. Betweenness centrality measures how often a node lies on the shortest paths between other nodes, indicating its potential control over the flow of information or data. Eigenvector centrality instead reflects not only how connected a node is, but also how well connected its neighbours are – offering a proxy for influence within highly interconnected clusters. In this sense, centrality analysis enables us to conceptualise power and vulnerability not only in territorial terms, but also in structural ones. It allows us to identify states that may act as infrastructural gatekeepers or bottlenecks, those that benefit from high levels of connectivity, and those that are relatively marginal in the topology of global information flows. A complementary perspective is offered by the notion of *structural holes*, introduced by Ronald Burt (1992). Rather than focusing solely on how central a

node is, this framework emphasises the advantage that comes from occupying non-redundant positions within the network – that is, from *bridging* otherwise disconnected segments. In this context, a node is structurally powerful not because of the number or weight of its connections, but because it links together actors or clusters that would not otherwise be directly connected. Two key measures capture this dimension: effective size, which reflects the number of non-redundant contacts a node maintains; and constraint, which quantifies the extent to which a node's connections are themselves interconnected. Nodes with low constraint and high effective size are well positioned to broker information, mediate between regions, and exert disproportionate influence relative to their degree. In the case of submarine cable networks, such countries may not appear as hubs in conventional centrality rankings, but they function as critical gateways whose role is amplified by their unique structural positioning.

Second, this modelling approach offers an opportunity to test how far geographical determinants continue to shape the structure of connectivity when physical space is abstracted away. That is, by "removing" geography from the visualisation and replacing it with a purely relational network, we can observe whether spatial logics continue to assert themselves in the topological structure of the system. In practice, the analysis confirms that geography does not disappear when translated into network form – rather, it re-emerges through patterns of connection, concentration, and clustering. Physical constraints, infrastructural investment, and geostrategic alliances continue to manifest as structural features of the graph, demonstrating that digital connectivity is still deeply conditioned by material and spatial realities. Consider, for example, the case of cluster analysis. This method enables the identification of modular structures within the network – that is, groups of nodes that are more densely interconnected with one another than with the rest of the graph (on this see for a more complete discussion Blondel et al. 2008; Newman 2006). These clusters do not necessarily correspond to predefined geographic regions, but their spatial distribution can be analyzed to assess the extent to which relational proximity mirrors territorial proximity. In other words, even when geography is abstracted from the model, spatial logics may continue to shape the network's topological configuration. If, for instance, regional clusters consistently emerge around continental or subregional groupings, this suggests a persistence of geographic influence within the structure of digital connectivity. In this respect, network analysis does not negate the spatial logic of interconnection – on the contrary, it provides a complementary analytical lens through which to make such logics empirically visible and structurally intelligible. It allows us to interrogate how much of the configuration of cyberspace can still be attributed to geographic embeddedness, even when modelled as a system of abstract relational ties.

The empirical analysis will make it possible to move beyond descriptive mapping and to formally test specific hypotheses about the spatial and topological organization of cyberspace. The second hypothesis posits that submarine infrastructure is disproportionately concentrated around major maritime chokepoints. The rationale behind this claim is that distance, cost, and exposure to disruption constrain global network design, pushing cables to follow shortest-path routing and historically consolidated maritime corridors. The third hypothesis advances the idea that the global submarine cable system is characterized by a hierarchical structure in which a limited number of states act as central anchors of connectivity, while peripheral regions remain dependent on a small number of strategic gateways and brokers positioned at the intersections of regional clusters.

Finally, the last two hypotheses both concern the siting of data centers. The first posits that their global distribution is far from random, but rather highly concentrated in the world's most economically advanced and digitally interconnected regions. Should this prove correct, it would suggest that data centers function not merely as service infrastructures, but also as strategic hubs of power, thereby reinforcing existing hierarchies of wealth, connectivity, and technological capacity. The second hypothesis holds that siting decisions reflect a balance between environmental advantages, the avoidance of natural hazard–prone areas, and proximity to major population centers. While operators seek out cooler climates and stable energy supplies to reduce operational costs, they must also account for exposure to risks such as floods, earthquakes, or sea-level rise, all while remaining close enough to concentrations of digital demand to guarantee low latency and efficient service delivery.

The presentation of the empirical datasets, together with a discussion of the analytical tools employed and the methodological limitations of the study, has been provided in the Research Design chapter. The aim of the present section was to offer a theoretical and methodological framing of the analytical approach, without anticipating its empirical implementation. The chapter, as said, focuses on two core components of cyberspace's physical infrastructure – submarine cables and data centres – each analysed through a dual lens that combines historical-technological reconstruction with spatial and quantitative analysis. In both cases, the historical component – introduced first – serves to contextualize these infrastructures within the broader strategic and political rationales that have shaped their development over time. This diachronic perspective highlights how spatial constraints, technological trajectories, and geopolitical constraints have converged to shape the material configuration of global digital connectivity. Building on this foundation, the chapter then introduces the spatial and network-based analyses, employing Geographic Information Systems and network analysis to examine how the distribution and interconnection of digital infrastructures continue to reflect geographical logics. The originality of this approach lies exactly in the integration of historical,

spatial, and topological dimensions within a single analytical framework. Rather than offering static or descriptive accounts, it aims to render visible – and, to a certain extent, empirically measurable – the ways in which the architecture of cyberspace is shaped by material geography, territorial constraints, and infrastructural legacies. While avoiding deterministic conclusions, the analysis seeks to provide a systematic investigation of how geographic factors continue to condition the organization of cyberspace – an aspect that is increasingly discussed in recent debates on digital geopolitics (see for instance Deruda 2024; Suffia 2018), but still relatively underexplored through the systematic use of spatial methodologies.

The Geo-politics of Submarine Cables

Submarine data cables represent one of the most indispensable yet least visible infrastructures of the digital age. As discussed in the previous sections, the quasi-totality of global data traffic relies on this vast undersea network, which enables transoceanic digital communication across continents. These cables transmit the full spectrum of digital communications essential to the functioning of modern societies – including financial transactions, interbank transfers, corporate data flows, cloud services, voice communications, streaming media, and the operational traffic of critical public and private institutions. Their uninterrupted functioning is thus vital not only for individual connectivity, but for the stability of global markets, logistical chains, and national security infrastructures (as discussed more in depth in Landoni 2020).

As of early 2025, TeleGeography (2025) – a leading telecommunications market research and consulting firm that constantly provides data and analysis on global internet infrastructure – tracks nearly 600 active submarine cable systems, with a total of approximately 1,712 landing stations worldwide. When including both active and planned systems, the total exceeds 600 cables, covering a staggering 1.48 million kilometres of optical fibre deployed beneath the oceans. These lengths vary significantly – from the relatively short 230-km Italy-Croatia cable connecting Mestre in Italy and Umag in Croatia to the nearly 20,000km Asia-America Gateway system, which bridges the two continents across a single route. The physical scale of this network positions submarine cables among the most extensive infrastructures ever realized by humanity, reflecting the enormous material commitment needed to sustain global data flows. Beyond their scale, submarine cable systems are characterized by increasingly complex ownership and governance dynamics. Historically dominated by consortia of telecommunication operators, often including state-backed entities, the sector has undergone a significant transformation with the entry of global technology firms. In particular, companies such as Google, Meta, Microsoft, and Amazon have become major investors in, and operators of, new cable systems driven by the need to support ever-expanding cloud services, content

delivery networks, and data-intensive applications. A parallel trend is observable in China, where leading firms such as Huawei Marine Networks and China Telecom are closely integrated into state-led strategies for digital expansion. What emerges is a competitive landscape in which private actors are increasingly aligned with national strategic priorities. The United States and China, in particular, appear to be consolidating distinct spheres of influence through their respective corporate ecosystems, using cable infrastructure as a means of projecting digital presence and securing critical communication pathways. This alignment blurs the boundary between commercial investment and geopolitical strategy, transforming undersea cables not merely a technical asset but also a vector of international rivalry and infrastructural diplomacy (Balestrieri and Balestrieri 2019, 2024).

It is worth briefly considering the technical procedures involved in the deployment of submarine cables, in order to better grasp the scale, complexity, and strategic implications of these operations. The laying of submarine cables is carried out by highly specialised vessels known as cable-laying ships. These are large-scale maritime platforms specifically designed to transport and install optical fibre cables along pre-defined routes on the seabed. Equipped with massive spools capable of carrying tens or even hundreds of kilometres of cable, these ships rely on advanced navigational systems, satellite guidance, bathymetric survey instruments, submersible drones, and sonar technologies to ensure the accurate placement and protection of the cable infrastructure. Their number is limited: globally, there are approximately seventy cable-laying ships currently in operation owned by only 20 operators, but fewer than half possess the technical specifications required for complex deep-sea deployments. Their availability is therefore constrained, and their operation constitutes a non-negligible strategic resource, especially in crisis scenarios or during urgent repair interventions. It is not coincidental that China has recently invested heavily in this domain, developing some of the most advanced vessels of this kind in the world (for a more in-depth discussion on this see Deruda 2024, 26-31). The deployment process begins with a detailed definition of the optimal route, taking into account topographic, environmental, and geopolitical constraints. In near-shore segments, where cables are more vulnerable to anthropogenic threats such as fishing, anchoring, or deliberate physical tampering, they are typically buried beneath the seabed using ploughing or trenching equipment, which covers them with sediment for added protection. In deeper waters, instead, burial is generally not necessary: cables are laid directly on the ocean floor, where the depth of the water provides natural protection against both accidental damage and intentional interference. In fact, in deep-sea environments the technological and operational requirements for accessing them – whether to sever or to tap the data they carry – are considerable. Intercepting data transmissions typically involves advanced capabilities such as submarines, remotely operated vehicles (ROVs), or specialised underwater tapping devices, and may go undetected without sophisticated monitoring systems (Lehto

2019, 19). Conversely, in shallow waters, such as the Baltic Sea, limited depth renders cables significantly more exposed to human threats. In these contexts, intentional tapping or sabotage can be conducted with relatively unsophisticated means, raising serious security concerns (See Lehto 2019 on the specific case of the Artic Connect Project). Once the marine section of the cable is laid, it reaches a designated landing point on the coast, where it is brought ashore and connected to a cable landing station. From there, it is integrated into terrestrial networks, ensuring the continuation of data transmission between continents. The entire process, from deployment to integration, underscores the strategic, technical, and security complexity of submarine cable systems, and the extent to which global digital interconnection depends on their secure and uninterrupted functioning. All of this serves as a reminder that the infrastructure underpinning the digital space is in fact deeply material and inextricably rooted in geography. Its deployment depends on the physical contours of the ocean floor, the sediment composition of the seabed, and the accessibility of coastal areas. Yet geography does not only shape where cables can be laid but, as we saw, it also influences how secure they are. Submarine cables running through shallow waters or heavily trafficked maritime zones face higher exposure to accidental damage or deliberate interference, while those routed across deeper, less accessible oceanic basins benefit from a degree of natural insulation.

Despite their fundamental role in sustaining contemporary economies, governmental functions, and everyday digital practices, these infrastructures have long remained peripheral in public awareness and scholarly research alike (Bueger and Liebetrau 2021). While popular imagination tends to associate digital connectivity with wireless technologies and satellites, the physical backbone of the internet lies, quite literally, on the ocean floor.

This apparent invisibility stands in stark contrast to the growing strategic relevance of submarine cables in the context of global power competition. In recent years, geopolitical tensions have increasingly centred on the control, security, and governance of critical digital infrastructures, with submarine cables emerging as a key site of attention. Major global actors – including state powers such as the United States, China, and Russia, as well as large technology firms – have begun to view, as discussed in the first chapter, these infrastructures not only as a technical asset, but as a strategic domain in its own right. Thus, cables have been integrated into broader security concerns, infrastructural rivalries, and geopolitical alignments. They have become, in effect, critical terrain in the digital geopolitics of the 21st century (Hillmann 2021; Sunak 2017).

Yet, despite this shift, a significant gap persists in both academic literature and policy discourse. Compared to other domains of security and infrastructure, submarine cables remain relatively understudied – particularly in relation to their spatial distribution, historical evolution, and

geopolitical implications. In recent years, however, fiber-optic submarine cables have periodically come to the forefront of public and strategic attention. Heightened geopolitical tensions have led to targeted attacks and operational disruptions involving these systems – most notably in the Red Sea, where Houthi forces have damaged undersea cables and complicated repair operations (Solon & Hatem, 2024); in the Baltic Sea, where incidents of suspected sabotage have triggered heightened security concerns (Besch & Brown, 2024); and in the South China Sea, where rising instability has amplified fears surrounding the safety of maritime infrastructure (Kuo, 2025). While such episodes have drawn renewed attention to the vulnerability and strategic centrality of undersea networks, this visibility has often proved episodic and short-lived, failing to translate into sustained engagement at the level of public policy or strategic planning.

As Bueger and Liebetrau (2011) argue in their article, the persistent neglect of submarine cables can be partially explained by what they term the "triple invisibility" of this infrastructure. The first form of invisibility is, they say, a general characteristic of infrastructures themselves. As Edwards (2003, 185) has noted, infrastructures such as roads, sewer systems, or buildings tend to recede into the background of everyday life and become «naturalised» – despite the fact that they serve as the «connective tissues and circulatory systems of modernity». Their embeddedness in broader technical and social systems makes them them largely invisible, routinely taken for granted and rarely questioned (Blok et al. 2016; Bowker and Star 1999). In the case of submarine cables, this "standard" condition of infrastructure is further intensified. Unlike other infrastructures that are physically visible, publicly contested, or part of daily experience such as roads or bridges, submarine cables lie beneath the seabed and are constructed in ways that cause minimal disruption or public awareness (Starosielski, 2015). Their lack of physical presence contributes, the two scholars argue, to a second layer of invisibility that is specific to their material and technical characteristics.

Finally, the third dimension of this invisibility stems from their maritime location. Not only are cables situated under the surface, but they are also located in a space – the oceans and the seas – that is itself often treated in policy discourse as an empty or unregulated void. Some scholars have described this condition as "sea blindness", referring to the persistent neglect of the ocean as a site of human activity and geopolitical relevance (Steinberg 2001). Maritime infrastructures thus operate in spaces that are poorly governed and under-monitored, and where vulnerabilities have only recently begun to appear on security agendas (Bueger & Edmunds, 2017).

While these forms of invisibility offer a compelling explanation for the limited attention cables have received, their marginal status within security studies remains puzzling – particularly in light of their strategic and economic significance. The centrality of submarine cables to contemporary economies,

global communications, and public life would suggest a higher degree of scrutiny. This is especially striking given how other domains of cyber infrastructure have attracted sustained attention following the Snowden disclosures, the rise of tech giants, and intensifying geopolitical rivalries between the United States and China. Nevertheless, a growing – even if still fragmented – body of literature has begun to examine the cable infrastructure more systematically (Morel 2021; McGeachy 2022; Deruda 2024). Certainly, the work of Starosielski (2015) has been pivotal in bringing attention to submarine cable infrastructures. Her anthropological study of fibre-optic networks helped introduce the topic to media studies, geography, and the social and cultural analysis of infrastructure – even if it did not immediately generate a sustained wave of research across these disciplines. Building on these foundations, the following sections will reconstruct the history, technological development, and security challenges associated with these infrastructures, while maintaining a consistent focus on the different ways in which space, geography, and politics have shaped – and continue to shape albeit sometimes for different reasons – their organization and strategic relevance.

The Early History of Submarine Cables and the British Empire

While fibre-optic submarine cables are a relatively recent technological development, undersea communications themselves are not. The first international submarine cable, a copper telegraph line, was laid across the English Channel between Dover and Calais in 1850. Just eight years later, in 1858, the first transatlantic cable connected the United Kingdom and the United States. Although this early attempt proved fragile and inefficient – transmitting a single character required over two minutes, and the entire message took seventeen hours to deliver – it nonetheless marked a major technological change. A more stable interoceanic connection was only achieved in 1866 with the work of the Atlantic Telegraph Company. The central technical challenge in these early projects was the insulation of cables against seawater. Whereas terrestrial telegraph lines required minimal protection due to air's low conductivity, marine environments demanded more robust solutions: British companies responded by developing advanced insulation techniques using *gutta-percha*, a natural latex derived from trees native to Southeast Asia, particularly Malaysia, over which they soon established commercial and logistical control. This innovation contributed to Britain's dominance in the global cable industry throughout the second half of the nineteenth century (See also Landoni 2020).

Importantly, submarine cables soon came to be perceived not only as technical innovation but also as a fundamental strategic asset. The perceived security of seabed infrastructure began to surpass that of terrestrial systems. As Paul Kennedy (1971) notes in his extremely detailed article on British imperial communications that imperial strategists were very much aware of the vulnerabilities associated with terrestrial telegraphy: cables that traversed multiple sovereign states could be intercepted, censored,

or severed with relative ease. This reasoning was explicitly articulated in a 1902 report – as cited by Kennedy (1971) – by the British *Inter-Departmental Committee on Cable Communication*, which observed:

> «The greater the number of states through which a land telegraph passes, the greater is the probability that one or more of them, at some supreme and critical moment, when telegraphic intercommunication between the United Kingdom and its dependencies or its allies is of the highest importance, may exercise its power of interrupting communication; and, unless we maintain our own more secure alternative routes, may thereby imperil our most serious interests, the safety of our dependencies, or even our existence as a nation.»

Submarine cables, by contrast, offered a more secure means of communication – provided they were routed through friendly or controlled territories and their landing points remained under national authority. As noted in a communication from the Colonial Defence Committee «The maintenance of submarine cable communications throughout the world in time of war is of the highest importance to the strategic and commercial interests of every portion of the British Empire» (as retrieved in Kennedy 1971).

This recognition of the vital role of secure communication channels contributed directly, Kennedy argues, to the decision to develop the All-Red Line, a vast and expensive network of submarine telegraph cables that connected the principal territories of the British Empire without transiting through third-party states. Designed to ensure uninterrupted imperial communications, particularly in times of conflict, the All-Red Line exemplified the strategic logic underpinning early cable infrastructure: global connectivity was not only a matter of technical innovation but a tool of geopolitical control and this infrastructure became what Alex Nalbach (2003, 76) refers to as the «hardware of the new imperialism». Indeed, it was precisely this infrastructure that rendered Britain's projection of power across the world's oceans more rigid and structured. While maritime space had traditionally been characterised by fluidity and mobility, the establishment of a cable network such as the All-Red Line introduced a form of infrastructural rigidity anchoring imperial communication and control to fixed nodes and routes beneath the sea.

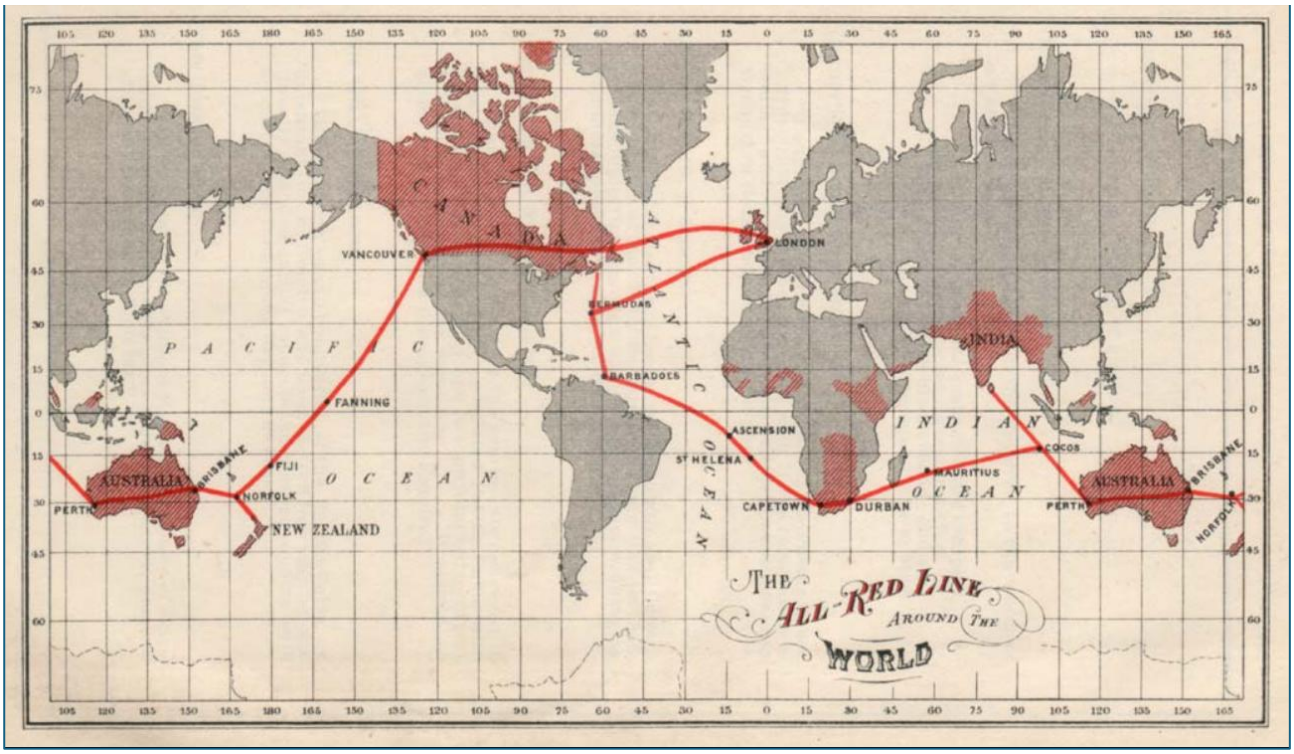

Figure 1 - Sketch map of the All Red Line drawn in 1902

This historical testimony reveals how the British Empire had come to regard control over submarine cable networks not simply as a matter of technological progress, but as a condition for imperial governance and military readiness. A widely developed and secure system of undersea cables was seen as essential to the coherence and resilience of imperial communications – an assumption that would echo, albeit under different guises, in the geopolitical logics of the digital age.

As Starosielski (2015, 35) notes, at the beginning of the twentieth century, territorial security became an increasingly central rationale for the expansion of undersea cable networks. This logic was particularly evident in the planning of the first two transpacific cables. Until then, undersea cable traffic from Europe to Asia and Australia was channeled through Singapore – where the British Eastern Telegraph Company held a monopoly. This configuration, in fact, effectively preserved London's centrality within the global cable system and reinforced British control over intercontinental communications. British-based companies, understandably, resisted proposals for a transpacific route that would have decentralised the network and diluted their influence. Particularly interesting is to follow the development of the first transpacific submarine cable systems as it was shaped by a combination of different strategic, political, and commercial rationales. The justification for these routes rested largely on their ability to diversify global communications beyond the vulnerabilities of

existing Mediterranean and Asian routes, and to undermine monopolistic positions such as that of the, always British, Eastern Extension company.

The first establishment of the Pacific Cable Board was in 1902. The chosen route, which stretched from British Columbia to Fanning Island, Fiji, and Norfolk Island before bifurcating toward Australia and New Zealand, was intentionally designed to traverse only British imperial territory. This geographical constraint was not the result of technical optimization but, as said, of a political imperative: with the aim to insulate the cable from foreign interference by maintaining its entire length within sovereign imperial control. This strategy of imperial insulation, however, came with trade-offs. The strict adherence to British-controlled landing points often meant bypassing more efficient or better-connected locations. The case of Fanning Island illustrates these tensions: although selected precisely because of its status as British territory, its limited infrastructure and the withdrawal of regular shipping services in 1911 left the station dependent on American commercial routes for basic logistical support, an ironic outcome for a network designed to avoid foreign reliance (Starosielski 2015, 37). Despite these contradictions, the system was still perceived as secure, underscoring the primacy of territorial sovereignty over infrastructural efficiency in early twentieth-century cable geopolitics.

However, a parallel development occurred in the United States, where growing imperial ambitions in the Pacific prompted calls for a transpacific cable to be operated entirely under American control (Squier, 1900). By the end of the nineteenth century, following the "closure of the American internal frontier" (for an in depth study of the role of the closure of the frontier in American internationalism see: Stefanachi 2017), the United States, driven by both economic imperatives and geopolitical considerations, moved decisively to break from the isolationism that had characterized much of its nineteenth-century posture. In seeking to project power beyond its continental borders, Washington turned its attention to the Pacific Ocean, which was increasingly imagined as the natural extension of the Western frontier. As had been the case for the British Empire a few decades earlier, secure and direct lines of communication with overseas territories became essential to sustaining imperial ambitions. Submarine cables thus emerged as critical instruments in the United States' external expansion, linking its Pacific possessions and newly acquired territories into an integrated strategic space. American policymakers and strategists framed the establishment of a transpacific cable as a matter of national necessity, initially envisioning it as a state-led endeavour in which the manufacture, deployment, and operation of the system would remain entirely under U.S. control.

The resulting project was that of the Commercial Pacific Cable, linking San Francisco with Hawaii, Midway Island, Guam, Japan, and the Philippines, and was similarly driven by the strategic logic of

national self-sufficiency and influence projection. Rather than aiming to connect underserved areas, these routes sought to consolidate control over already strategic nodes, reinforcing both commercial reach and geopolitical presence. This way, submarine cables became not only conduits for communication, but also spatial technologies of empire, inscribing territorial claims and securing influence across oceanic space. This phase marks a symbolic yet significant shift in infrastructural centrality from the United Kingdom to the United States – an evolution that, as is well known, would not be confined to submarine cables alone. The transpacific cable projects not only repositioned North America as a key node in global communication networks, but also exemplified how cable deployment was governed by deeply geostrategic logics. Decisions about routing were never purely technical or economic: rather, they were shaped by geographical constraints, access to critical raw materials, and, above all, by the imperative to secure sovereign control over the infrastructure of communication. As these early transoceanic systems reveal, the construction of global connectivity has always entailed a material geography of power, embedding political interests into the seabed and coastal territories that host and sustain the cable network.

Particularly interesting for the objectives of this work is to note how the Colonial Defence committee imagined British cable strategy. By the final years of the nineteenth century, it had developed an increasingly systematic approach to securing imperial cable communications in the event of conflict. In its 1898 report, the Committee – we read in Kennedy's work (1971) – concluded that Britain «ought to cut an enemy's cables wherever necessary for strategic purposes» – a doctrine that subsequently guided the identification of precise operational plans to isolate hostile state powers. A key strategic principle lay in territorial control: «where one end of a foreign cable is landed on British territory it would not be necessary to cut it, as the control would remain in our hands». On this basis, the Committee maintained an updated inventory of both British and foreign submarine cables, detailing all alternative routes and calculating the minimum number of severance operations required to isolate each country under different wartime scenarios. France – then considered the most likely adversary – was identified as the principal target: its seven cables to North Africa, as well as those to Corsica, the West Indies, and the Pacific, were all listed for disruption. In many of its colonial holdings – such as Madagascar, Djibouti, and French Congo – communications relied entirely on British infrastructure, making them particularly vulnerable. Not all states, however, were equally susceptible to cable cutting. Russia was considered largely immune to this tactic due to its geographical position and structure, in fact Russia's cable communications relied mainly on continental landlines and on a few submarine cables routed through neutral countries, such as Denmark. Only in the event of a Franco-Russian alliance would it have been possible to attack that submarine cable that connected Russia and France operated by the Danish Great Northern Telegraph Company. These constraints

highlight the enduring role of geography in shaping strategic calculations: underwater infrastructure, while extensive, was not uniformly vulnerable, and cutting operations had to account for geographical limits.

A particularly emblematic episode that underscores both the vulnerabilities and strategic advantages of cable physical control was the interception of the so-called Zimmermann Telegram in January 1917. Sent from the German Foreign Office to the German ambassador in Mexico, the message passed – perhaps imprudently – via a transatlantic cable operated by the British Eastern Telegraph Company. Though Germany believed it could transmit through the United States as a neutral intermediary, British intelligence at the cryptographic unit Room 40 successfully intercepted and decrypted the message (Finn 2017). Its contents, proposing a military alliance between Germany and Mexico against the United States, played a crucial role in shifting American public opinion and hastening the U.S. entry into the First World War. This episode illustrates how control over cable infrastructure, both physical and informational, could decisively shape geopolitical outcomes, further justifying the strategic doctrine long advocated by the Colonial Defence Committee.

Considered together, these elements show how the submarine cable infrastructure, even at its beginning, in the age of the British empire, was not merely a vehicle for communication, but a cornerstone of geopolitical strategy. Far from being neutral technical systems, early undersea networks were embedded within territorial logics, commercial monopolies, and military planning. The British and American examples demonstrate how control over cable routes, landing points, and maintenance capacity was integral to sustaining imperial power across vast oceanic distances. In this context, not only the sea but also the seabed emerged as a domain of strategic importance, inscribed with hierarchies of control and vulnerability, and monitored through detailed wartime contingency planning. Importantly, geography was not a passive backdrop but a determining factor in shaping both the opportunities and constraints of cable deployment, possibility for attack and defense. The physical location of landing points, the depth of the seabed, the proximity to rival powers, and the alignment of territorial possessions all contributed to the relative security or exposure of different segments of the network. As the interception of the Zimmermann Telegram further showed, control over both the material and informational dimensions of cable systems, often made possible by geographical positioning and political control of the company that operated the infrastructure, could decisively shape the course of international conflict.

A New Perspective: The Coaxial Cabels and The Cold War

If early submarine cable systems were deeply embedded within imperial territorialities and strategic calculations of the late nineteenth and early twentieth centuries, the mid-twentieth century ushered in

a distinct infrastructural and geopolitical regime. This shift was marked not only by the collapse of formal colonial empires, but also by the emergence of new technological capacities in telecommunications and security concerns shaped by the Cold War. A central turning point in this regard was the introduction of coaxial submarine cable systems, which – unlike their telegraphic predecessors – enabled high-capacity transmission of telephone calls, telex signals, and visual data across vast oceanic distances (Martinage 2015). Developed initially in the 1930s but actually used only after the invention of the submersible repeater in the 1940s, these new systems expanded the material and functional horizons of submarine communication. Starosielski (2015, 71) in her book maintains that technologically, coaxial cables signaled a radical departure. Whereas earlier networks had been limited by the physical properties of copper wire and the attenuation of telegraphic pulses, the deployment of repeaters on the ocean floor allowed continuous signal amplification, making transoceanic voice communication both feasible and commercially viable. The first of these systems was laid in 1950 between Florida and Cuba, and then the more ambitious Transatlantic No. 1 (TAT-1) linking Scotland and Newfoundland was laid in 1956. These infrastructures required a comprehensive reorganization of the cable industry: ships had to be redesigned, repeater stations constructed, and new insulating materials – most notably polythene – introduced in place of gutta-percha, effectively decoupling the industry from previous colonial supply chains in Southeast Asia. Yet this transformation was not only technical.

The geopolitical logics underpinning coaxial cable systems reflected the restructuring of global power after World War II. The collapse of European empires, the nationalisation of telecommunications carriers, and the strategic imperatives of U.S. military and intelligence agencies gave rise to a new political economy of cable infrastructure. In place of the imperial model – centred on exclusive control and territorial insulation – emerged a more decentralised and collaborative architecture, characterised by multinational «club» or consortium (Starosielski 2015, 77) arrangements. Within this system, cable construction and management were undertaken collectively by state-aligned companies, such as AT&T in the United States, KDD in Japan, and the General Post Office in the United Kingdom, which coordinated landing rights, route planning, and revenue distribution. While such arrangements introduced a degree of institutional pluralism, access remained tightly controlled and often conditioned and subordinated by political Cold War alliances and strategic alignments.

The geographies of this new infrastructure continued to reflect security imperatives, though reconceived in light of nuclear anxieties and the growing importance of redundancy (See Vanderbilt 2010). Cable landing sites were increasingly located in peripheral or rural zones, less exposed to enemy strikes or dense marine traffic, and coaxial routes deliberately avoided politically unstable or contested regions. As in the age of empire, the undersea environment remained a space of insulation

and strategic control, but the logics of that control had shifted: from colonial territorial sovereignty to infrastructural dispersion, from territorial exclusivity to multilateral coordination among allied states. Moreover, the Cold War cemented the perception of submarine cables as more secure than both radio and satellite links, reinforcing their centrality in military communications systems, including those used during the Vietnam War.

For these reasons, we can argue that the transition from telegraphic to coaxial cable infrastructure marked more than a technical upgrade: it represented a reconfiguration of how states imagined and enacted global connectivity. The ocean floor, once a medium of imperial command, now served as a platform for competing national interests within an increasingly integrated but carefully partitioned network. This evolution paved the way for the next major transformation in submarine communications – the development and global expansion of fibre-optic technology.

The Nineties: The Fiber Optic and The Liberal Market

The introduction of fibre-optic submarine cables in the late 1980s and early 1990s marked a second decisive technological break in the history of undersea communications. By encoding information as light pulses transmitted through strands of glass, fibre-optic systems offered exponentially greater transmission capacity, lower latency, and higher signal integrity than their coaxial predecessors. This innovation enabled the acceleration of global data flows and supported the emerging architecture of the Internet as we know it today. However, while the technical characteristics of fibre-optic cables represented a clear discontinuity, at the beginning, the geographical and organisational frameworks into which they were initially inserted bore the imprint of earlier systems. In many respects, the network's spatial logics evolved through inertia (on this the main reference is Starosielski 2015, 81-94): Cold War-era decentralisation strategies, colonial-era territorial imperatives, and long-standing infrastructural corridors were not immediately displaced but rather repurposed and reproduced in new technological forms. Indeed, the early fibre-optic systems were largely conservative in their deployment. Projects such as Trans-Pacific Cable 3 (TPC-3), completed in 1989, and PacRim (1993), the first fibre-optic cable in the South Pacific, closely followed the routes of prior coaxial and even telegraph cables. This continuity reflected both the perceived reliability of existing paths and the entrenched institutional practices of the cable industry, which had long been governed by a logic of stability and risk aversion, with the sole main intent to reinforce and add capacity to existing communications. Even when new landing points were considered – such as in the case of the Australia-Japan cable in 2001 (Starosielski 82) – technical and logistical difficulties often led companies to revert to known configurations.

However, the fibre-optic-era was not simply a case of technological enhancement within an old spatial framework. It coincided with profound shifts in the political economy of global telecommunications, which collectively redefined how cables were planned, financed, and deployed. The liberalization and privatization of telecom markets – already discussed in the first chapter of this work – undermined the postwar "club system" of state-aligned telecommunications providers. What had once been a field dominated by public utilities operating within intergovernmental consortia became increasingly subject to market logics, speculative investment, and financial risk-taking. In this context, the 1990s saw the rapid proliferation of private cable systems developed outside the traditional consortium model. New actors often venture-backed firms with little prior experience in cable engineering, entered the field, competing with legacy providers and introducing more flexible, market-driven approaches to cable planning. See for instance projects such as FLAG (Fiber-Optic Link Around the Globe, 1997) and the Southern Cross Cable Network (2000) exemplify this shift. These ventures often selected routes and landing points based not on long-term strategic considerations, but on immediate financial viability and commercial logic. In some cases, this led to the creation of redundant routes or to a concentration of infrastructure in certain high-demand corridors, thereby producing new forms of unevenness and vulnerability. This transition was not merely infrastructural, it was also deeply ideological. The end of the Cold War fostered – the long discussed here – liberal optimism that tended to downplay the strategic dimensions of global telecommunications. In policy and business discourse, undersea cables came to be seen less as instruments of geopolitical power and more as conduits of global economic integration and digital modernity. Security logics that had once structured cable planning were either sidelined or reinterpreted in market-friendly terms. Although some practices, such as route redundancy, persisted due to a sort of "path dependency", their underlying rationales were increasingly reframed through the lens of market efficiency, cost optimisation, and investor appeal. As Starosielski (2015, 88) notes, the industry shifted from a strategic to a speculative rationale, with network planners responding more to projected demand curves and risk assessments than to territorial or military considerations.

The physical geography of cable networks also reflected these new imperatives. The fibre-optic boom of the 1990s led to the construction of thousands of kilometres of new cable each year. Yet, rather than diversifying global infrastructure in a balanced way, much of this expansion reinforced existing hierarchies and centre-periphery dynamics. Cables continued to land in a relatively small number of hubs, creating dense clusters of connectivity while leaving other regions underserved. In some instances, competition among private actors resulted in the duplication of capacity along similar routes, contributing to overinvestment and, ultimately, financial collapse. As one engineer interviewed by Starosielki (2015, 93) wryly observed: «five or six companies all guaranteed they'd

get 100 percent of the traffic», leading many to bankruptcy when they only captured a fraction of the expected flows. This speculative fervour culminated then in the early 2000s cable bust, during which major firms such as Global Crossing, WorldCom, and 360Networks collapsed under the weight of unsustainable debt. The crash revealed the limits of a purely market-driven to global infrastructure inherent to market speculation. Following the crisis, some elements of the consortium model were reintroduced, and a hybrid system emerged, combining state-aligned and private investments.

The market failures that characterized the fibre-optic cable boom of the 1990s – overcapacity, speculative investment, and infrastructural redundancy – were not only the result of technological optimism and deregulated planning, but also the product of a broader political moment. These dynamics mirrored the liberal euphoria of the immediate post-Cold War period, during which the primacy of the market was presumed to offer a stable and efficient substitute for the strategic coordination formerly exercised by states. However, just as in the domain of cybersecurity, where the early 2000s saw a growing awareness of the strategic vulnerabilities embedded in digital interdependence, so too in the field of infrastructure policy we observe the gradual return of the state. As the illusion of a self-regulating global network faded, infrastructure, long treated as a technical and commercial matter became progressively re-politicized and securitized. This shift did not occur abruptly, but paralleled the transformation of international order from unipolar liberal optimism to multipolar competition and structural insecurity of the West (see chapter I). The same infrastructures once imagined as the vectors of globalization and openness began to be reframed as potential targets of disruption, and thus as critical national assets requiring protection. Strategic planning, state oversight, and security doctrines *re-emerged* in response to the perceived fragility of cable systems, their geographic exposure, and their centrality to both economic functioning and military coordination. What emerged, in other words, was a partial reversal of the previous logic: if during the 1990s the state receded in favour of private actors and market coordination, the early 21st century saw its re-entry – not as an opponent of the market, but as a necessary guarantor of infrastructure security. This dual movement of liberalization and re-securitization reflects a deeper structural tension that characterizes the geo-politics of interconnection in the post-unipolar world: infrastructures are simultaneously shaped by the incentives of private capital and the imperatives of national strategy. And just as cybersecurity evolved from an initially techno-optimistic discourse to a logic of risk management and resilience, undersea cable governance increasingly mirrored this transformation, blending commercial rationality with renewed forms of infrastructural geopolitics.

The Return of Strategy

A striking indication of the renewed strategic importance attributed to submarine infrastructure in the current geopolitical context is found in recent publications by the prestigious *U.S. Naval Institute*, which explicitly revisit the strategic vision of the British Empire's telegraphic system as a blueprint for contemporary maritime information warfare. Notably, works such as *To Secure Undersea Cables, Take Lessons from the British Empire's All-Red Line* by Burnett and Berdan (2024), and *Information Warfare in the Depths* by Long (2023), invoke the nineteenth-century logic of the All-Red Line as a historical precedent to guide U.S. strategy in the age of fiber optics and cloud computing. The analogy is far from incidental. Much like the British planners of the late Victorian era, today's American naval thinkers are concerned with how to ensure the operational resilience and territorial security of submarine cables in scenarios of inter-state competition and potential conflict. The British logic of "imperial insulation", and thus maintaining cable landings exclusively on British territory and under British control, reappears, *mutatis mutandis*, in calls for geographically diverse landings, allied redundancy, and enhanced repair capacity through publicly supported maritime assets such as the Cable Security Fleet (On this see also Deruda 2024, 35-39). The strategic rationale that shaped the All-Red Line, namely the idea that secure and sovereign cable infrastructure was a precondition for sustained global influence has resurfaced albeit in transformed political-economic conditions. Today's fiber-optic cables, connecting the data centers of major platform companies (Google, Meta, Amazon, Microsoft, Tencent), are not only commercial arteries but essential infrastructures of state capacity. Despite the privatized and ostensibly market-driven nature of current network construction, the growing acknowledgment of cable systems as critical national security assets reflects a broader reconfiguration of state-market relations in the context of great power rivalry, Burnett and Berdan argues (2024). As seen, the renewed strategic concern must be understood against the backdrop of the broader shift already described in the first chapter of this work: the transition from a liberal-universalist vision of global interconnectivity to a world shaped by insecurity, vulnerability, and systemic mistrust. After the Cold War, Western liberal thought embraced the idea that market forces and digital globalization would ensure long-term peace and prosperity. The internet and its infrastructure, of which submarine cables are a foundational layer, were imagined as enablers of openness, decentralization, and mutual interdependence. Yet, as that optimism unraveled, especially in the wake of growing cyber threats, geopolitical tensions, and asymmetric vulnerabilities, states have returned forcefully as actors of infrastructural securitization.

The liberal belief that connectivity would dilute power asymmetries has been replaced by an acknowledgment that such infrastructures consolidate influence at specific nodes – be they technical

(landing points, data centers) or political (regulatory regimes, commercial governance). Consequently, the securitization of submarine cable infrastructure has emerged not solely from technical vulnerabilities, but from a political shift in perception, in which connectivity itself is now seen as a potential liability as well as an instrument of power projection.

In this sense, the analogy with the British Empire's All-Red Line is more than a historical echo; it represents a strategic template whose geographical and political logics continue to inform today's thinking on submarine cable security. As Burnett and Berdan (2024) recall, the All-Red Line was conceived to guarantee "imperial insulation" by routing all critical connections through British-controlled landing points and ensuring that relay stations were staffed exclusively by British personnel. This approach rested on a double geographical rationale: political control over the sovereign territory hosting the landing stations, and a dispersion of routes that reduced the number of cuts required to isolate the network. These same principles, albeit in a transformed political world, re-emerge in contemporary calls for geographically diverse landings, redundancy through allied territories, and publicly supported repair capabilities such as the U.S. Cable Security Fleet. The continuity is not accidental: in both cases, geography was – *and remains* – integral to strategic resilience, determining not only the physical vulnerability of the network but also the extent to which it can be insulated from adversarial interference. Today, sovereignty over undersea cable systems is only apparently divided between state and market. While infrastructure is largely financed, owned, and operated by a handful of global platform companies (Google, Meta, Amazon, Microsoft) the U.S. strategic community increasingly treats these assets as extensions of state capacity, whose resilience and security are essential to maintaining operational autonomy in an era of systemic rivalry. This perception is sharpened by the assessment, detailed in Long (2023), that authoritarian powers are actively seeking to shape, exploit, or disrupt the global cable network. China's state-linked investments in cable construction and landing stations, including in allied territories, are viewed as part of a long-term strategy to embed influence and create technological dependencies. Russia, for its part, has been identified by U.S. intelligence as pursuing both physical seabed operations, such as deploying specialized vessels like the *Yantar* capable of tapping or severing cables, and cyber-enabled techniques to manipulate or intercept data flows, with particular attention to critical chokepoints near NATO territories.

Such concerns are inseparable from the broader geopolitical shift described in the first chapter: the erosion of the post-Cold War liberal assumption that global connectivity would naturally dilute power asymmetries and foster stability. Instead, fiber optic cables, celebrated in the nineties as neutral enablers of global commerce, are increasingly framed as contested strategic terrain. The political

economy of control has changed: whereas the British Empire could integrate imperial authority with subsidized private companies like the Eastern Telegraph Company, today authority is fragmented across states, corporations, and international regimes. Yet, as the U.S. naval discourse shows, this fragmentation does not diminish the centrality of the state; rather, it compels new forms of state-corporate alignment in the name of security both in authoritarian and in democratic states naturally. A telling example is the 2020 decision by the U.S. interagency Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector ("Team Telecom") to recommend denying the Pacific Light Cable Network's proposed direct connection between the United States and Hong Kong. Although the project promised significant commercial benefits, the Committee concluded that the link would expose U.S. traffic to interception by the PRC, citing both the ownership structure involving PRC-linked firms and the application of Chinese intelligence and cybersecurity laws. This reasoning closely echoes the British insistence that All-Red Line landing points remain on sovereign or controlled territory – mitigating adversary access by shaping the physical topology of global communications. The PLCN case demonstrates that, even in a privatized, market-oriented environment, state actors continue to assert strategic authority over undersea cable routes and landings as a core dimension of national security. In this context, the "imperial insulation" logic survives as a path dependency, reframed to address twenty-first-century threats but grounded in the same geographical insight that shaped the British network, meaning that the control over where cables land, and over how their routes traverse the oceans, remains decisive for sustaining both connectivity and strategic advantage.

In conclusion, the historical evolution of submarine cable systems, from the imperial telegraph networks of the late nineteenth century – epitomized by the British Empire's All-Red Line, to today's vast fibre-optic systems – provides strong evidence in support of the initial hypothesis advanced in this work: namely, that spatial-geographic factors fundamentally influence the capacity to control such infrastructures. This influence operates along two interrelated dimensions. First, political control over the territory hosting cable landing points determines the legal, military, and administrative capacity to secure and operate the network in times of crisis. Second, the spatial logic of cable deployment, namely its dispersion, redundancy, and avoidance of potentially hostile jurisdictions, affects its resilience and the ability to sustain uninterrupted communication flows. The British experience demonstrates that these principles are not circumstantial, but structural. The deliberate decision to land cables exclusively on British-controlled territory, to design geographically diverse routes, and to integrate maintenance capacity within imperial maritime assets constituted a coherent strategy of infrastructural sovereignty. Although the technological substrate has transformed – from copper telegraph lines to fiber-optic cables, and from imperial bureaucracies to transnational platform

companies – the strategic imperatives identified in the “age of empire” persist. Geography remains both a constraint and an instrument of power, shaping how communication infrastructures are built, governed, and defended.

The persistence of these spatial-strategic logics across different technological eras, political orders, and actors suggests that the control of submarine cable systems is inseparable from their geography. Far from being neutral artefacts of connectivity, these infrastructures have always been political technologies – embedded in strategies of global governance, influenced by material geography, and bound to the capacity of states to secure the physical and political spaces through which they pass. This continuity across time provides a robust empirical foundation for the hypothesis guiding this research and justifies its further examination through systematic, data-driven analysis.

The Distribution Pattern of Landing Stations and Submarine Cables

Building on the historical reconstruction of submarine cable infrastructure and the strategic logics underpinning its control, this section turns to the empirical examination of the current network’s geographical configuration. This analysis draws on the dataset and methodological framework described in the *Research Design* section, to which the reader is referred for detailed information on sources, coverage, and limitations. In brief, the submarine cable data (Greg’s cables, 2018) refer to a single temporal snapshot, which is the year 2018, and cover 265 systems, representing a substantial but incomplete portion of the estimated global total of approximately 570 cables (TeleGeography, 2025). While this temporal and coverage constraint inevitably limits the ability to capture the most recent expansion and modernization trends, the dataset remains in the author’s view sufficiently robust to allow for systematic spatial and network analysis. By integrating Geographic Information Systems (GIS) and network analysis techniques, the empirical approach adopted here enables a detailed examination of the spatial distribution, connectivity patterns, and topological relationships between critical infrastructure nodes. This dual methodology provides a more concrete and systematic perspective on the geography of the submarine cable network, complementing the historically grounded strategic analysis with quantifiable evidence. Although the quality and completeness of the dataset may influence the precision of the results, the application of these tools offers a valuable starting point for investigating the materiality and geopolitics of digital infrastructure, and for developing analytical frameworks that can be refined with more up-to-date and comprehensive data in future research.

Spatial Pattern of Landing Stations

To examine the spatial distribution of submarine cable landing stations, a Kernel Density Estimation (KDE) was applied using QGIS. This method transforms a set of discrete points, in this case landing stations, into a continuous surface that estimates the intensity of their spatial concentration. The algorithm assigns to each point a weighted influence within a defined radius – in this case 200 km – and produces a raster output in which areas with higher density are visually emphasized. In practical terms, KDE makes it possible to identify territorial clusters of landing stations, thereby moving beyond a simple point-based representation and highlighting the regions where infrastructural concentration is greatest. The results clearly show a highly uneven global geography of landing stations.

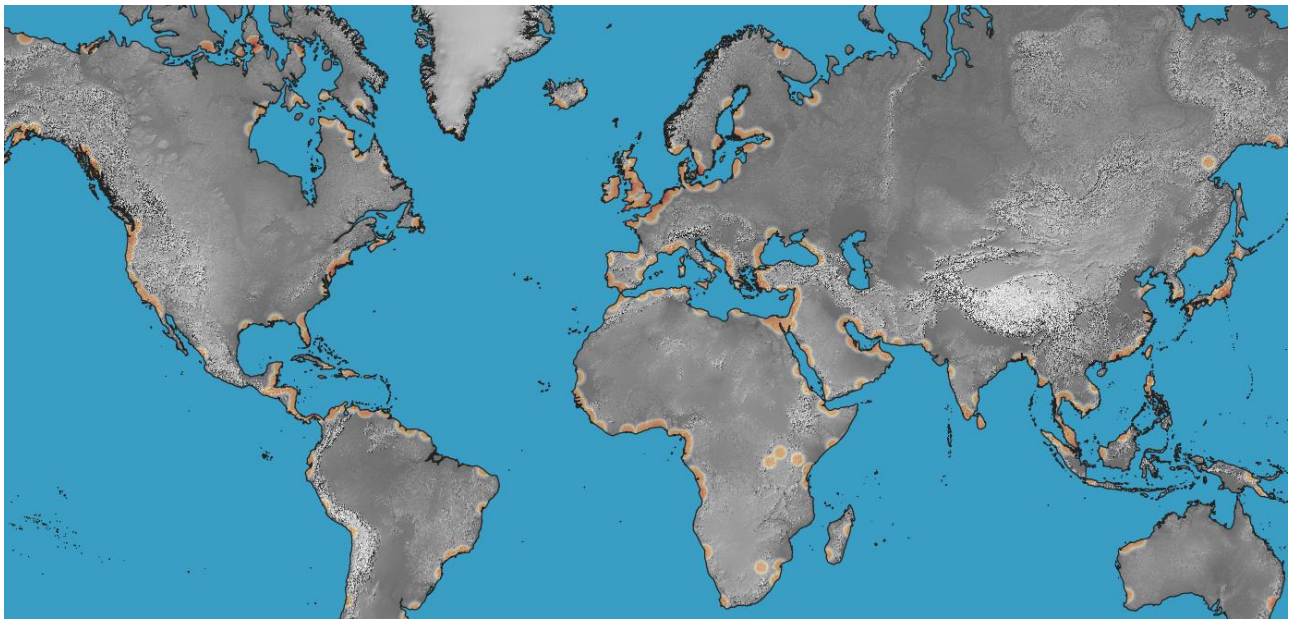

Figure 2 - Landing Stations Global Distribution Heatmap

At the global scale, the analysis demonstrates that landing stations are overwhelmingly concentrated in the Northern Hemisphere, with density hotspots emerging along the Eurasian rimland and the North American Atlantic seaboard. Northwestern Europe appears as the single most saturated region, with a dense network of stations stretching from the British Isles through the Benelux countries, northern France, and into Scandinavia. This reflects both the multiplicity of short national coastlines and the region's long-standing role as a hub in global telecommunications. Similarly, the northeastern United States, from Virginia to Massachusetts, exhibits a strong concentration of landing points, consolidating its position as a critical gateway between North America and Europe.

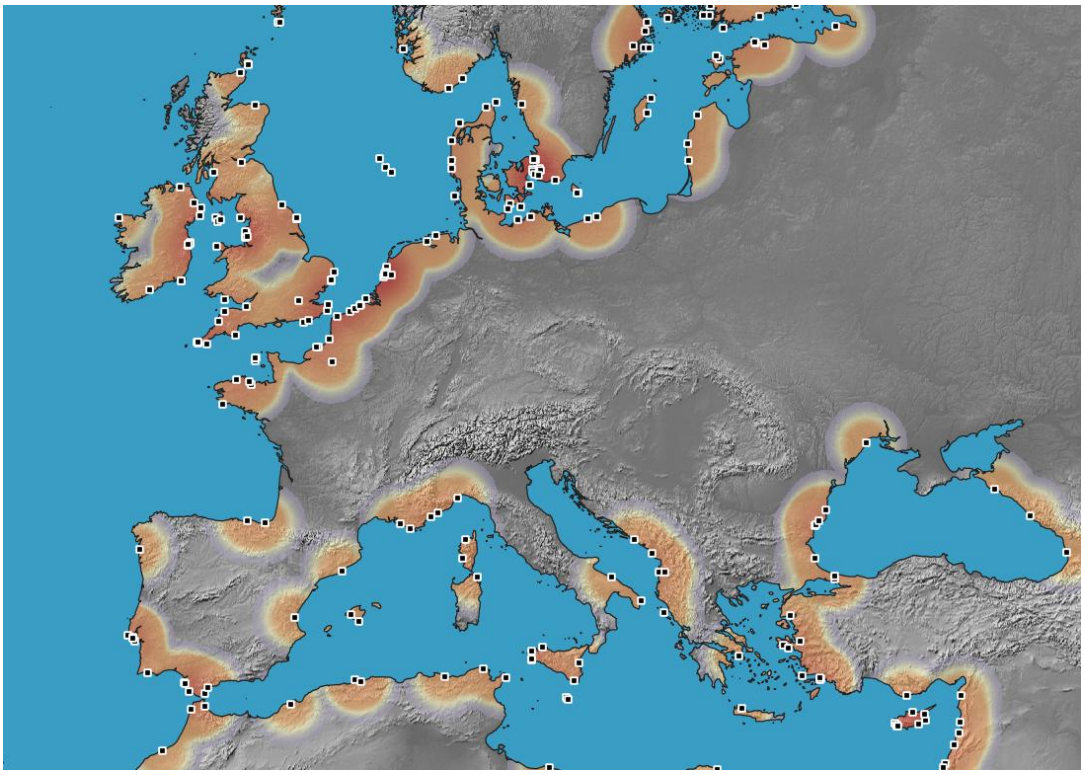

Figure 3 - Heatmap Landing Station Europe and the Mediterranean

Beyond these two core clusters, several additional dense regions emerge. In the Mediterranean basin, landing stations are distributed along the coasts of Spain, France, Italy, and Greece, with a notable concentration at the central and eastern Mediterranean choke points, such as Sicily and the Aegean archipelago and the proximity of the Suez Canal in Egypt. Further east, the Persian Gulf stands out as another strategic cluster, where small coastal states with limited territorial extent, such as the United Arab Emirates, Qatar, and Bahrain, host disproportionately high densities of landing facilities. In Southeast Asia, the Malay Archipelago exhibits dense concentrations, especially in Singapore and surrounding islands, where the fragmentation of the coastline and the need for regional interconnectivity amplify the infrastructural footprint. Other regions show sub-dense but still significant patterns. The southeastern coast of China hosts a string of stations extending from Hong Kong through Guangdong and Fujian, reflecting the country's integration into transpacific and regional networks. The western seaboard of North America similarly displays a continuous though less dense distribution, particularly in California. The Caribbean also emerges as an intermediate-density zone, where insular geography necessitates a high number of connections despite relatively smaller populations and economies.

In contrast, much of the southern hemisphere is characterized by sparse coverage. Along the African coastline, landing stations cluster in a limited number of nodes, particularly in North Africa, South Africa, and Nigeria, leaving vast stretches of coastline with little connectivity. South America follows a similar pattern, with dense points around Brazil but limited infrastructure along the Pacific coast. Oceania is marked by especially low densities, with Australia hosting relatively few stations compared to the length of its coastline, underscoring the infrastructural asymmetry between continental states with extended coastlines and insular or fragmented geographies. Finally, the Arctic Circle stands out as the only coastal region with almost no presence of landing stations, highlighting the physical and economic constraints of extreme latitudes.

Taken together, these patterns demonstrate how the geography of submarine cable landing stations reflects both physical and political-economic factors. Physically, the density of islands and fragmented coastlines such as in the Caribbean or the Malay Archipelago tends to generate clusters, while long, uninterrupted coastlines, as in Australia or India, correspond to sparse distributions. Politically and economically, the weight of advanced digital economies, such as those of the United States, the United Kingdom, or northern Europe more broadly, has resulted in disproportionately dense landing infrastructures. Thus, the spatial imprint of submarine cable landing stations embodies a combination of natural geography and geopolitical economy, reinforcing the central role of certain regions – particularly the Eurasian rimland and the North Atlantic corridor – in structuring the distribution of the physical entry point on land of the global cyberspace infrastructure.

Spatial Pattern of Submarine Cables

To analyse the distribution of submarine cables, a different methodological approach was required compared to landing stations. Since cables are represented as linear features rather than discrete points, the analysis first entailed generating a regular distribution of points along each cable segment. This transformation allowed the use of kernel density estimation (KDE), which operates on point data, to model the spatial intensity of submarine cable routes. So to generate a continuous surface where areas with overlapping or converging cables emerge as hotspots (in red). This procedure is particularly effective in visualising not only the geographical spread of the network but also the concentration of traffic corridors within global maritime space.

The resulting heatmap highlights several patterns of global significance. At the planetary scale, submarine cables do not follow a uniform distribution across the oceans but rather concentrate along a limited number of maritime corridors. The densest areas correspond to the transatlantic routes

connecting the eastern seaboard of North America with northwestern Europe, particularly between the United States, the United Kingdom, and France. This corridor constitutes the historical backbone of global telecommunications and continues to represent one of the most saturated infrastructures of cyberspace.

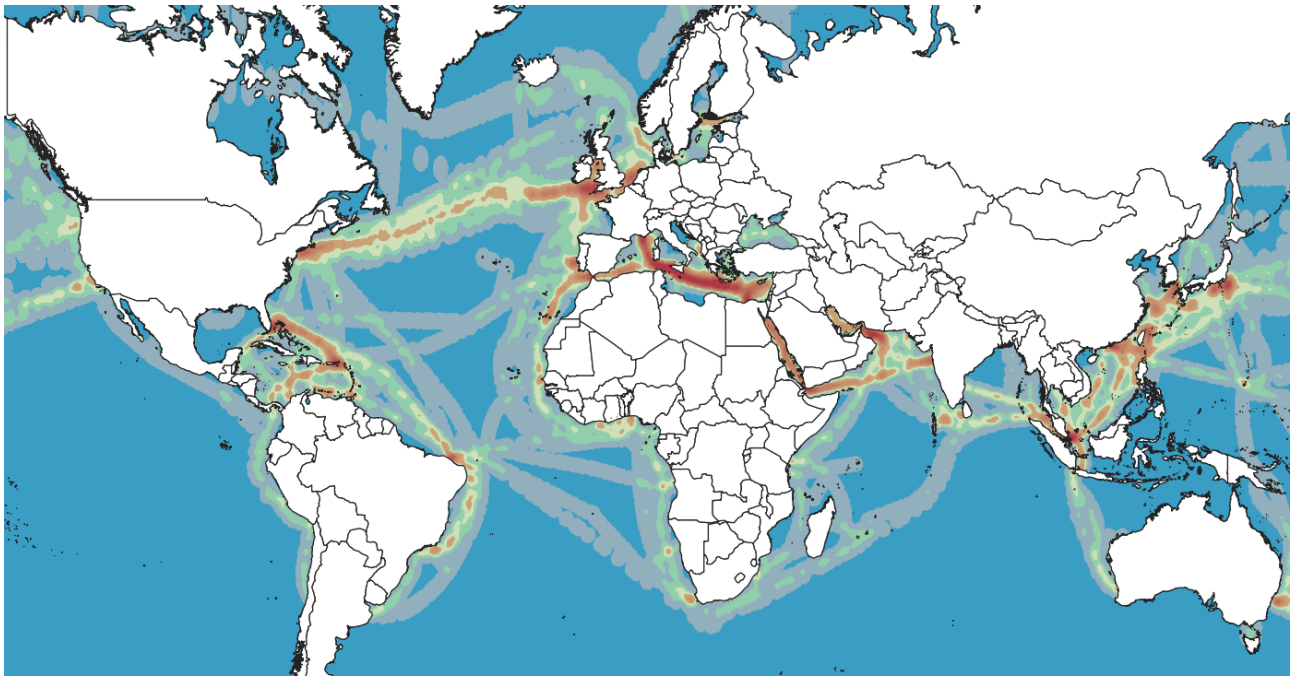

Figure 4 - Submarine Cables Global Hotspots

A second dense cluster is visible across the Mediterranean Sea, which emerges as a central hub linking Europe with North Africa, the Middle East, and further towards Asia. Within this basin, choke points such as the Strait of Gibraltar, Sicily, and the eastern Mediterranean near Cyprus and the Levantine coast show particularly intense concentrations, underlining the strategic nature of these geographies.

Further east, the Red Sea and the Arabian Sea form another critical axis, where cables converge along the Suez Canal and extend towards the Persian Gulf and the Indian Ocean. This region represents one of the few obligatory passages between Europe and Asia, producing very high levels of density. A similar intensity is visible in Southeast Asia, where cables cluster around Singapore, the Strait of Malacca, and the South China Sea. These areas, characterised by narrow maritime chokepoints and archipelagic geography, constitute indispensable junctions for the global system. The Pacific routes, while less dense than the transatlantic corridor, reveal strong concentrations between East Asia (notably Japan, China, and South Korea) and the western coast of North America, especially California. This corridor underlines the role of the Pacific Rim as a second pole of global connectivity. Other regions exhibit far lower densities. The South Atlantic is comparatively underdeveloped, with

a few routes connecting Brazil to Europe and Africa. Similarly, the coasts of Africa show limited densities except at a handful of landing points such as South Africa, Nigeria, and Egypt. Oceania, despite its long coastlines, has only sparse and peripheral connections, reflecting its marginal position in the global submarine cable system.

It is imperative to highlight that the spatial configuration of submarine cable routes closely mirrors the geography of global shipping lines. This convergence is not coincidental but rather the outcome of enduring geographical constraints and economic needs (for an overview see: Cerreti et al. 2019, 376-394). The oceans impose a limited set of navigable corridors, funnelling both trade and digital infrastructures through a few critical chokepoints. The Strait of Malacca, for example, has for more than two millennia served as the main passage between the Indian and Pacific Oceans, and it continues to concentrate a dense flow of both vessels and submarine cables. Similarly, the Suez Canal, the Gulf of Aden, and the Strait of Gibraltar are unavoidable crossings for Europe–Asia connections, while the Caribbean Basin and the Central American isthmus emerge as focal points in the Atlantic system. Economic and technical considerations reinforce this geographical determinism. Submarine cables represent costly investments, and their efficiency is constrained by both latency and vulnerability to disruption. Longer routes not only increase construction costs but also reduce transmission efficiency, which makes shortest-path routing across seas the primary option. This explains, for instance, why Europe–Asia connectivity does not follow the circumnavigation of Africa via the Cape of Good Hope, but rather cuts through the Mediterranean and Red Seas, paralleling millennia-old trade routes. In this sense, physical distance remains a decisive factor in the organisation of the digital network. Even though data travel at the speed of light, latency accumulates with distance, making shorter routes not only more economical but also more efficient in terms of transmission. As a result, the spatial configuration of submarine infrastructure demonstrates that the "virtual" space of cyberspace continues to be shaped by material geography and the enduring constraints of distance. To further illustrate this dynamic we could look at the potential opening of Arctic maritime passages: just as they may offer faster shipping alternatives, they also present possible new corridors for submarine cable deployment (Saunavaara and Salminen, 2020).

Overall, the analysis shows that the geography of submarine cables is shaped by both physical and geopolitical constraints. Physically, narrow maritime corridors and choke points appear as unavoidable convergence zones, concentrating a disproportionate share of the infrastructure. Geopolitically, the dominance of the North Atlantic and the Eurasian rimland reflects the historical centrality of Euro-American and East Asian economies in structuring the backbone of cyberspace. By

contrast, the Southern Hemisphere remains underrepresented, reinforcing the asymmetrical distribution of global connectivity.

The empirical analysis of the spatial distribution of submarine landing stations and cable routes makes it possible to test the second working hypothesis of this research: namely, that the submarine infrastructure of cyberspace is not distributed evenly across global coastlines, but is disproportionately concentrated in proximity to key maritime chokepoints and historically consolidated corridors of oceanic navigation. The results of the density analysis of landing stations confirm that cable landings cluster heavily in certain areas where geographical and infrastructural constraints converge: Northwestern Europe, the Mediterranean basin, the Persian Gulf, the Malay Archipelago, and the Northeastern seaboard of the United States stand out as privileged nodes. Similarly, the analysis of submarine cable lines, conducted through a kernel density estimation of points along the cable paths, demonstrates that the global topology of undersea infrastructure mirrors that of shipping routes. The same maritime chokepoints that structure centuries-old trade patterns, such as the Strait of Malacca, the Suez Canal, and the Strait of Gibraltar, also emerge as unavoidable corridors for digital connectivity. Taken together, these findings corroborate the hypothesis that maritime chokepoints and the broader morphology of oceanic geography exercise a decisive influence on the spatial configuration of cyberspace infrastructure. Far from being an immaterial or deterritorialized space, the global digital infrastructure reproduces and amplifies the logics of territorial chokepoints, embedding the vulnerabilities of maritime geography into the architecture of the internet itself.

The Network of the Fiber Optic Connectivity

The global fiber-optic submarine cable system cannot be understood merely as a neutral and technical assemblage of nodes and links enabling the circulation of data. Beyond its material function of transmitting flows, the network actively generates interactions, facilitates exchanges, and diffuses practices that profoundly shape societies, economies, and political orders worldwide (McNeill and McNeill 2003, 269). In this sense, submarine cables are not inert infrastructures but political technologies whose topology carries strategic implications. Within this framework, concepts of centrality and proximity acquire particular salience. The relative position of states and territories in the global cable network is not simply a matter of technical efficiency; it defines degrees of connectivity, exposure, and influence. Highly central actors function as indispensable hubs whose disruption would reverberate across multiple regions, while peripheral actors remain structurally dependent on a limited number of connections. Likewise, the clustering of ties between certain groups of countries signals not only geographical proximity but also technological integration, patterns of

dependence, and potential political alliances. To capture these structural properties, I transformed the spatial dataset of submarine cables and landing stations into a relational graph. In this graph, countries are treated as nodes, and submarine cables constitute the edges connecting them. The nominal cable capacity was used as a weight for the edges, enabling the differentiation between stronger and weaker ties. Since submarine cables function bidirectionally, the network was analyzed in its undirected form, which better reflects the reciprocal character of connectivity.

On this representation, a series of formal network measures were applied using the igraph library in R. First, degree centrality was computed to capture the number of direct links a country maintains, offering a straightforward measure of connectivity. Complementing this, strength was calculated as the weighted equivalent, indicating the cumulative capacity of a country's cable connections. To assess the role of actors as intermediaries, betweenness centrality was introduced: this measure quantifies the extent to which a node lies on the shortest paths connecting other nodes, thereby identifying critical transit hubs whose disruption would fragment connectivity across regions. Closeness centrality was also measured, expressing how close a node is to all others in the network in terms of path length; countries with high closeness are structurally positioned to reach all others with fewer intermediaries, enhancing their efficiency of communication. Finally, eigenvector centrality was employed to capture not just the number or strength of a node's connections, but also their quality: countries connected to other highly central actors score higher, reflecting their embeddedness in influential clusters of the network. Beyond these node-level indicators, the analysis also considered the meso-structure of the network, that is, the intermediate patterns of association that emerge when nodes form more densely connected subgroups. To identify such patterns, the Louvain algorithm for community detection was applied to the undirected network. This modularity-based method partitions the graph into clusters of countries that are more densely connected internally than with the rest of the network. The identification of these communities provides crucial insight into how submarine cable infrastructure reinforces regional integration, geopolitical alignments, or dependencies that may not be immediately visible on the global map. Finally, measures derived from Burt's structural hole theory were calculated, namely constraint and effective size. These indicators highlight countries that serve as brokers or bridges between otherwise weakly connected communities. A low constraint value indicates that a country connects otherwise disconnected clusters, granting it structural autonomy and strategic leverage. Conversely, actors with high constraint are embedded within tightly knit groups, limiting their brokerage capacity.

Taken together, this methodological framework integrates node-level centrality measures, community detection, and structural hole analysis. This allows for a systematic assessment of connectivity, hierarchy, and clustering within the submarine cable network. In this way, the analysis

moves beyond a descriptive mapping of cables and landing stations to interrogate the relational architecture of digital infrastructure, revealing how material geography and political influence are inscribed in the topology of global connectivity.

The Network

The visualization of the global submarine cable network shown above was generated using a force-directed layout algorithm - specifically, the Fruchterman-Reingold (Fruchterman & Reingold, 1991) implementation provided in igraph. This type of algorithm simulates the network as a physical system in which nodes repel each other like charged particles, while edges act as springs that draw connected nodes together. The result is a two-dimensional projection that tends to place densely interconnected clusters closer to the centre, while more peripheral or weakly connected nodes are pushed outward. In this representation, the size of the nodes is proportional to their degree centrality - the number of direct cable connections a state maintains. The United States clearly emerges as the most central node, positioned near the heart of the network and displayed at a much larger size than most other states. This reflects both its exceptionally high degree (number of distinct cable connections) and its high strength (weighted degree, accounting for cable capacity).

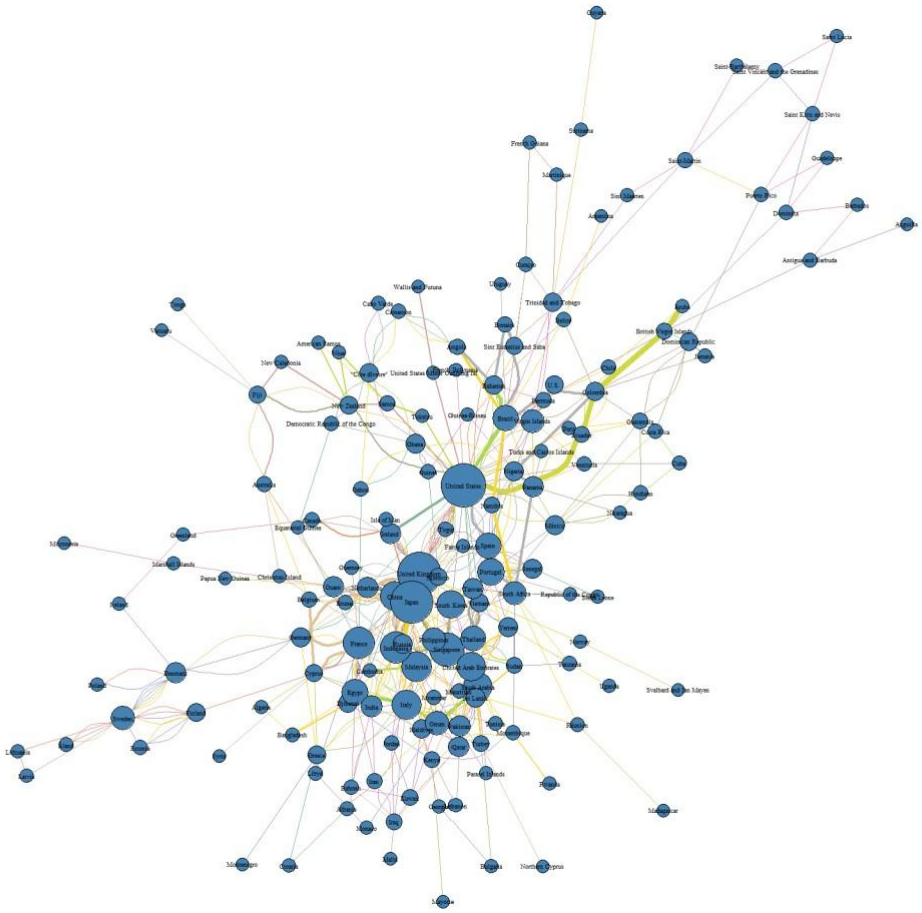

Figure 5 - Submarine Cables Network Graph

The prominence of the United States is consistent with its role as the principal transatlantic and transpacific hub, anchoring the two densest global corridors of connectivity. U.S. landing stations serve as the primary gateways linking North America with Europe on one side and East Asia on the other, while also connecting to Latin America and the Caribbean, as we saw in the heatmap (Figure 4). This multiplicity of links means that the United States is not only directly connected to a very large number of partners, but also indirectly facilitates connectivity among other regions. Interestingly, China does not yet emerge in this representation as an autonomous hub within the global submarine cable network. This is likely a reflection of the temporal scope of the dataset, which extends only to 2018, and therefore captures only partially the country's growing involvement in the sector. As McGeachy (2022) notes, Chinese engagement in submarine cable construction intensified markedly from 2016 onwards, with Chinese companies participating in approximately 20 per cent of all global cable projects between 2016 and 2019. This growing role is primarily driven by large state-owned telecommunications firms with international reach, such as China Telecom, China Unicom, and China Mobile, complemented by private actors like Huawei Marine that contribute to fabrication

and installation capacities. The absence of China as a highly central node in the 2018 snapshot should therefore be read less as an indicator of structural marginality and more as a lag in the data, which does not yet fully capture the geopolitical and infrastructural implications of Beijing's intensified strategy in this domain.

Centrality Measures

Degree centrality (Figure 6) offers a straightforward indication of connectivity by capturing the number of direct cable links each state maintains. The results show that the United States, the United Kingdom, Japan, Singapore, and Indonesia are the most directly connected actors. This pattern reflects the concentration of submarine cable hubs in advanced digital economies and at major maritime crossroads in East and Southeast Asia.

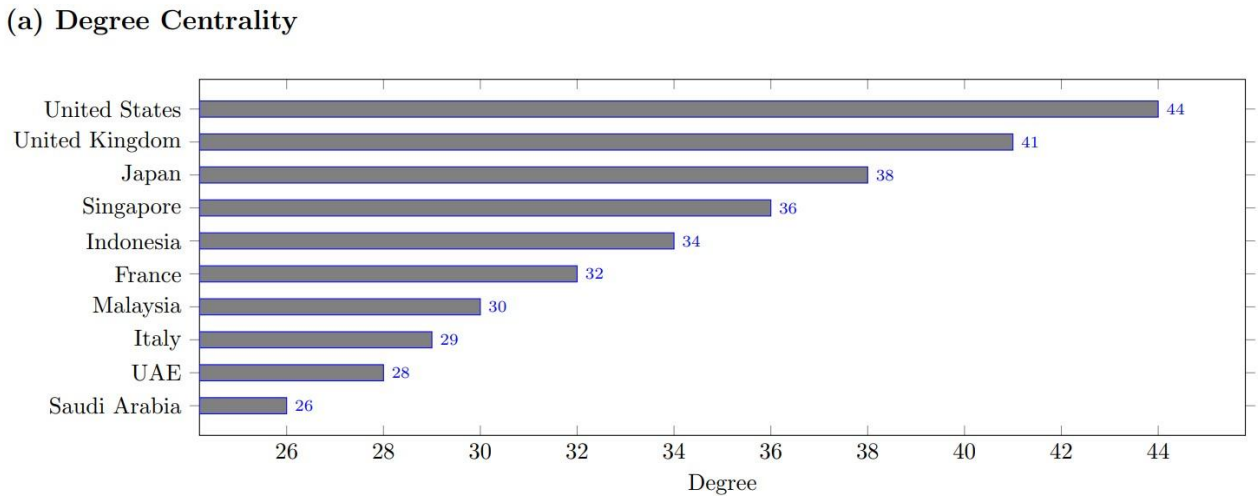

Figure 6 - Degree Centrality

Degree centrality, however, captures only the quantity of ties, without differentiating their relative importance. For this reason, *strength centrality* - the weighted equivalent of degree (Figure 7) - is particularly revealing. Here, the United States remains the most prominent actor, but Japan and Brazil also emerge as major hubs, alongside Singapore and the United Kingdom. The appearance of Brazil among the global leaders suggests that the South American network, although less dense in absolute terms, is anchored by a small number of highly capacitated connections. The Chinese case is also significant: while not at the top in degree centrality, China moves into the upper tier in weighted terms, reflecting its investment in a smaller number of high-capacity routes.

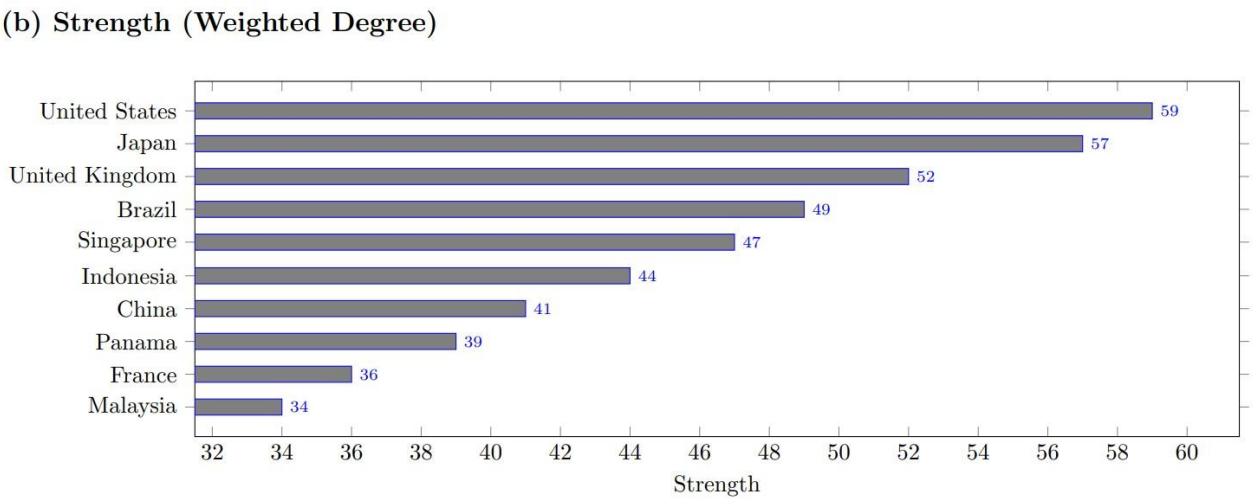

Figure 7 - Strength (Weighted Degree)

Betweenness centrality (Figure 8) shifts the focus from the number or weight of ties to the role of actors as intermediaries. This measure highlights the strategic importance of Italy, South Africa, Brazil, and Oman, all of which occupy critical bridging positions between otherwise distant regions. Italy links the Mediterranean to transatlantic and intra-European networks; South Africa connects the Atlantic and Indian Oceans; Oman functions as a pivotal hub for Gulf and Indian Ocean routes; while Brazil serves as the principal connector between South America, North America, and Europe. These findings indicate that states with relatively fewer total connections can nonetheless acquire disproportionate importance by controlling key transit points.

(c) Betweenness Centrality

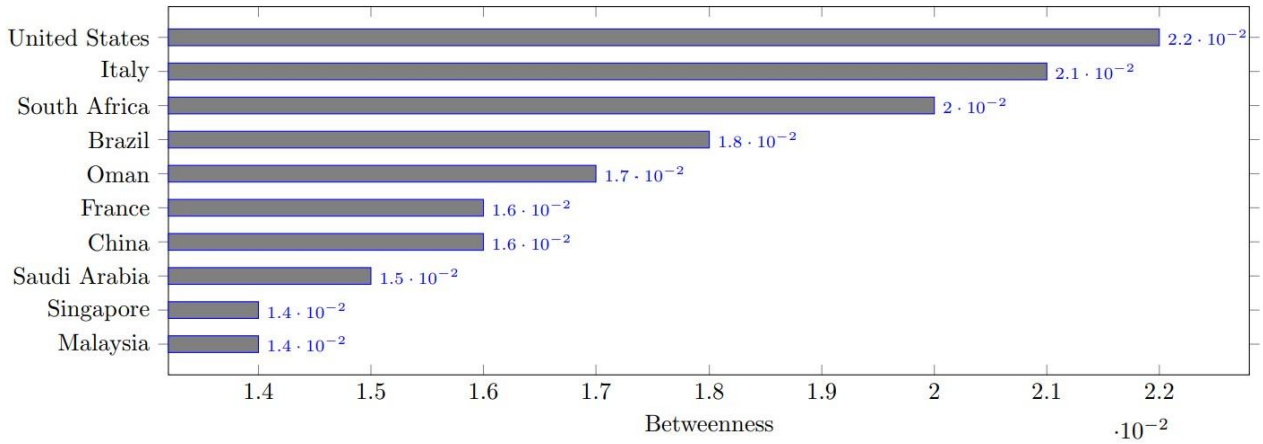

Figure 8 - Betweenness Centrality

Figure 9 displays the results for *closeness centrality*, highlighting the nodes that are on average at the shortest topological distance from all others in the network. Interestingly, the ranking is dominated not by major global hubs but by a series of small island territories and geographically strategic states. The United States Minor Outlying Islands and the Virgin Islands appear at the top of the distribution, despite their limited infrastructural weight in terms of cable capacity or number of connections. This outcome suggests that closeness in this network should not be interpreted as a direct measure of infrastructural power but rather as an indicator of positionality within the topology of submarine connectivity. Because these islands are tied directly to large hubs, often across multiple basins, they achieve high proximity scores even with few links. The same logic explains the presence of Panama, South Africa, Sigapore and New Zealand in the top ten. Each occupies a critical geographical hinge that connects otherwise distant maritime basins. Their cables effectively reduce the average distance across regions, placing them “close” to the rest of the network despite their more modest scale. This finding underscores the degree to which physical geography continues to shape digital topologies. At the same time, it is important to note that these results may also reflect artefacts of the dataset and network construction. Since the model aggregates connections at the state level, small territories directly attached to highly central hubs may be artificially boosted in their relative closeness. Nevertheless, the pattern remains consistent with the broader hypothesis that geography plays a constitutive role in the organization of cyberspace, as natural chokepoints and peripheral islands alike condition how “close” states appear in the global cable network.

(d) Closeness Centrality

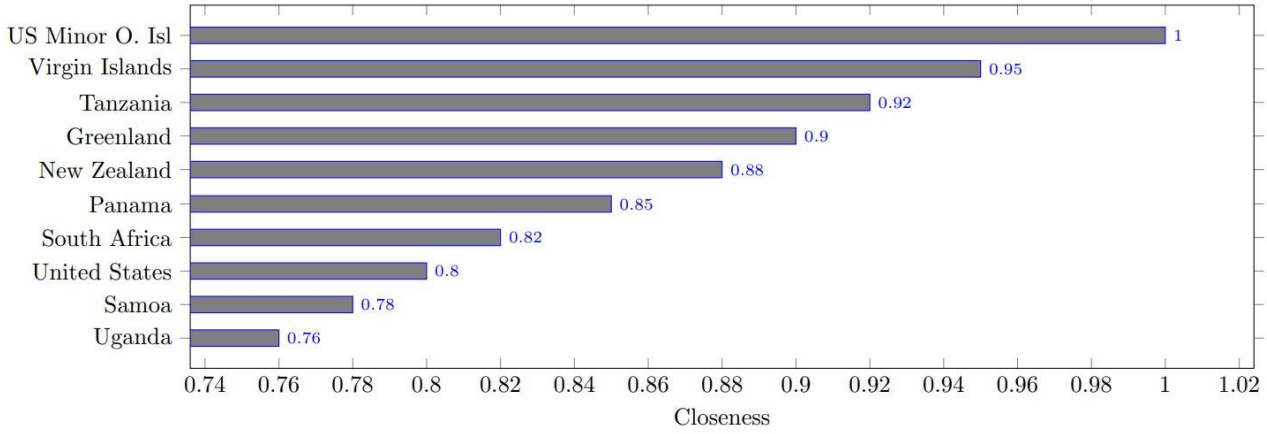

Figure 9 - Closeness Centrality

Finally, in the *eigenvector centrality* measure (Figure 10) the ranking is dominated by the Asia–Pacific rim: Japan tops the distribution, followed by Indonesia, China, and Singapore, with the United States, the Philippines, South Korea, and Malaysia also scored highly; the United Kingdom and Russia round out the top ten. Because eigenvector centrality rewards connections to *well-connected* partners (and here edges are weighted by cable capacity), these results indicate a densely interlinked APAC nucleus in which leading actors are mutually connected via high-capacity systems and simultaneously tied into trans-Pacific routes to the U.S. Japan's position reflects multiple, capacious links to other central nodes (U.S., Korea, China, Southeast Asia) within a tightly knit regional core. Indonesia's elevated score is consistent with its role as an archipelagic gateway between the Indian and Pacific basins, connected to Singapore, Malaysia, Australia, and trans-oceanic systems; its neighbors' high centrality lifts its own. China and Singapore likewise benefit from proximity to, and interconnection with, highly central partners within this East/Southeast Asian cluster. The U.S. remains among the most influential nodes, but eigenvector centrality places slightly greater emphasis on being embedded inside a dense *regional* core than on spanning multiple regions, hence several APAC hubs outrank it. The UK appears as Europe's principal representative owing to its strong ties to both North America and Northwestern Europe, while Russia's placement reflects connections across the Baltic/Black Sea and the Far East. Two caveats are warranted. First, eigenvector scores are sensitive to modeling choices: here we compute them on a state-level, undirected graph and weight edges by nominal cable capacity, which privileges densely inter-connected regions with many high-capacity systems. Second, the dataset is time-bounded (to 2018 in this study); under-representation of post-2016 Chinese outward investments may depress or reshape some rankings. With those

limitations in view, the pattern is substantively meaningful: influential "eigenvector hubs" concentrate along the Eurasian rimland and its trans-Pacific extensions, underscoring how regional clustering and high-capacity mutual ties structure the hierarchy of global submarine connectivity.

(e) Eigenvector Centrality

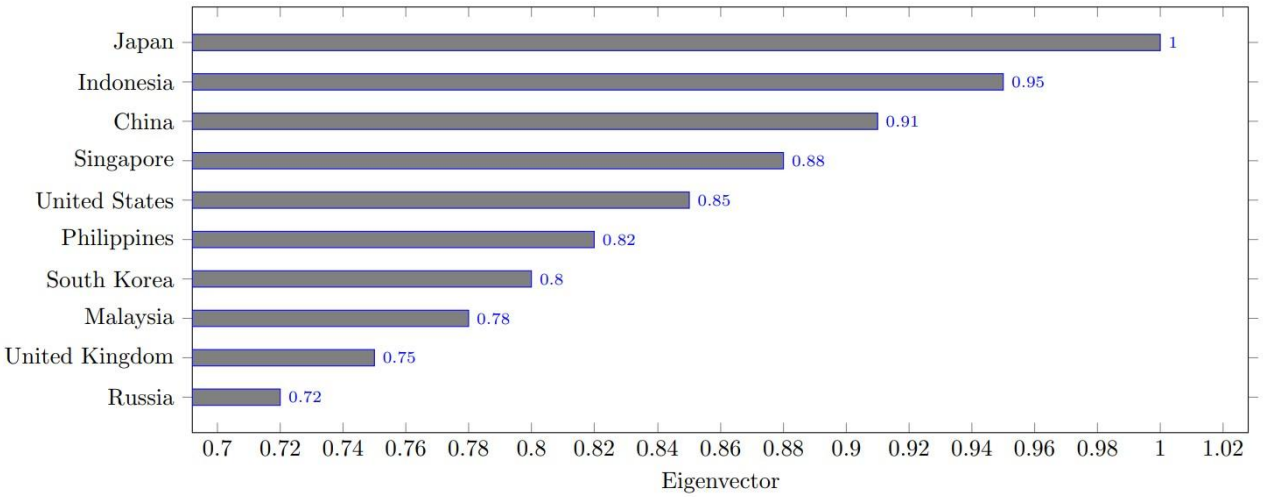

Figure 10 - Eigenvector Centrality

Regional Clusters in the Submarine Cable Network

The application of the Louvain modularity algorithm to the representation of the submarine cable network graph produced a set of regional clusters that reflect both infrastructural interconnection and enduring geographical patterns (see figure 11 and Appendix, Cluster List). While the network is not strictly determined by physical proximity, the results indicate that geography continues to exercise a significant influence on how states are grouped together. For instance, one of the largest clusters encompasses the countries of Northwestern Europe and the North Atlantic, where dense historical ties and overlapping cable landings have created an integrated community of connectivity. Similarly, a cluster spanning the Malay Archipelago, East Asia, and the Western Pacific demonstrates how island

geographies with short coastlines and high demand for digital traffic are bound into tightly knit subnetworks.

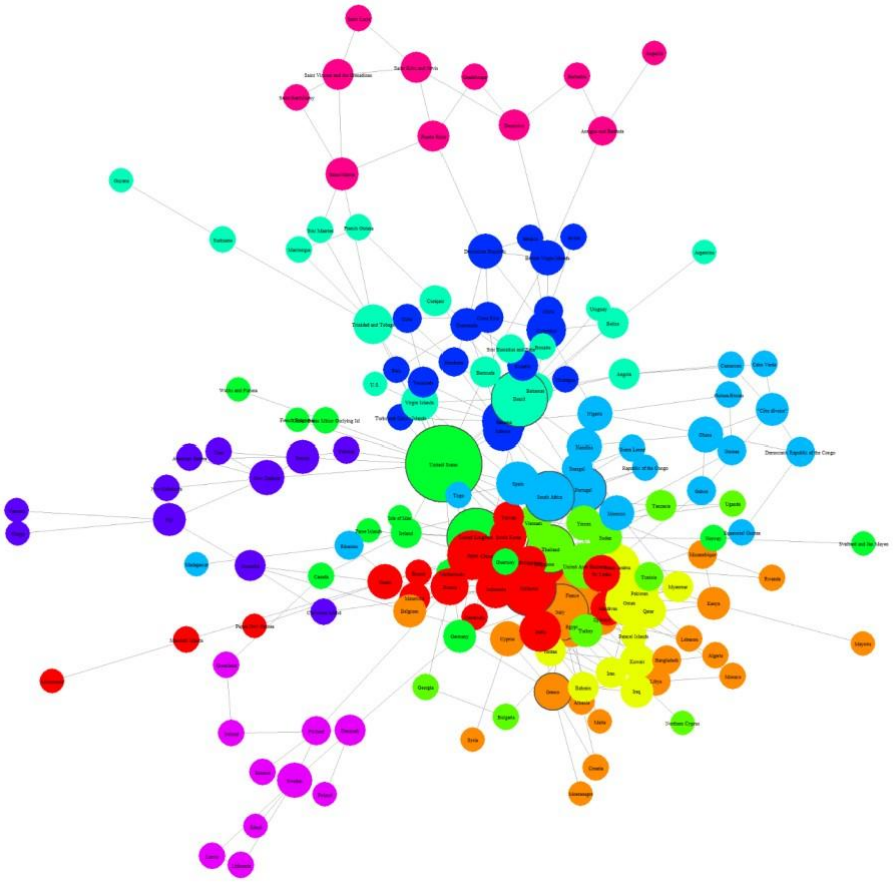

Figure 11 - Clusters in the Submarine Cables Network

Other clusters are organized around strategic maritime basins: the Mediterranean and Red Sea region forms a distinctive community linking Europe, North Africa, and the Middle East, while West Africa and the Iberian Peninsula appear as another cohesive grouping. The Americas are split into several communities, with the United States and its Atlantic and Pacific territories forming one cluster, South America another, and the Caribbean basin yet another. Oceania is grouped separately, with Australia, New Zealand, and their Pacific island neighbors constituting a distinct community. These results show that the modular structure of the submarine cable network echoes, at least in part, the underlying morphology of global geography. Coastal proximity, the presence of narrow straits, and shared maritime corridors strongly condition the density of interconnections.

Brokerage and Strategic Intermediation

Beyond identifying communities, it is equally important to assess which actors bridge these otherwise dense but separate regions of the network. For this purpose, measures derived from Ronald Burt's (1995) theory of structural holes were applied, namely constraint, effective size, and efficiency. These indicators highlight the extent to which particular countries act as brokers, connecting otherwise weakly tied clusters, and thereby gaining strategic leverage in the network.

Country	Degree	Constraint	Eff. Size	Efficiency
United States	25	0.103	22.40	0.897
United Kingdom	17	0.151	14.40	0.849
Italy	16	0.131	13.90	0.869
Brazil	16	0.145	13.70	0.855
Malaysia	15	0.176	12.40	0.824
France	14	0.170	11.60	0.830
South Africa	13	0.129	11.30	0.871
Japan	13	0.190	10.50	0.810
Thailand	12	0.150	10.20	0.850
Oman	12	0.208	9.51	0.792

Figure 32 - Structural Hole Measures (Top 10 Countries)

The results reveal that the United States occupies by far the most advantageous brokerage position, with very low constraint values and a very high effective size. This reflects its role as the principal intermediary between the Atlantic and Pacific basins, as well as its connections to Latin America and the Caribbean. The United Kingdom and France also emerge as important brokers, leveraging their extensive transatlantic and Mediterranean connections. Interestingly, Italy ranks particularly high, a result of its geographical location as a pivot between Europe, the Mediterranean, and the Middle East. Outside the Euro-Atlantic core, Brazil and South Africa demonstrate notable brokerage roles, acting as bridges between the Global North and the Global South. In Asia, Malaysia, Japan, Thailand, and Oman appear as key intermediaries linking different regional communities: the first two reflecting their position in dense East Asian and Pacific subnetworks, while Oman highlights the strategic role of the Arabian Peninsula as a gateway between Asia, Africa, and Europe.

All this shows that brokerage power is not simply a function of overall connectivity, but of being structurally positioned at the margins of clusters, where one can connect otherwise fragmented parts of the network. This structural autonomy provides leverage and influence, since actors occupying such positions can control or facilitate flows between otherwise poorly connected communities. In

this sense, Burt's measures complement traditional centrality indicators, showing not just who is most connected, but who is best placed to mediate across the fragmented geography of the submarine cable system.

A Geopolitics of the Network

The results of the network analysis underscore that the global submarine cable system cannot be conceived as a "flat", evenly distributed infrastructure. Rather, it is characterized by a markedly hierarchical topology, in which a limited number of states concentrate the bulk of connectivity while vast peripheral regions remain structurally dependent on a handful of strategic intermediaries. The empirical evidence derived from centrality measures, community detection, and structural hole analysis converges on a single conclusion: geography continues to matter, and the absolute spatial location of states on the globe exerts a profound influence on the architecture of digital connectivity.

At the core of the system lies the United States, whose unrivalled centrality is visible across all metrics. The U.S. does not merely host the largest number of cable connections; it anchors the densest transoceanic corridors. This multiplicity of links situates the U.S. as both a regional hub and an indispensable global interconnector, ensuring resilience through redundancy and exercising influence through the structural dependence of other actors. Its position illustrates how digital infrastructures are not only technical assemblages but also embodiments of geopolitical power, enabling the United States to act simultaneously as guarantor and gatekeeper of global flows. Beyond the absolute dominance of the core, the modular structure of the network reveals the persistence of geography in shaping connectivity. The Louvain clusters correspond closely to major maritime basins and rimland regions, including the North Atlantic, the Mediterranean and Red Sea, the Malay Archipelago, and the Caribbean. These clusters highlight how physical proximity continues to underpin digital interconnection. The spatial organization of the submarine cable system thus mirrors centuries-old patterns of maritime exchange: the same chokepoints and corridors that once concentrated shipping now channel global data flows. This continuity underscores that cyberspace, despite its apparent immateriality, is profoundly inscribed in the physical logics of geography. Yet the results also show that geopolitical leverage does not rest solely with the largest hubs. Burt's measures of structural holes bring to the fore a second layer of power dynamics, highlighting the brokerage roles of states such as Italy, Oman, Malaysia, and South Africa. These countries, though not dominant in terms of volume or density of connections, bridge otherwise weakly linked clusters. Their geography at the hinges of maritime chokepoints, the Strait of Malacca, the Mediterranean basin, the Persian Gulf, or the Cape of Good Hope, confers upon them a disproportionate importance as gatekeepers of interregional communication. Their structural autonomy derives not from size but from geographical position: by

linking fragmented communities, they mitigate disconnection and acquire a strategic leverage that exceeds their quantitative weight.

The network thus exhibits a multilayered geopolitical hierarchy. At the global level, a handful of core states - above all the United States - anchor the densest transoceanic corridors. At the regional level, modular clusters emerge along historical maritime basins, reflecting how proximity and demand coalesce into cohesive communities. At the intermediary level, strategically located states function as bridges, sustaining inter-cluster connectivity and concentrating risks. In contrast, peripheral regions in Africa, South America, and Oceania remain marginal, tied into the global network primarily through a small number of intermediaries. This peripheral positioning generates inefficiencies, since data flows must traverse longer paths, but, more importantly, produces dependencies, as the stability of entire regions hinges on the continuity of links managed by a few central or brokerage states. Taken together, these findings corroborate the third working hypothesis advanced in this dissertation: that the submarine infrastructure of cyberspace is not characterized by a flat or evenly distributed architecture, but rather reproduces a hierarchical structure in which a limited number of highly central hubs concentrate connectivity, vast peripheral regions remain dependent on a few gateways, and brokerage power accrues to states strategically positioned at the intersections of regional clusters. The analysis demonstrates that the submarine cable system embodies a reproduction, within the digital domain, of the same asymmetries, constraints, and affordances that have long defined maritime geopolitics. Geography thus persists not as a residual factor but as a constitutive determinant of global connectivity, embedding relations of power, dependence, and vulnerability into the very architecture of the internet, an image that stands very far from the image of cyberspace from which we started this chapter.

These findings must also be interpreted through the lens proposed by Farrell and Newman (2019) in their conceptualization of *weaponized interdependence*. Their framework provides a structural explanation of interdependence, showing how the topology of global networks generates enduring power asymmetries among states. As research in sociology and computational network science has long demonstrated, complex systems tend to produce asymmetric structures in which a few nodes emerge as “hubs,” far more connected than others. Such asymmetry creates opportunities for coercion: states with political authority over the central nodes through which capital, goods, and information circulate are uniquely positioned to impose costs on others. Where domestic institutions allow, they can exploit these networks to monitor flows, restrict access, expose vulnerabilities, and compel policy change. Farrell and Newman identify two distinct mechanisms through which states can translate network centrality into strategic advantage: the *panopticon effect*, which refers to the

informational benefits derived from privileged access to flows, and the *chokepoint effect*, whereby dominant actors can restrict or deny flows to others. Seen through this framework, the hierarchical structure of the submarine cable network is not simply a matter of uneven geography, but a potential source of political leverage, enabling certain states to weaponize their centrality or brokerage positions within the global infrastructure of cyberspace. Seen through this framework, the hierarchical structure of the submarine cable network is not simply a matter of uneven geography, but a potential source of political leverage. The United States − the actor that emerges as the unrivalled hub in our network analysis − has already demonstrated how network centrality can be exploited through both the *panopticon* and *chokepoint* effects. The Snowden revelations exposed the extent to which U.S. intelligence agencies relied on their jurisdiction over key infrastructural nodes to intercept, filter, and analyze information flows, thereby transforming centrality into informational dominance. At the same time, the U.S. position within global financial infrastructures, most notably through its ability to influence the SWIFT network, has illustrated the coercive potential of chokepoints, where adversaries and even allies may be selectively excluded from vital transactions (on this see: Farrell and Newman 2023). These examples confirm that the asymmetric topology revealed in our analysis is not a merely descriptive property of the system, but one that can be actively weaponized to shape international outcomes. The strategic implications extend naturally beyond the United States. China, as Hillman (2021) observes, is in fact deliberately seeking to construct its own infrastructural sphere of influence through the *Digital Silk Road*. This effort to position itself at the center of alternative networks reflects an awareness of the advantages accruing to infrastructural centrality. While concerns are often raised that deeper integration into centralized networks may expose technologically advanced states to novel vulnerabilities, it is equally plausible, and indeed empirically supported, that centrality generates greater benefits than costs. For states capable of mobilizing their domestic institutions to harness both informational and coercive potentials, occupying the hub of infrastructural networks remains a source of enduring structural power.

The Geography of Data: Where Do the Data Reside (and why)?

Having examined submarine cables as the connective backbone of global cyberspace, the analysis now turns to a second infrastructural pillar whose strategic and material importance has surged over the last two decades: data centers. If cables function as the arteries of global data flows, data centers operate as their vital organs − absorbing, storing, and processing vast amounts of information, before redistributing it into circulation. In contrast to the almost two centuries-old genealogy of submarine infrastructure, data centers constitute a more recent yet indispensable component of the digital

economy, propelled by the expansion of cloud services and the exponential growth in data-intensive applications such as artificial intelligence, blockchain technologies, and real-time streaming (Holt & Vonderau 2015).

In this work, the term "data center" will be employed as an umbrella designation for a diverse set of infrastructures that are otherwise referred to in both technical and public discourse by names such as *data hall*, *data farm*, *data warehouse*, *computer room*, *server room*, *research and development laboratory*, *high-performance laboratory*, *hosting facility*, or *colocation site*. Although each of these terms emphasizes distinct dimensions, ranging from spatial characteristics to technological sophistication or organizational function, this work follows Geng (2015) in consolidating them under the single notion of the "data center."

At the technical level, data centers are defined as facilities housing electronic equipment devoted to data processing (servers), data storage (storage arrays), and communications (networking hardware). These core functions are sustained by elaborate subsystems of energy provision often involving backup generators and specialized power conversion technologies and by climate-control systems designed to maintain stable temperature and humidity levels for information and communication technologies (ICT). In this sense, data centers are not simply rooms filled with servers; they are highly engineered environments in which multiple technological domains such as energy, cooling, hardware, software, are integrated to guarantee the uninterrupted flow of information.

Yet to define data centers purely in infrastructural terms would be analytically insufficient. From a political science perspective, data centers must also be understood as strategic sites of power, governance, and social ordering. They are simultaneously technological assemblages and institutional nodes that sustain the informational foundations of contemporary societies. Their existence makes possible the operations of state agencies, multinational corporations, financial markets, universities, and cultural industries alike. The services they support ranging from e-commerce and digital communication to national security, public administration, and health care, illustrate the extent to which they now form part of the essential infrastructure of social and political life. This functional centrality has at least three implications for how data centers should be conceptualized. First, they are geo-political objects, insofar as their siting, regulation, and energy consumption provoke debates about sovereignty, security, environmental sustainability, and economic competitiveness. Second, they are global infrastructures: although physically localized, they are enmeshed in transnational networks of capital investment, supply chains, and governance regimes, producing new asymmetries of dependency between regions and actors. Third, they embody a sociotechnical imaginary of digital

modernity, representing both the promise of innovation and the challenge of managing its material and ecological costs.

Data centers vary enormously in size, from installations consuming a single megawatt to hyperscale complexes surpassing 500 megawatts, but this diversity does not diminish their conceptual coherence. Regardless of scale, their unifying purpose remains the processing, storage, and transmission of information. It is this functional and systemic commonality that justifies the adoption of "data center" as the operative category throughout this dissertation, in line with the approach outlined in Geng's *Data Center Handbook* (2015). Framing the analysis in these terms allows us to treat data centers not only as technical facilities but also as critical infrastructures of the digital state and economy, whose governance and implications are at the core of the political questions explored in this study.

As with cables, the geography of data centers is not a neutral or purely technical matter, but rather the outcome of a complex interplay between environmental conditions, regulatory frameworks, market demand and naturally political decision. Their material footprint is particularly controversial, since these facilities consume immense quantities of both electricity and water, raising harsh discussions about sustainability, sovereignty, and social priorities. In Ireland, for example, the data center industry now accounts for more than one-fifth of national electricity demand, prompting the national grid operator to freeze new connections near Dublin until 2028 (O'Brien 2024). This has generated a polarized debate: while policymakers see data centers as magnets for foreign investment and digital innovation, civil society groups argue that their expansion jeopardizes the country's climate targets and strains limited renewable energy capacity (O'Carrol 2024). Similar tensions have unfolded in the Netherlands, where hyperscale facilities operated by Microsoft and Google have drawn scrutiny for their excessive consumption of drinking water − up to 84 million liters in a single year in the case of Microsoft's Middenmeer complex (Judge 2022). These controversies illustrate how the siting of data centers intersects with local ecologies and resource politics, transforming what might appear as purely technical infrastructures into contested terrains of governance and legitimacy.

Yet environmental factors are not only liabilities; they also create locational advantages. Cool and stable climates, such as those of Northern Europe, reduce reliance on energy-intensive cooling systems, making regions like Scandinavia particularly attractive (Payton 2023). Moreover, data centers usually remain geographically proximate to major population and economic centers to minimize latency and ensure service efficiency. These tensions − between environmental suitability, regulatory contexts, and digital demand − makes their geography particularly illustrative of how cyberspace is grounded in both physical terrain and socio-political conditions.

In this section, I will first explore the historical emergence and growth of data centers within the broader architecture of digital infrastructure, from simple mainframe rooms to hyperscale facilities. Thereafter, I will leverage available spatial data to examine whether discernible geographical patterns emerge in their distribution − particularly with respect to climate, natural hazard exposure, and population density. The objective is to assess to what extent geography continues to be a constitutive factor in shaping not only the connective arteries of cyberspace, but also the computational nodes that render that connectivity meaningful. At the same time, it is important to delimit the scope of the present analysis. While the legal and regulatory regimes governing data center development, as well as the precise quantification of their environmental impact, are crucial dimensions of current scholarly and policy debates, they fall beyond the remit of this dissertation. The empirical contribution offered here will instead be restricted to assessing whether discernible geographical patterns emerge at the global scale, focusing in particular on physical variables such as climate and natural hazard exposure, alongside human-geographical factors like population distribution. In this way, the aim is not to adjudicate on the legitimacy or sustainability of data centers, but rather to investigate how their spatial configuration reflects broader geographical logics and constraints, and how these in turn shape the architecture of cyberspace.

A Brief History of Datacenters

Although the genealogy of data centers[12] is much shorter than that of submarine cables, their historical emergence illustrates in a similarly striking way how digital infrastructures are embedded in specific material and political contexts. In their earliest incarnations, mid-twentieth-century computer rooms for military and research machines already displayed the essential features that continue to define data centers today: concentration of expensive and fragile hardware, strict environmental control, and a regime of restricted access that marked them off as spaces of authority and surveillance. In their earliest incarnation, what we now call data centers were not separate facilities but the very rooms that housed the only computers in existence. During the 1960s, these were enormous and expensive mainframes, carefully enclosed in climate-controlled environments to ensure stable operation. Because of their prohibitive cost, few organizations could own such machines outright; instead, businesses and public agencies often rented computational time or space on a mainframe to perform specific functions. These “glass houses” were therefore simultaneously spaces of architectural specialization − designed for cooling, power conditioning, and restricted access − and infrastructures of shared computation, long before the advent of distributed networks or cloud services.

[12] On this the main reference is the timeline proposed by Angela Bartes 2011

The following decades witnessed a gradual transformation. With the advent of minicomputers in the 1970s and, later, personal computers in the 1980s, the monopoly of the mainframe declined. Yet this did not mark the disappearance of centralized facilities. On the contrary, as organizations accumulated ever-larger volumes of digital information, they continued to build dedicated rooms for storing servers, ensuring reliable power, and protecting against environmental hazards. What changed was not the necessity of such spaces, but their scale and purpose: data processing ceased to be a singular, rarefied resource and instead became a routine requirement of both business and administration. By the 1990s, this evolution had accelerated dramatically. The rise of the internet generated an unprecedented demand for connectivity, storage, and computational power. Servers multiplied, networks expanded, and the physical infrastructure required to sustain them became increasingly specialized. Purpose-built data centers emerged, often in the basements of office buildings or in converted industrial facilities, designed not only to house machines but to guarantee uninterrupted service through redundancies in cooling, power, and connectivity. It is in this period that the term "data center" began to acquire its contemporary meaning: not just a computer room, but a strategic infrastructural node within the emerging architecture of global communication.

The turn of the millennium marked a decisive shift. What had begun in the 1960s as scarce mainframes confined to a handful of rooms had, by the early 2000s, evolved into vast server farms forming the backbone of digital globalization. One of the main and most important changes is marked by the rise of hyperscale facilities and the development and consolidation of cloud computing. Hyperscale data centers, typically defined as facilities hosting thousands of servers[13] with scalable architectures, emerged as the preferred model of the major technology companies. Rather than functioning as isolated units supporting the needs of a single organization, these new infrastructures were conceived as vast computational ecosystems capable of serving millions of users simultaneously across multiple services. Unlike the server rooms and corporate data centers of earlier decades, hyperscale infrastructures were conceived from the outset as vast, modular ecosystems capable of hosting tens of thousands of servers and scaling computational capacity in step with exponential demand. Their growth was propelled first by the expansion of e-commerce and search engines, then by the explosion of social media platforms, and more recently by the rise of data-intensive services (Holt & Vonderau, 2015). At the heart of this transformation lies the rise of a handful of global platform companies − Amazon, Google, Microsoft, and Meta foremost among them − which invested massively in building hyperscale facilities. These operators "simply" leveraged economies of scale

[13] According to IBM (Powell and Smalley 2024) to be considered a true hyperscaler, a company must use 5,000 servers or more and devote at least 10,000 square feet to the operation.

to reduce costs and ensure reliability, but in doing so they also restructured the geography of digital infrastructures. Rather than being dispersed across company headquarters or public agencies, computational power became increasingly concentrated in a relatively small number of massive sites, each serving millions of users worldwide. Cloud computing was both the enabler and the outcome of this process: by decoupling processing and storage from local hardware, it allowed organizations and individuals to outsource their digital needs to remote infrastructures, thereby reinforcing the centrality of hyperscale nodes as the true backbone of the global digital economy.

If submarine cables constitute the hidden skeleton of cyberspace, data centers represent its most visible flesh − though one often carefully staged. As Holt and Vonderau (2015) have noted, since the early 2010s corporations such as Google, Apple, Facebook, and Microsoft have increasingly placed their facilities on display through curated photographs, video tours, and infographics − branding campaigns that invite the public to "see where the Internet lives". Images of brightly colored pipes, vast halls of blinking servers, and pristine architectural spaces circulate as visual assurances of transparency, safety, and environmental responsibility. In Europe, operators such as Bahnhof have gone even further, converting Cold War bunkers into spectacular server farms, marketed simultaneously as fortresses of free speech and as monuments of technological resilience. This newfound visibility is, however, profoundly paradoxical. On one level, these images construct the physicality of "the cloud" for publics otherwise accustomed to thinking of data as immaterial. They aestheticize infrastructures, stripping them of technical complexity and recasting them as consumable icons of modernity and security. On another level− Holt and Vonderau (2015) contend − they obscure as much as they reveal: no information is offered about the precise functioning of servers, the scale of electricity and water consumption, or the transnational networks of which these facilities are a part. In this sense, the hyper-visibility of data centers conceals their opacity. As Holt and Vonderau argue, they embody the "politics of artifacts": their architectural and visual design is not neutral but actively produces imaginaries of digital space, shaping how infrastructures are perceived, legitimized, and contested. The staging of data centers thus participates in competitive corporate strategies as much as in environmental or political debates. Google's stylized portrayals project universal reach and ecological responsibility; Bahnhof markets resilience, secrecy, and the defense of civil liberties; Apple and Facebook emphasize clean energy and social responsibility. Each representation doubles as a territorial claim, embedding infrastructures with values that simultaneously promote corporate legitimacy and obscure their material contradictions. What emerges are persuasive designs: physical facilities that, through their public imagery, normalize dependence on private infrastructures while masking the asymmetries of power, ownership, and environmental cost on which they rest.

Despite these efforts at camouflage, controversies have nevertheless multiplied. Each of the dimensions just outlined has generated public debate: corporate concentration and asymmetries of control over data raise persistent concerns about sovereignty, while the environmental footprint of data centers has emerged as a particularly contentious issue. A paradigmatic illustration of the first set of controversies lies in the transatlantic dispute over data ownership and legal sovereignty. The extraterritorial reach of US legislation (on this see for instance Bittencourt 2025), most notably the CLOUD Act, grants American authorities access to data stored by US providers regardless of its physical location. This principle directly collides with European privacy regimes, exposing a fundamental asymmetry: infrastructures may be hosted on European soil, but their ownership and legal control often remain tethered to US corporations and jurisdiction. The Court of Justice of the European Union's *Schrems II* decision in 2020, which invalidated the EU–US Privacy Shield framework, made this conflict explicit, underscoring how the material location of servers does not translate into sovereign control over data. Here, the very geography of infrastructures is subordinated to competing legal geographies, illustrating that data centers are simultaneously local presences and transnational legal battlegrounds.

At the same time, the environmental dimension of these infrastructures has become an equally visible and polarizing field of contention. Whereas disputes over ownership and sovereignty emphasize the disjunction between territorial presence and legal authority, ecological debates foreground the material demands of infrastructures on their immediate surroundings. Data centers require colossal amounts of energy and water, drawing them into conflict with national climate targets, local ecologies, and community priorities. Thus, while the previous controversy points to the way infrastructures unsettle political jurisdictions, environmental debates highlight how they unsettle geographic and ecological equilibriums. Before turning to the explicitly political and territorial dynamics, addressed more thoroughly in the following chapter, this section focus on these environmental controversies, where the relationship between infrastructures and geography emerges most starkly, shaping both the selection of sites and the tensions that arise around them.

Environmental Opportunities and Constraints: Location, Location, Location!

If the debates around the environmental footprint of data centers have become particularly visible in the public sphere, the technical literature makes clear that the issue is neither incidental nor reducible to recent political controversies. At its core, a data center is an energy machine, and its

thermodynamics impose hard environmental and geographical constraints. As Geng (2015) explains, roughly half of the electricity that enters a facility feeds the ICT load − servers, storage devices, switches, and routers − while the other half is consumed by the "invisible" support infrastructure that keeps these machines alive: chillers, air-handling units, pumps, transformers, UPS chains, and distribution losses. Every watt of computation is instantly transformed into a watt of heat that must be expelled. This seemingly banal physical principle has profound consequences: it means that climate, humidity, and the availability of cooling water are not secondary factors but constitutive elements in determining where global cloud infrastructure can, and cannot, be sited. Cold and dry air can be mobilized to reduce the cost of cooling through free-air or water-side economization; conversely, hot and humid climates multiply the need for mechanical cooling, pushing up costs and carbon intensity. In this sense, geography is not an external backdrop to digital infrastructures but an active force that shapes their material configuration.

And yet, as Baudry (2015) underscores in his extensive discussion of site selection practices, the process is never as straightforward as simply identifying the "best" climatic or geological location. Rather, siting unfolds as a process of elimination that begins with very broad filters − legal jurisdiction, regulatory environment, macro-regions within acceptable latency windows − and proceeds through successive rounds of refinement. In principle, the criteria are clear: stable governments, favorable tax and energy policies, robust utilities, diverse carrier networks, and low exposure to natural hazards. In practice, however, the weighting of these factors is deeply uneven and often politically mediated. For example, while hazard avoidance is regularly listed as a "must-have" criterion, data centers continue to proliferate in areas exposed to earthquakes (California), hurricanes (the U.S. East Coast), or flooding (the Netherlands). The contradiction is resolved not by geography disappearing but by the belief that engineering solutions such as seismic bracing, hardened substations, redundant fiber routes can in fact neutralize environmental risk. In Baudry's words, site selection is rarely a quest for the perfect site, but rather a negotiation between acceptable flaws, economic incentives, and institutional path-dependencies. Latency adds another irreducible layer. No amount of financial subsidy or regulatory leniency can alter the speed of light, and thus certain workloads like data replication, high-frequency trading, transaction-intensive applications impose strict spatial envelopes on where facilities can be placed. Baudry (2015) illustrates this with the simple case of replication between New York and Mumbai: even in the best-case scenario, a one-way signal requires about 70 milliseconds to traverse the distance, before accounting for network interfaces and switching delays. This defines an absolute floor below which performance cannot be optimized. Geography therefore reappears in an even harder form: while energy and water costs can be

negotiated, and risks can be mitigated, the laws of physics delimit the catchment areas within which global operators can realistically deploy their nodes.

What emerges from the juxtaposition of Geng's and Baudry's accounts is a picture of infrastructural geography that is simultaneously rationalized and contingent. On the one hand, operators draw up detailed matrices of requirements, quantifying energy tariffs, latency windows, tax incentives, and permitting delays. The objective, in theory, is to minimize total cost of ownership over the lifetime of the facility. On the other hand, the actual decision is frequently filtered through subjective criteria: quality of life for relocated employees, proximity to corporate headquarters, or even the persuasive campaigns of local development agencies eager to advertise themselves as "data center friendly". Baudry notes that site searches are almost always conducted in secrecy, under code names and non-disclosure agreements, precisely to manage the political and economic stakes involved. Once public, these decisions become irreversible "territorial claims", locking infrastructures into places that may not have been the most rationally optimal but were rendered acceptable through a mixture of negotiation, narrative, and compromise.

The effect is paradoxical. In industry discourse and even in some policy debates, geography is often downplayed, as if the global reach of fiber networks and the modular design of hyperscale facilities rendered place irrelevant. But in practice, geography constantly reasserts itself, whether in the form of cooling requirements, latency thresholds, disaster risks, or the price of electricity (See on this Ciaramella and Roveda 2018). Indeed, the very fact that so much secrecy surrounds site selection− so much emphasis on not revealing plans until deals are signed − suggests how acutely contested the question of location remains. The ideal of a frictionless cloud dissolves under the weight of local negotiations over tax abatements, water rights, labor markets, and grid access. Far from erasing geography, the expansion of hyperscale facilities multiplies the ways in which local ecologies, infrastructures, and political economies come to matter.

Finally, this tension between rational calculation and political contingency is mirrored in the broader spatial distribution of data centers globally. Climatic suitability makes the Nordic countries appear as natural havens for "green" data centers, a trend reflected in the marketing of operators who emphasize the availability of renewable hydropower and cold air. Yet the same decade has witnessed an enormous concentration of hyperscale investment in Ireland, an island with neither abundant cooling advantages nor infinite grid capacity, but with favorable tax policies, English-language labor markets, and robust connectivity to North America and Europe. In other words, the geography of the cloud is never reducible to physical determinants alone. What Baudry describes as the "process of elimination" is always also a process of political selection, in which certain risks are bracketed out,

others are engineered away, and still others are deemed acceptable in exchange for economic concessions. What is left, as Geng's energy arithmetic reminds us, is a profoundly material infrastructure whose global map is the outcome of choices that are as political as they are thermodynamic.

Placed side by side, these cases underscore Baudry's observation that site selection is not about finding the "best" location, but about weighing trade-offs and eliminating options until only those deemed politically and economically viable remain. In Ireland, political will and fiscal incentives outdo environmental fragility; in the Netherlands, social resistance highlights the costs of overlooking water and land-use pressures; in Scandinavia, climatic and energy endowments are converted into comparative advantage. What is striking, however, is that in all three contexts the discourse of operators tends to minimize or even deny the geographical constraints that underpin their choices. Marketing narratives present facilities as placeless "cloud" infrastructure, while in practice their viability hinges on the negotiation of profoundly local factors: grid capacity, water rights, community acceptance, and the ability of municipalities to expedite permitting processes. Equally telling is the way in which exposure to natural hazards − from floods and rising sea levels to seismic or extreme weather risks − is frequently downplayed or bracketed out of decision-making. To use Baudry's (2015, 97) words: « [when searching and selecting where to build a datacenter] Avoiding forces of nature is one area where there is often a discrepancy between what people say and do». Despite recurrent recommendations in industry to avoid high-risk areas, in practice major facilities continue to cluster in coastal zones, seismic regions, or storm-prone corridors whenever these locations offer compelling economic or strategic advantages. As a result, the geography of data centers is marked not only by calculated optimization but also by tolerated vulnerabilities, where infrastructural resilience is assumed to be engineered ex post rather than built into site selection itself. Geography, in short, is both the substrate and the blind spot of the data center industry − constantly at work in shaping infrastructural landscapes, yet systematically ignored, displaced, or aestheticized in corporate imaginaries of seamless connectivity.

If the preceding discussion has emphasized the paradoxes, imaginaries, and contested politics of data center siting, the next step is to assess how these tensions materialize in the actual global distribution of facilities. Rather than treating geography as an abstract set of constraints, this empirical analysis seeks to make visible how infrastructures are actually inscribed in space: where facilities cluster, where gaps persist, and how these patterns articulate broader logics of concentration and exclusion. Mapping the geography of data centers in this way serves a dual purpose. On the one hand, it highlights concentrations of infrastructural power in specific regions, often revealing striking

asymmetries in the global landscape of the cloud. On the other, it provides an entry point for examining the factors that may explain such distributions. This empirical analysis will be the terrain on where to test the two hypotheses that this work formulated concerning the siting of datacenters. The first is that the global distribution of data centers is highly concentrated in the world's most economically advanced and digitally interconnected regions. If confirmed, this would indicate that data centers operate not merely as technical service infrastructures, but also as strategic hubs of power, reinforcing pre-existing hierarchies of wealth, connectivity, and technological capability. The second hypothesis is that siting patterns reflect a balance between environmental opportunities and risks on the one hand, and human-geographical priorities on the other. In this view, operators seek climates and energy regimes that reduce costs, while minimizing exposure to hazards such as flooding, earthquakes, or sea-level rise, and simultaneously ensuring proximity to population centers and markets where digital demand is concentrated. Testing these hypotheses requires attending to both physical and human-geographical variables. After all, data centers are not simply neutral facilities that provide services: they are infrastructural nodes through which political, economic, and informational influence is consolidated and projected.

The empirical exercise that follows is therefore not intended to claim determinism, but to examine to what degree the locational footprint of data centers reflects rational calculations of geography and to what degree it embodies political-economic logics. In short, by examining clusters and voids on the global map of the cloud, the analysis seeks to illuminate how material geography continues to shape, and be shaped by, the infrastructural beating heart of the digital age.

Datacenter's global spatial pattern

The empirical analysis of this part is based on an original dataset of data centers constructed through a two-stage process. In the first stage, facility addresses were collected using a Python-based web-scraping script from the public repository *datacenters.com*. In the second stage, these addresses were geocoded through QGIS in order to obtain precise spatial coordinates. Inevitably, a number of entries were lost in the cleaning process, primarily due to incomplete or ambiguous address information. The final dataset comprises 2,422 mapped facilities worldwide as of 2024. While this represents only a fraction of the estimated global total − around 10,000 operational sites (see Flack 2024)− it nonetheless provides a significant empirical window into the geography of the cloud.

Several limitations must be acknowledged. The first is quantitative: covering roughly one-quarter of the global population of data centers, the dataset cannot claim to be exhaustive. The second is geographical: the availability of reliable information varies markedly across national contexts. In countries with transparent regulatory frameworks or active industry reporting, coverage is comparatively robust; in others, data is scarce or altogether absent. The most notable example is Russia, where only a single facility appears in the dataset—clearly an artefact of information gaps rather than a reflection of infrastructural reality. Such asymmetries inevitably introduce distortions and call for caution when generalizing the findings. Despite these caveats, the dataset retains considerable analytical value. Its scope is sufficiently broad to allow the identification of global and regional clusters, the recognition of conspicuous voids, and the exploration of correlations with both physical and human geographical variables. Perhaps more importantly, it highlights the importance of assembling empirical evidence in a domain where infrastructural data is often fragmented, proprietary, and tightly guarded by corporate actors. The analysis that follows should thus be read not as a definitive cartography of the world's data centers, but as an empirical experiment: one that illuminates the spatial logics shaping digital infrastructures while laying the groundwork for future refinements and integration.

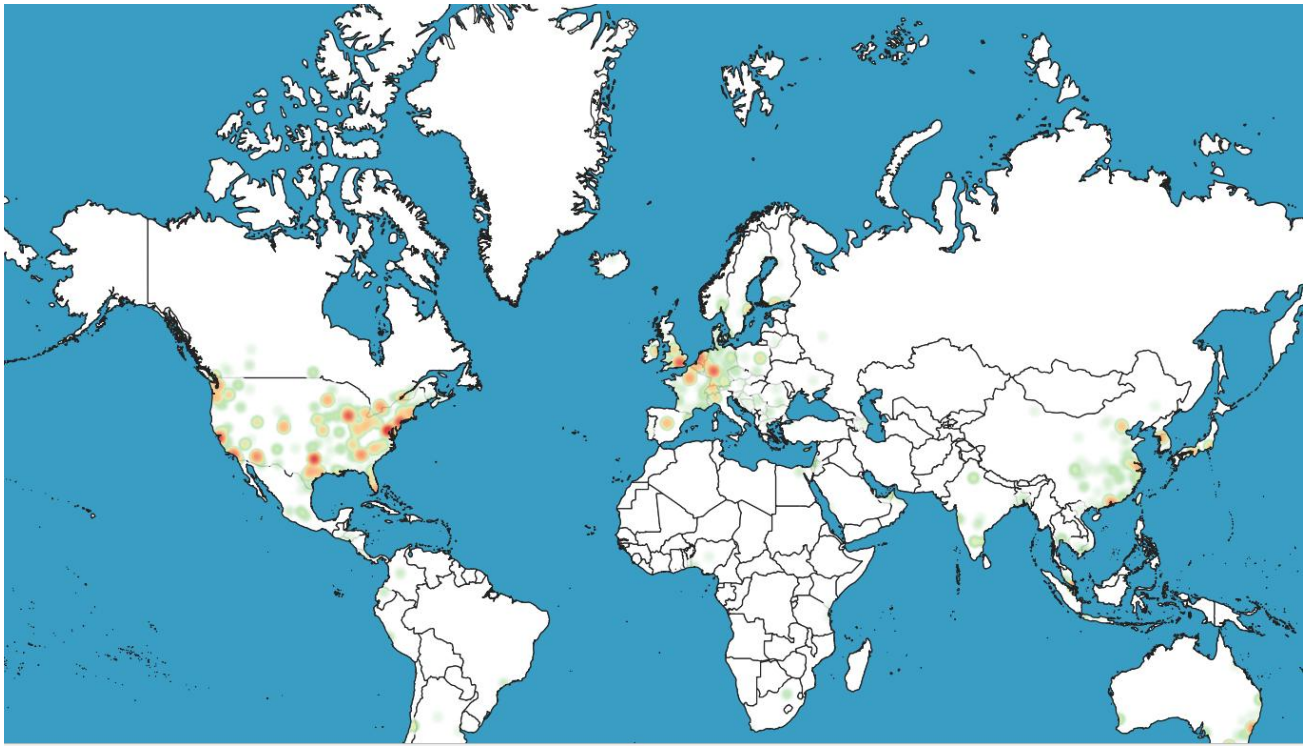

Figure 13 - Datacenter Global Distribution Heatmap

This first map (*Figure 13*) offers a global view of the distribution of data centers as captured in the dataset. What emerges immediately is a striking geography of concentration: North America and Western Europe appear as the undisputed cores of the cloud, with dense clusters spanning the US East Coast, Texas, California, and a corridor stretching from the Benelux countries through Germany to Northern Italy. Secondary but still visible concentrations appear in East Asia, particularly Japan, South Korea, and the coastal regions of China, alongside scattered presences in Southeast Asia, Australia, and a handful of sites in Latin America and Africa. By contrast, vast portions of the globe — from most of Africa and the Middle East to Russia and Central Asia — remain almost entirely blank, underscoring the unevenness of the infrastructural landscape.

The choice of a heat map representation is not incidental. It allows us to move beyond the sheer counting of facilities and instead capture relative concentrations, making visible clusters and voids even when the dataset may miss some entries. This visual strategy helps to mitigate biases linked to the partial nature of the data: while the exact numbers should not be taken at face value, the pattern of infrastructural density and absence remains robust. In this sense, the map highlights not only where the cloud is most materially entrenched, but also where it is conspicuously absent, foregrounding an infrastructural geography marked by both agglomeration and omission. Placed alongside the global map of submarine cables presented earlier, a strong resonance becomes evident. Just as cable landing points cluster along the main axes of the North Atlantic, Northern Europe, and East Asia, so too do data centers gravitate toward the same circuits of wealth and connectivity. Both infrastructures reproduce the hierarchies of the global economy, with dense concentrations in the Global North and marginal presence elsewhere. Seen through this lens, the first hypothesis finds strong preliminary support. The global distribution of data centers is far from random: it is overwhelmingly concentrated in the world's most advanced economies. Facilities cluster where financial markets, population density, and technological capacity already converge, confirming that data centers function not only as service infrastructures but also as centers of power. Their absence from large parts of Africa, South Asia, and Latin America is equally revealing: the cloud may be marketed as ubiquitous, yet its backbone is anchored in a narrow set of geographies that reproduce and deepen asymmetries of access. At the same time, the map should not be mistaken for an exhaustive census of global infrastructures. The underrepresentation of certain regions, whether due to gaps in data availability or deliberate opacity in the industry, accentuates the impression of concentration but also mirrors the unequal transparency surrounding these facilities. In this sense, the dataset is not merely a technical source but a political artifact, reflecting both the infrastructures that exist and the difficulties in rendering them visible.

While this first cartographic cut underscores the gravitational pull of advanced economies and high-connectivity hubs, it also leaves open the question of how far physical geography itself has shaped, or been sidelined in, these locational patterns. Do clusters simply mirror global economic hierarchies, or do they also reflect climatic suitability, exposure to natural hazards, and proximity to centers of digital demand? In other words, beyond the evident concentration in the Global North, the next step is to assess whether the geography of data centers also embodies a balance between environmental opportunities and constraints on the one hand, and the pressures of market demand and latency on the other. It is to this second hypothesis that the analysis now turns.

Climate, Natural Hazards and Population Density

The climatic dimension of data center siting was explored by linking each facility in the dataset to its local average annual temperature. Climatic data were obtained from the WorldClim 2.1 database (Fick & Hijmans, 2017), which provides high-resolution global climate surfaces widely used in environmental and spatial research. Specifically, the layer of *mean annual temperature* was employed, offering interpolated values derived from weather station records, remote sensing, and climate models for the period 1970–2000. While not a real-time measure, this dataset remains the most robust and spatially consistent source available for global comparative analysis.

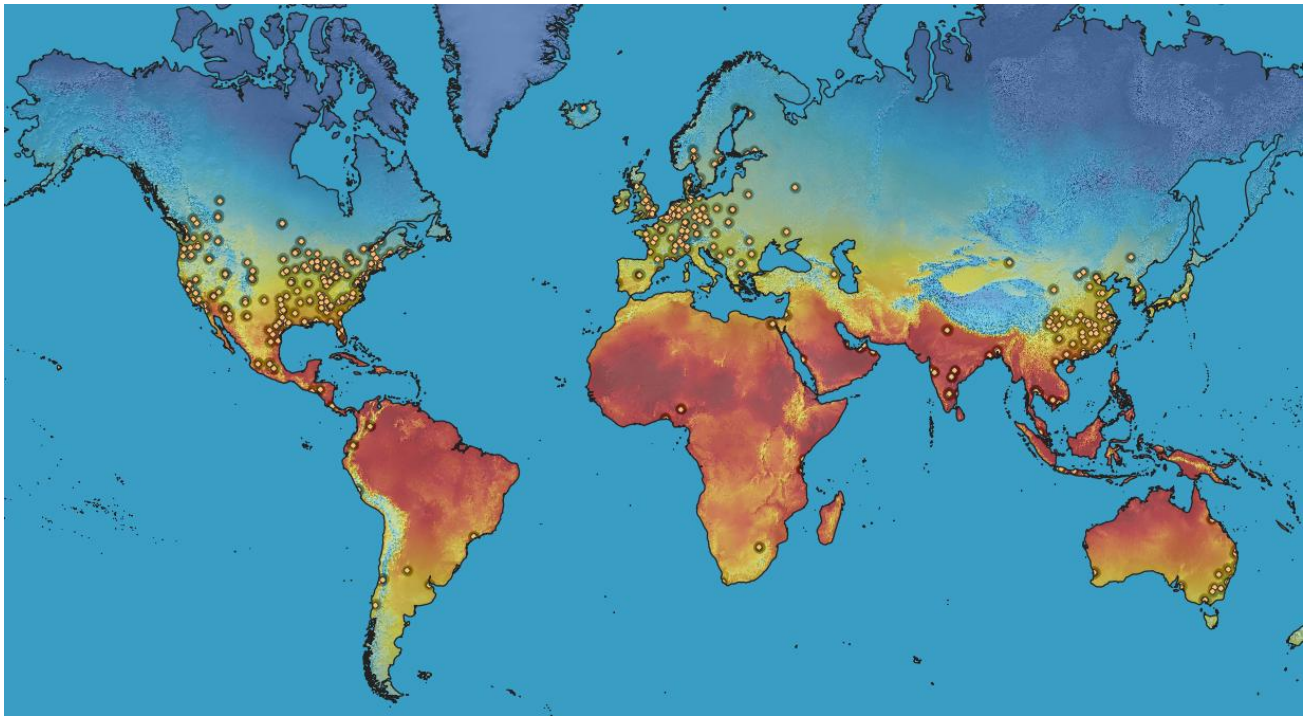

Figure 14 - Datacenter Distribution by Avarage Annual Temperature

Examining the role of temperature is particularly relevant in the context of data centers because cooling constitutes one of the most energy-intensive aspects of their operation. The practice of so-called *free cooling* (Ciaramella and Roveda 2018), that is, exploiting the natural difference between indoor and outdoor air temperatures to maintain stable conditions for servers, represents a crucial factor in reducing operational costs and environmental impact. Dry and temperate climates are especially advantageous, as they reduce reliance on mechanical chillers and allow greater use of outside air or water-side economization. Conversely, hot and humid climates increase dependence on energy-intensive refrigeration and complicate humidity control, while dusty or insect-prone environments raise filtration costs substantially. In this sense, climate is not a peripheral consideration but a structural element in the energy geography of data infrastructures. To conduct this analysis, the Point Sampling Tool in QGIS was applied to the dataset of 2,422 geocoded data centers (*Figure 14*). This tool allowed the extraction of the value of mean annual temperature at each precise geographic coordinate. The result was a dataset in which every data center could be associated with a specific climate zone, thereby enabling the exploration of correlations between environmental conditions and the global distribution of facilities. While this method does not establish causality, it offers a systematic basis for evaluating whether climatic factors exert a visible influence on the geography of the cloud.

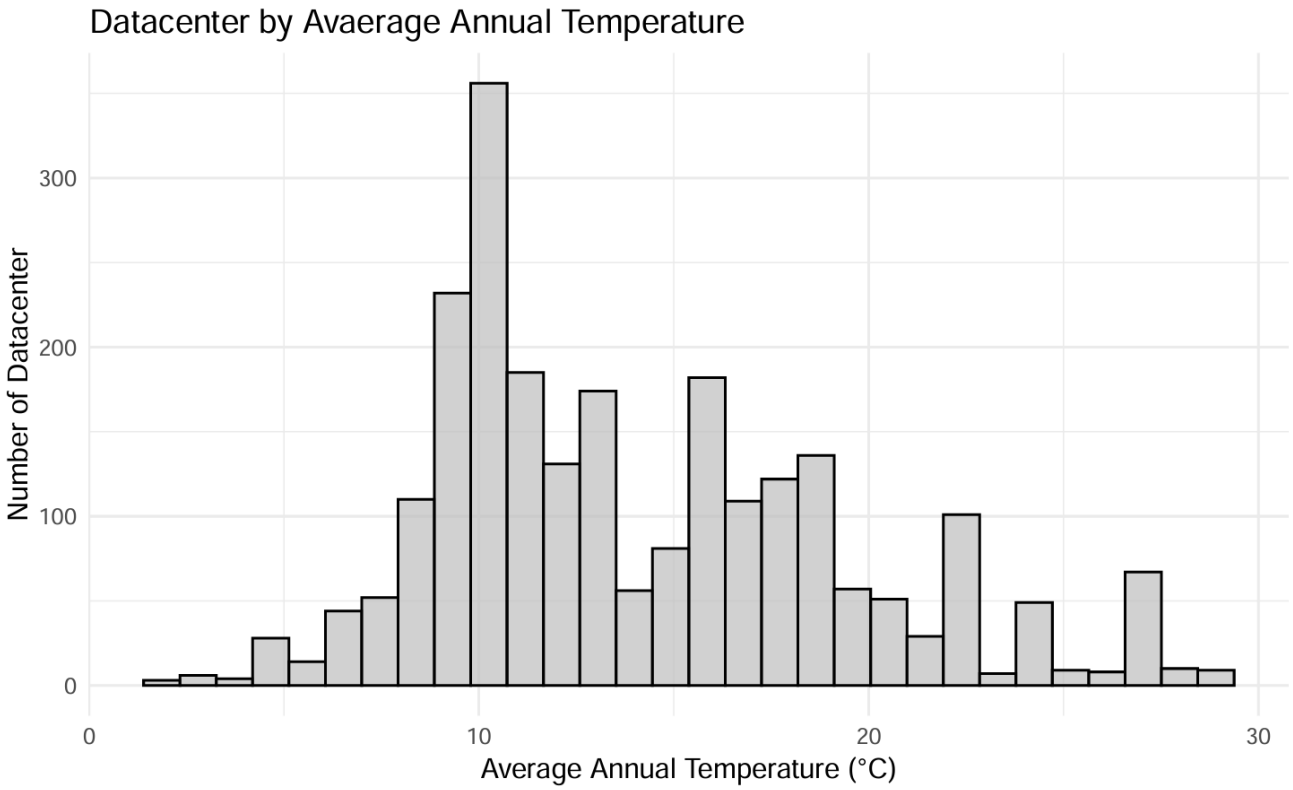

Figure 15 - Histogram Datacenter by Average Annual Temperature

Figure 15 (the histogram) presents the distribution of data centers according to their associated annual mean temperatures. The pattern is clearly skewed toward lower temperature ranges: the majority of facilities fall within temperate or relatively cool zones (roughly between an average annual temperature of 5°C and 15°C), while far fewer are located in hot climates exceeding 20°C. This skew suggests that, despite the industry's tendency to downplay geography in its rhetoric, climatic considerations do leave an imprint on infrastructural siting. The distribution supports the idea that operators privilege environments where natural cooling can be harnessed, thus reducing both energy costs and ecological footprints. Nonetheless, it must be stressed that this is a correlation rather than an explanatory model: multiple other factors, as said, such regulatory incentives, tax regimes, connectivity also shape location decisions. Still, the histogram provides an important first indication that climate is an interesting factor in the overall siting decision.

An additional dimension of the geography of data centers concerns their relationship to environmental hazards. To explore this, the global dataset of data center locations was overlaid with NASA's Global Multihazard Frequency and Distribution dataset (CHRR 2025), which integrates records of six major hazards: cyclones, droughts, earthquakes, floods, landslides, and volcanic eruptions. This dataset, developed within the SEDAC program, provides a global raster grid of hazard exposure based on

frequency and intensity observations, enabling an assessment of the coincidence between infrastructural concentration and environmental vulnerability. Using QGIS, each data center was assigned a hazard exposure level through the *Point Sampling Tool*, creating a spatially explicit profile of infrastructural risk.

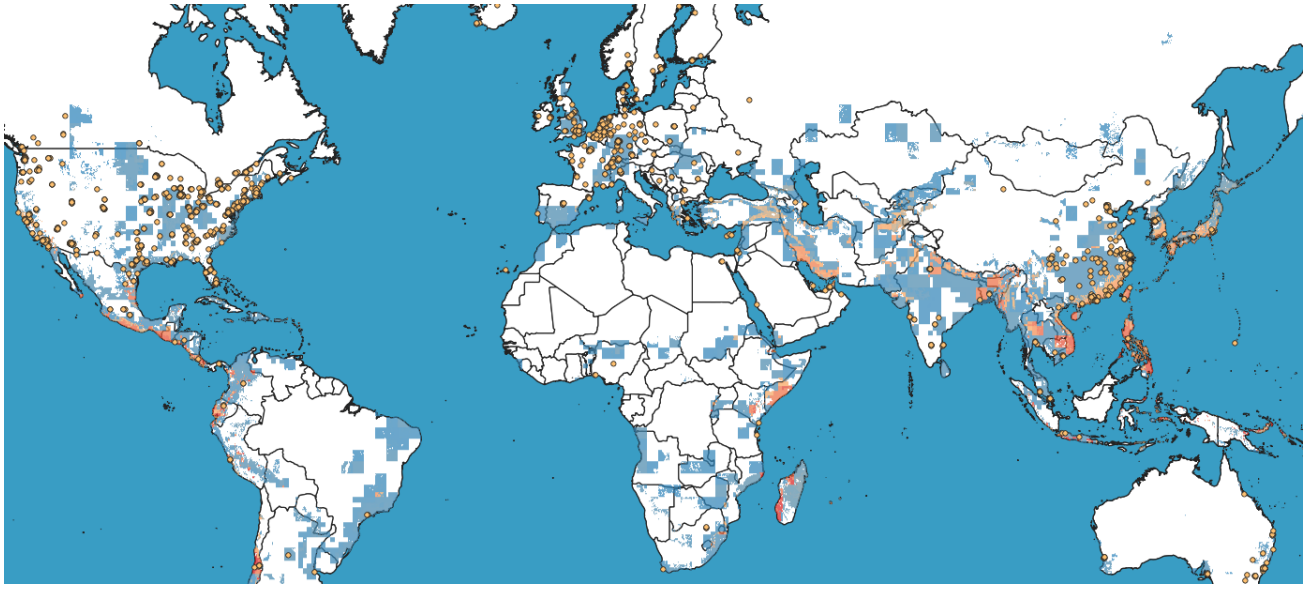

Figure 16 - Global Mult Hazard Index Datacenter Overaly Map

The results of this overlay (Figure 16) demonstrate a striking pattern. Although industry guidelines routinely emphasize the need to avoid hazard-prone areas, in practice many data centers continue to cluster in zones of high seismicity, cyclone frequency, or flood risk. This is particularly visible along the Pacific Rim, the eastern seaboard of the United States, and low-lying regions of Southeast Asia. A closer look at California (Figure 17) illustrates this tension with particular clarity: despite being one of the most seismically active regions in the world, the Bay Area and Southern California remain dense hubs of data center activity.

Rather than relocating to safer but less connected areas, operators appear to rely on engineering solutions like seismic bracing, redundancy in power supply, multiple fiber entry points, to mitigate risk *ex post*, rather than avoiding it *ex ante*. This observation confirms what Baudry (2015) described as a structural contradiction in site selection practices: while natural hazards are recognized as a constraint, they are often bracketed out when weighed against other priorities such as market access, connectivity, and fiscal incentives.

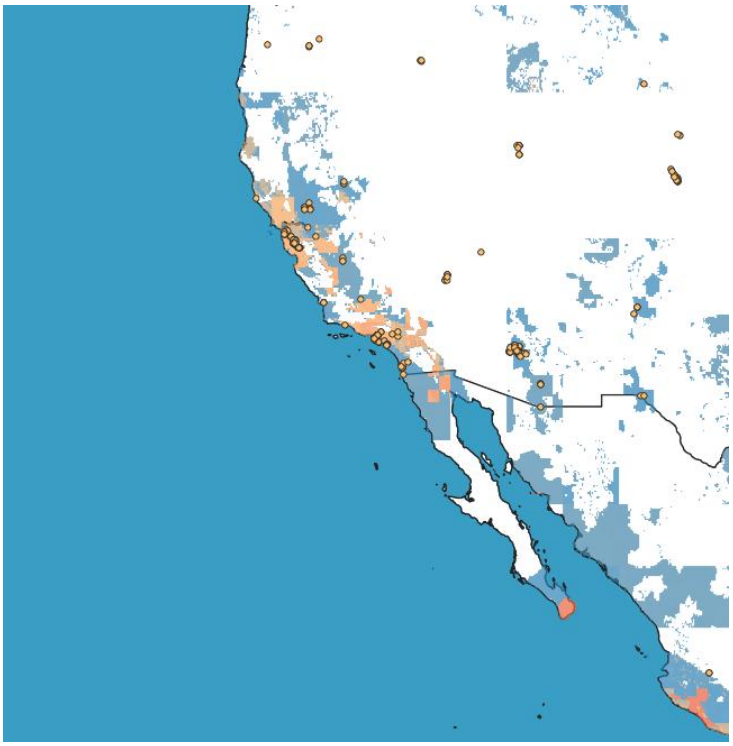

Figure 17 - California Multi Hazard Map

Placed within this broader perspective, hazard exposure emerges not as a determinant but as one variable negotiated within a hierarchy of competing factors. The choice to locate in high-risk regions is not irrational: it reflects the spatial coincidence of demand, connectivity, and political-economic incentives with hazard zones. For instance, California, Florida but also the Tokyo region in Japan embody precisely this trade-off: they are simultaneously global economic centers, network interconnection points, and high-risk environments. This paradox underscores the extent to which the geography of the cloud cannot be understood solely through physical variables; rather, it reflects the negotiated interplay between risk, resilience, and infrastructural imperatives.

To complement this picture, a second layer of analysis was introduced by incorporating population density data. For this purpose, NASA's Gridded Population of the World, Version 4 (GPWv4) was used (CIESIN 2018). GPWv4 provides global raster estimates of human population density at a 1-km resolution, based on national census data adjusted to UN standards. Using QGIS, data center locations were sampled against this raster to determine the degree of coincidence between infrastructural siting and concentrations of human population. The rationale for this step is straightforward. Data centers are demand-driven infrastructures: their primary function is to serve users, institutions, and

businesses. While climatic suitability and hazard avoidance may provide technical advantages, latency and service efficiency impose hard spatial constraints. Locating close to population centers minimizes the physical distance that data must travel, reducing latency and enabling efficient service delivery. In this sense, population density acts as a proxy for digital demand, allowing us to test whether the global distribution of data centers mirrors the geography of major urban and economic centers.

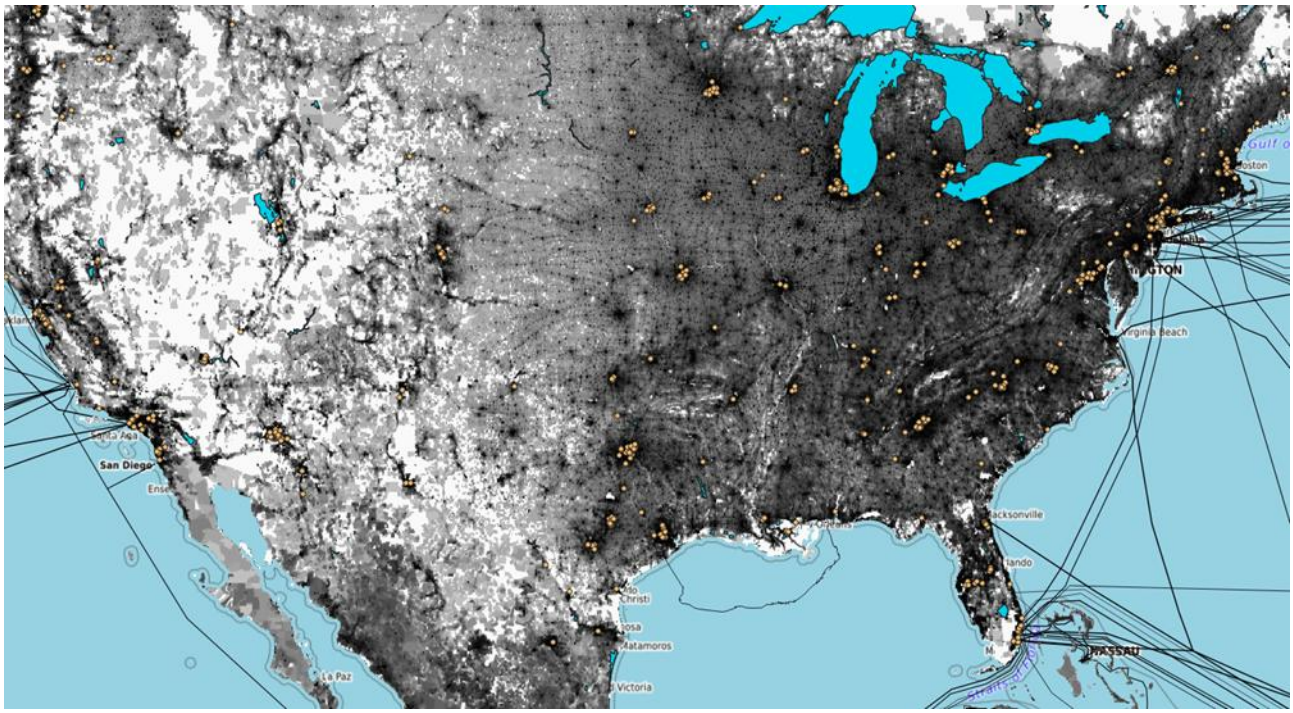

Figure 18 - Population Density and Datacenter Location USA

The overlay of GPWv4 population data with data center locations reveals a strong spatial correspondence. This correspondence is perhaps most evident when zooming in on the United States (Figure 18). Here, data centers closely mirror the distribution of population density, with heavy concentrations in the northeast, around the Great Lakes, and along the Pacific and Gulf coasts. The effect is not merely correlation but causation: operators prioritize proximity to dense markets to reduce latency, ensure redundancy, and capture the benefits of colocation with existing economic infrastructures.

Taken together, the hazard and population overlays highlight the central paradox of data center geography. On the one hand, technical discourse emphasizes the need to minimize environmental risk, and indeed some regions such as Scandinavia are marketed precisely on their climatic stability and renewable energy endowments. On the other hand, the empirical distribution of facilities reveals

that population density and market access consistently outweigh hazard avoidance. Facilities remain clustered in earthquake-prone California, cyclone-exposed Southeast Asia, and flood-prone northern Europe, not because risks are ignored but because they are deemed acceptable in light of infrastructural and economic imperatives.

From maps to models: probing correlates of siting decisions

The descriptive maps already establish two recurrent patterns: a strong clustering of facilities in a handful of techno-economic cores, and a visible attraction toward temperate belts. To move from pattern to mechanism, without any claim to causal identification, these visual regularities were translated into a simple, transparent statistical framework. A uniform analytical grid was imposed on the global dataset, and three theoretically salient covariates were derived for each cell. Local demand was proxied by the summed population count (GPWv4, 2.5′ resolution); operating conditions were proxied by mean annual temperature (WorldClim 2.1 BIO1, converted from tenths of °C to °C); and environmental exposure was proxied by a composite multi-hazard score (SEDAC Global Multihazard Frequency and Distribution). Raster values were aggregated to the grid through exact zonal extraction, while data-center points were intersected with the same grid to obtain the count of facilities per cell. The result is a cell-by-cell dataset linking the intensity of deployment to population, climate, and hazard exposure on a common spatial footing.

On this basis, an ordinary least squares model was estimated in the form

$$n_{dc} = \beta_0 + \beta_1 \cdot p\text{opulation} + \beta_2 \cdot t\text{emperature} + \beta_3 \cdot h\text{azard} + \varepsilon$$

treating the exercise as exploratory rather than explanatory. OLS was chosen for its interpretability and because diagnostic tests indicated negligible multicollinearity (all VIFs close to 1). While the dependent variable is technically a count and displays a heavy concentration of zeros, OLS was retained here as a deliberately simple and transparent specification. This choice does not aim at providing the most efficient estimator but rather at producing coefficients that are straightforward to interpret and consistent with the descriptive purpose of the analysis. More sophisticated count-data models could be applied in future robustness checks, yet the baseline OLS already suffices, in the author view, to illustrate the direction and relative weight of the main covariates.

The estimates, reported in Figure 19, are consistent with the narrative emerging from the maps. Population is positively and strongly associated with the number of facilities per cell, confirming that

data centers gravitate toward dense demand basins. Temperature enters with a negative coefficient, indicating a systematic penalty for warmer climates: facilities are less likely to be sited as ambient temperatures rise, a result that aligns with engineering practice whereby cooler environments reduce the energy costs of cooling. By contrast, the composite hazard score is statistically indistinguishable from zero once population and temperature are held constant. In other words, exposure to floods, earthquakes, or storms does not appear to deter siting decisions in any systematic way. Model fit is modest (adjusted R^2 around 0.05), which is not surprising given the complexity of the phenomenon and the deliberately parsimonious specification.

Table 1: Linear regression: number of data centers per grid cell

Variable	**Estimate**	**Std. Error**	**p-value**
Intercept	0.565	0.101	$< 0.001^{***}$
Population	3.14×10^{-7}	1.84×10^{-8}	$< 0.001^{***}$
Temperature	-0.330	0.055	$< 0.001^{***}$
Hazard Score	-0.00014	0.00094	0.884
Variance Inflation Factors (VIF):			
Population = 1.055	Temperature = 1.036	Hazard Score = 1.033	
Observations	5,943		
R^2	0.0489		
Adjusted R^2	0.0484		
Residual Std. Error	3.465 (df = 5939)		
F Statistic	101.8 ($p < 0.001$)		

Figure 19 - Linear Regression

Substantively, two readings follow. First, the positive population effect lends empirical support to the idea that data centers are not neutral service utilities but anchor institutions embedded in dense urban-economic systems. Second, the temperature effect corroborates the existence of a climatic pull, consistent with the industry's emphasis on energy efficiency and the extension of "free-cooling" envelopes. The null effect of hazard is also in line with the literature: at a global level and with this kind of coarse index, natural hazards appear less as determinants of siting than as constraints that operators actively manage through engineering redundancies, insurance, and contractual risk transfers. This explains why facilities are often located in hazard-prone areas whenever other

advantages like proximity to demand, fiscal incentives, or network connectivity outweigh environmental vulnerability. Two qualifications are necessary before interpreting magnitudes too literally. Aggregation choices matter: different grid resolutions would reweight urban peripheries and transport corridors, potentially altering coefficients. More importantly, the three covariates employed are blunt instruments relative to the multidimensional decision problem operators face. Factors such as electricity prices and grid headroom, renewable energy availability, fiscal and regulatory incentives, fiber backbones and IXPs, land markets, permitting velocity, and path-dependent clustering almost certainly explain most of the residual variance. Finally, the dependent variable's distribution suggests that complementary count-data or spatial models would be more appropriate for robustness checks. In this sense, the OLS model should be read as a baseline: interpretable, transparent, but deliberately modest in scope.

With these caveats in mind, the regression provides a useful bridge between descriptive cartography and theoretical expectations. It quantifies the pull of population, corroborates the climatic signal, and shows that "risk" is less a deterrent than an element managed within infrastructural strategies. Taken together, these findings lend partial confirmation to the second guiding hypothesis. While siting decisions do reflect a balance between environmental opportunities and constraints, the balance is asymmetric: climatic suitability exerts a measurable influence, whereas hazard exposure is tolerated when offset by market and connectivity advantages. Geography, therefore, does not dictate outcomes in a deterministic sense, but it reappears persistently in the global footprint of the cloud.

Conclusions

The analysis carried out in this chapter has empirically demonstrated that cyberspace, far from being an ethereal or placeless domain, is deeply and enduringly anchored in geography. The persistent metaphor of the cloud as an immaterial space dissolves once infrastructures are brought into focus: submarine cables, landing stations, and data centers are the indispensable backbone of digital interconnection. Their distribution follows logics that are spatial, political, and strategic. Far from being evenly spread, they concentrate in specific regions, reproduce historical hierarchies, and generate new importance to old geographic chokepoints exposing vulnerability and centers of control.

The historical reconstruction traced a long continuity: from the imperial logics of the nineteenth century, through the Cold War's consortia and redundancy strategies, to the liberalized fiber-optic market. Across these phases, infrastructures of communication were never neutral. They were designed, routed, and secured according to political rationales and strategic imperatives, inscribing

power relations into the very geography of global connectivity. The empirical analysis, based on GIS and network methods, further confirmed these dynamics. Submarine cables converge on a limited set of routes and landing points, creating infrastructural hierarchies and positional advantages for a few states. Network centrality measures highlighted the extent to which global connectivity depends on a small number of actors functioning as hubs or brokers, magnifying geopolitical relevance through infrastructural positioning. The focus on data centers confirmed the same principle: geography matters. The mapping exercise revealed spatial clustering in a handful of techno-economic cores, while regression analysis quantified the pulls of demographic demand and climatic suitability. Population density increases the likelihood of hosting facilities, while lower temperatures provide an operational advantage. Natural hazard exposure, by contrast, does not exert a systematic deterrent effect at this scale, confirming that operators tend to manage risk rather than avoid it, through engineering redundancies, insurance, and governance arrangements. Although the model explains only a modest share of the variance, its interpretive value lies in showing the expected direction of key relationships and corroborating the visual evidence of concentration and climatic preference.

Yet, this account remains partial. To complete the territorial skeleton of cyberspace, one would also need to examine satellite ground infrastructure, which provides another essential layer of connectivity. On average, satellites transmit only around five percent of global voice and data communications, but this figure conceals significant geographical asymmetries. Landlocked states, or countries unable to attract substantial investment in submarine and terrestrial cabling, rely on satellites far more extensively. Despite their importance, satellite systems remain structurally disadvantaged compared to fiber-optic cables: they are about five times slower due to the long distances to geostationary orbit, offer only 0.3% of the capacity of a modern submarine cable, and are roughly fifty times more expensive per megabit. Their operational lifespan is shorter (around ten years versus up to twenty-five for cables), and their deployment requires high upfront investments and long production times, often resulting in equipment that is technologically outdated by the time it enters service. Signal quality is also more unstable, prone to interference and latency issues, which further limits their competitiveness with cable-based infrastructures. At the same time, recent technological developments invite reflection. Low Earth Orbit (LEO) constellations, such as *Starlink*, depart from the geostationary model and promise to reduce latency by positioning thousands of satellites in much closer orbits. Their architecture relies on a dense mesh of mobile ground terminals and inter-satellite links, which could, in principle, mitigate some of the rigidities and bottlenecks of traditional terrestrial infrastructures (Stovall 2025). If fully realized, these systems may loosen the dependence on submarine chokepoints and cable landings, introducing a more flexible form of connectivity. Beyond technical performance, they also carry important geopolitical consequences.

Unlike submarine cables and terrestrial landing points − fixed, more or less visible, and thus vulnerable − LEO constellations introduce mobility and redundancy. The strategic relevance of this shift was already demonstrated during the Russian invasion of Ukraine, when Starlink terminals were rapidly deployed to sustain both civilian and military communications under conditions of infrastructural disruption (The Economist 2025). In this sense, satellite constellations embody not only a technological alternative but a novel instrument of geopolitical power. Nonetheless, skepticism is warranted. The scale of investment required, the regulatory and geopolitical hurdles, and the physical challenges of maintaining massive constellations in orbit suggest that these technologies, while promising, are unlikely in the near term to displace the entrenched dominance of fiber-optic systems. For now, however, they remain a complementary rather than substitutive infrastructure, but an in depth analysis of satellite systems for telecommunications goes beyond the aim of this work (on this see for instance: Labrador, 2025; Stovall, 2025)

To conclude, the chapter has shown that the geography of cyberspace is not accidental but structurally constitutive. Submarine cables, landing points, data centers, and potentially satellite bases compose a profoundly territorial architecture of digital connectivity. Geography reappears here not as a background condition, but as an active force shaping infrastructural siting, strategic dependencies, and geopolitical hierarchies. The empirical findings reinforce the central claim: the infrastructures of which cyberspace is made of are “tremendously territorial” and that geographical and topographical factors shapes cyber interconnectivity in a wide variety of ways. They inscribe flows of information into seabeds, coastal chokepoints, terrestrial hubs, and orbital constellations, and in doing so they remind us that cyberspace cannot be abstracted from material geography.

Bibliography

Agnew, J., & Shin, M. (2025). Georgia on Their Minds: Rethinking the Role of Geographic Scale in U.S. Elections. SAGE Open, 15(2).

Amazon Web Services Institute. (2022). Accelerate public service transformation with the cloud: Security – Ukraine. Amazon Web Services.

Balestrieri, F., & Balestrieri, L. (2019). Guerra digitale: Il 5G e lo scontro tra Stati Uniti e Cina per il dominio tecnologico. Luiss University Press.

Balestrieri, F., & Balestrieri, L. (2024). Tecnologie dell’impero: AI, quantum computing, 6G e la nuova geopolitica del potere. Luiss University Press.

Bartels, A. (2011). Data Center Evolution: 1960 to 2000. Rackspace.

Baudry, K. J. (2015). Data center site search and selection. In H. Geng (Ed.), Data center handbook (pp. 87–104). Hoboken, NJ: John Wiley & Sons.

Besch, S., & Brown, E. (2024, May 9). A Chinese-flagged ship cut Baltic Sea internet cables. This time, Europe was more prepared. Carnegie Endowment for International Peace.

Bittencourt, A. (2025). EU Cloud Sovereignty – Emerging Geopolitical Risks. Unit8.

Blok, A., Nakazora, M., & Winthereik, B. R. (2016). Infrastructuring environments. Science as Culture, 25(1), 1–22.

Blondel, V. D., Guillaume, J.-L., Lambiotte, R., & Lefebvre, E. (2008). Fast unfolding of communities in large networks. Journal of Statistical Mechanics: Theory and Experiment, 2008(10).

Borgatti, S. P., Everett, M. G., & Johnson, J. C. (2018). Analyzing social networks (2nd ed.). SAGE Publications Ltd.

Bowker, G. C., & Star, S. L. (1999). Sorting things out: Classification and its consequences. Inside technology. The MIT Press.

Bratton, B. H. (2015). The Stack: On software and sovereignty. The MIT Press.

Bueger, C., & Edmunds, T. (2017). Beyond seablindness: A new agenda for maritime security studies. International Affairs, 93(6), 1293–1311.

Bueger, C., & Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. Contemporary Security Policy, 42(3), 391–413.

Burnett, D. R., & Berdan, K. (2024). To secure undersea cables, take lessons from the British Empire's All-Red Line. Proceedings, 149(5), 1,443. U.S. Naval Institute.

Burt, R. S. (1992). Structural holes: The social structure of competition. Harvard University Press.

Casini, L. (2020). Lo Stato nell'era di Google: Frontiere e sfide digitali. Mondadori Università.

Center for Hazards and Risk Research – CHRR - Columbia University, (2025) Center for International Earth Science Information Network - CIESIN - Columbia University, and International Bank for Reconstruction and Development - The World Bank. 2005-12-31. Global Multihazard Frequency and Distribution. Version 1.00. Palisades, NY. Archived by National Aeronautics and Space Administration, U.S. Government, Center for Hazards and Risk Research (CHRR)/Columbia University.

Center for International Earth Science Information Network – CIESIN – Columbia University. (2018). Gridded Population of the World, Version 4 (GPWv4): Population Density, Revision 11 [Data set]. Palisades, NY: NASA Socioeconomic Data and Applications Center (SEDAC).

Cerreti, C., Marconi, M., & Sellari, P. (2019). Spazi e poteri. Geografia politica, geografia economica, geopolitica. Laterza.

Ciaramella A., Roveda M., (2018) Data Center. Localizzazione, caratteristiche e prestazioni delle nuove fabbriche dati, Franco Angeli.

Dawwas, E. (2014). The evolution of GIS as a land use planning conflict resolution tool: A chronological approach. American Journal of Geographic Information System, 3(1), 38–44.

Deruda, A. (2024). Geopolitica digitale: La competizione globale per il controllo della Rete. Carocci.

Di Salvatore, J., & Ruggeri, A. (2021). Spatial analysis for political scientists. Italian Political Science Review/Rivista Italiana Di Scienza Politica, 51(2), 198–214.

DiCicco, Jonathan and Jack Levy (1999). "Power Shifts and Problem Shifts." Journal of Conflict Resolution, Vol. 43, pp. 675–704.

Douzet F., Pétiniaud L., Salamatian L., Limonier K., Salamatian K., Alchus T., Measuring the fragmentation of the Internet: The case of the Border Gateway Protocol (BGP) during the Ukrainian crisis, 12th International Conference on Cyber Conflict (CyCon), 2020.

Edwards, P. N. (2003). Infrastructure and modernity: Force, time, and social organization in the history of sociotechnical systems. In P. Brey, A. Rip, & A. Feenberg (Eds.), Technology and modernity: The empirical turn (pp. 185–226). The MIT Press.

Farrell, H., & Newman, A. L. (2019). *Weaponized interdependence: How global economic networks shape state coercion*. *International Security, 44*(1), 42–79.

Farrell, H., & Newman, A. L. (2023). *Underground Empire: How America Weaponized the World Economy*. New York, NY: Henry Holt and Company.

Fick, S. E., & Hijmans, R. J. (2017). WorldClim 2: New 1-km spatial resolution climate surfaces for global land areas. International Journal of Climatology, 37(12), 4302–4315.

Finn, T. (2017). The Zimmermann telegram and Room 40. Foreign Office Historians, The National Archives, Prime Minister's Office, 10 Downing Street.

Fleck, A. (2024) Which Countries Have The Most Data Centers? Statista.

Flint, C., & Zhu, C. (2019). The geopolitics of connectivity, cooperation, and hegemonic competition: The Belt and Road Initiative. Geoforum, 99, 95–101

Geng, H. (2015). Introduction. In H. Geng (Ed.), Data center handbook (pp. 1–14). Hoboken, NJ: John Wiley & Sons.

Geng, H. (Ed.). (2015). Data center handbook. Hoboken, NJ: John Wiley & Sons.

Gilli, A., Gili, M., Ricchi, A., Russo, A., & Carniel, S. (2024). Climate change and military power: Hunting for enemy submarines in warming oceans. Texas National Security Review, 7(2), 16–41.

Gleditsch, Kristian and Michael Ward (1999). "A Revised List of Independent States Since the Congress of Vienna." International Interactions, Vol. 25, pp. 393–413.

Gooding, M. (2024 21). Google launches heat recovery project at data center in Hamina, Finland: Waste heat will be used to warm up nearby homes and businesses. Datacenter Dynamics.

Government of Canada. (2018). National cyber security strategy. Government of Canada.

Government of France. (2017). Stratégie internationale de la France pour le numérique. Ministère de l'Europe et des Affaires étrangères.

Government of the United Kingdom. (2016). National cyber security strategy 2016–2021. HM Government.

Gray, C. S. (1996). A debate on geopolitics: The continued primacy of geography. Orbis, 40(2), 247–259.

Greg's cable map

Guzzini, S. (2009). On the measure of power and the power of measure in International Relations. Danish Institute for International Studies.

Hilary McGeachy (2022) The changing strategic significance of submarine cables: old technology, new concerns, Australian Journal of International Affairs, 76:2, 161-177.

Hillman, J. E. (2021). The Digital Silk Road: China's Quest to Wire the World and Win the Future. Profile Books.

Holt, j., & Vonderau, p. (2015). "Where the Internet Lives": Data Centers as Cloud Infrastructure. In L. Parks & N. Starosielski (Eds.), Signal Traffic: Critical Studies of Media Infrastructures (pp. 71–93). University of Illinois Press.

Judge, P. (2022). Drought-stricken Holland discovers Microsoft data center slurped 84m liters of drinking water last year: After the company and local authority said the facility would only need 12 to 20 million liters. Datacenter Dynamics.

Kadlecová, L. (2024). Cyber Sovereignty. The Future of Governance in Cyberspace. Standford University Press.

Kelly Kadera & Gerald Sorokin (2004) Measuring National Power, International Interactions, 30:3, 211-230

Kennedy, Paul M. "Imperial Cable Communications and Strategy, 1870–1914." English Historical Review 86, no. 341 (1971): 728–52.

Labrador, V. (2025). Satellite communication. In Encyclopædia Britannica.

Landoni E.M., Reflections over cyber-development and submarine cables, Rivista Geopolitica ISAG - Istituto Alti Studi in Geopolitica e Scienze Ausiliarie, Vol. IX 1-2, Roma, Edizioni Nuova Cultura, 2020.

Lavorio, A. (2023). Guardiani del Nord. Gli Stati Uniti e la geopolitica della crisi climatica nell'Artico. Milano University Press.

Lehto, M., Hummelholm, A., Iida, K., Jakstas, T., Kari, M. J., Minami, H., Ohnishi, F., & Saunavaara, J. (2019). Arctic Connect Project and cyber security control (ARCY) (Informaatioteknologian tiedekunnan julkaisuja No. 78/2019). University of Jyväskylä.

Limonier K., Douzet F., Pétiniaud L., Salamatian L., Salamatian K., Mapping the routes of the Internet for geopolitics: The case of Eastern Ukraine, First Monday, volume 26, number 5-3 May 2021.

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, *22*(3), 365–404.

Lomsadze, G. (2011, April 8). A shovel cuts off Armenia's Internet. The Wall Street Journal.

Long, M. L. (2023). Information warfare in the depths: An analysis of global undersea cable networks. Proceedings, 149(5), 1,443. U.S. Naval Institute.

Mahan, A. T. (1890). The influence of sea power upon history, 1660–1783. Little, Brown and Company.

Martinage, R. (2015). Under the sea: The vulnerability of commons. Foreign Affairs, 94(1), 117–123.

McNeill, J. R., and W. H. McNeill. 2003. The Human Web. A Bird's-Eye View of World History. New York, N.Y., and London: W. W. Norton & Company.

Mijani, N., Shahpari Sani, D., Dastaran, M., Karimi Firozjaei, H., Argany, M., & Mahmoudian, H. (2021). Spatial modeling of migration using GIS-based multi-criteria decision analysis: A case study of Iran. Transactions in GIS, 25(6), 2901–2919.

Mitchell, R. (2022, December 15). How Amazon put Ukraine's 'government in a box' — and saved its economy from Russia. Los Angeles Times.

Morel, C. (2023). Les câbles sousmarins. CNRS Éditions.

Morgus, R., & Sherman, J. (2018). The idealized internet vs. internet realities (Version 1.0): Analytical framework for assessing the freedom, openness, interoperability, security, and resiliency of the global internet. Cybersecurity Initiative, New America.

Mueller, M. (2017). Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace. Polity Press.

Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., & Macias, J. M. (2023). Cyber operations during the Russo-Ukrainian war: From strange patterns to alternative futures. Center for Strategic and International Studies (CSIS).

Munn, L. (2023). Technical territories: Data, subjects, and spaces in infrastructural Asia. University of Michigan Press.

Murray, W. E. (2006). Geographies of globalisation. Routledge.

Nalbach, Alex. "'The Software of Empire': Telegraphic News Agencies and Imperial Publicity, 1865–1914." In Imperial Co-Histories: National Identities and the British and Colonial Press, edited by Julie F. Codell, 68–94. Cranbury, NJ: Associated University Presses, 2003

Newman, M. E. J. (2006). Modularity and community structure in networks. Proceedings of the National Academy of Sciences, 103(23), 8577–8582.

Organski, A. F. K. and Jacek Kugler (1980). The War Ledger, Chicago: University of Chicago Press.

O'Brien, M. (2024, December 19). Ireland embraced data centers that the AI boom needs. Now they're consuming too much of its energy. AP News

O'Carroll, L. (2024, December 10). AI-fuelled cloud storage boom threatens Irish climate targets, report warns. The Guardian.

Parfitt, T. (2011, April 6). Georgian woman cuts off web access to whole of Armenia. The Guardian.

Payton, B. (2023). The rise and rise of the Nordic data centre industry. Infrastructure Investor.

Powell, P., & Smalley, I. (2024). What is hyperscale? IBM.

Saunavaara J, Salminen M, 2020. Geography of the global submarine fiber-optic cable network: The case for Arctic Ocean solutions. Geographical Review

Schmitt, C. (1991). Il nomos della terra nel diritto internazionale dello “Jus Publicum Europaeum” (E. Castrucci, Trans.). Adelphi. (Original work published 1950)

Sherman, J. (2021). The politics of internet security: Private industry and the future of the web. Atlantic Council.

Shin, M., & Agnew, J. (2011). Spatial regression for electoral studies: The case of the Italian Lega Nord. In B. Warf (Ed.), Revitalizing electoral geography (pp. 117–132). Routledge.

Solon, O., & Hatem, M. (2024, July 17). Damaged subsea cables repaired in Red Sea amid militant attacks on ships. Bloomberg.

Squier, G. O. (1900). The influence of submarine cables upon military and naval supremacy. Proceedings, U.S. Naval Institute, 26(4/96), 861–884.

Starosielski, N. (2015). The undersea network. Duke University Press.

Steed, D. (2015). The strategic implications of cyber warfare. In J. A. Green (Ed.), Cyber warfare: A multidisciplinary analysis (pp. 73–95). Routledge.

Stefanachi C., 2017 America invulnerabile e insicura – La politica estera degli stati uniti nella stagione dell’impegno globale: una lettura geopolitica, Vita e Pensiero.

Steinberg, P. E. (2001). The social construction of the ocean. Cambridge University Press.

Stephenne, N., Burnley, C., & Ehrlich, D. (2009). Analyzing spatial drivers in quantitative conflict studies: The potential and challenges of geographic information systems. International Studies Review, 11(3), 502–522.

Stovall, J. (2025). Starlink. In Encyclopædia Britannica.

Suffia G. (2018). Geopolitica delle cyberwars. Uomini e stati alla prova dello spazio digitale. Giuffrè Editore.

Sunak, R., “Undersea cables: indispensable, insecure”, (UK: Policy Exchange, 2017)

Tangalakis-Lippert, K. (2022, March 14). Amazon helped rescue the Ukrainian government and economy using suitcase-sized hard drives brought in over the Polish border: “You can't take out the cloud with a cruise missile”. Business Insider.

TeleGeography 2025. Submarine cable FAQs: Frequently asked questions.

The Economist. (2023, January 5). How Elon Musk’s satellites have saved Ukraine and changed warfare. The Economist.

U.S. Department of Homeland Security. (2018). Cybersecurity strategy. U.S. Department of Homeland Security.

U.S. Department of Justice. (2020, June 17). Team Telecom recommends that the FCC deny Pacific Light Cable Network system’s Hong Kong undersea cable connection to the United States. Office of Public Affairs.

Vanderbilt, T. (2010). Survival City: Adventures among the ruins of atomic America (Flex. ed.). University of Chicago Press.

White House. (2017). National security strategy of the United States of America. The White House.

Chapter III - Territoriality and Cyber Power: U.S.-China Rivalry a Comparative Analysis

Introduction and Methodological Framework

In the previous chapters we examined the liberal imaginary that shaped early thinking about cyberspace. Thomas Friedman (1999), the great prophet of globalization, asserted that the old geopolitical world, divided by a wall, gave way to a new one bound together by the marvel of the World Wide Web and portrayed that digital network as the foundations of a post-territorial order in which geography, sovereignty, and the traditional logics of geopolitical rivalry had lost their relevance. At the time, in fact, cyberspace was not only a technological novelty but also the emblem of a broader transformation of world societies as well as the international system. Connectivity was expected to dissolve political boundaries, empower individuals, and replace power politics with market dynamics. As we have seen, this narrative became central to the post-Cold War understanding of cyberspace. As demonstrated in Chapter II, however, this idea of a borderless world was largely illusory. Cyberspace was never detached from materiality: it has always relied on infrastructures whose geography and ownership carried strategic significance. The supposed “flatness” of the network concealed profound path dependencies, as the architecture of digital connectivity followed and reinforced earlier political and economic hierarchies. Far from abolishing geopolitics, global networks reproduced American predominance by embedding it into the arteries of global communication and economy. From the late 1990s onward, Information Communications Technologies (ICT) infrastructures began to be explicitly recognized as strategic assets. In the United States, this shift was gradual. Networks initially conceived as neutral channels for commerce and communication were transformed out of fear, starting in the immediate aftermath of the attacks of September 11, 2001, into instruments of surveillance and coercion. American agencies exploited the country’s privileged position at the core of global infrastructures to monitor, restrict, and redirect flows of information and capital. This way, cyberspace itself became an extension of state power, one in which territorial control was no longer expressed through physical borders, but through the ability to dominate infrastructures and the flows they enable globally. This was the era of the so called unipolar moment.

It is in this context that the rise of China as a technological competitor must be situated. The U.S. appropriation of infrastructures for geopolitical purposes revealed both the vulnerability created by dependency and the strategic value of digital control. Confronted with the American appropriation of

global infrastructures, China came to recognize that sustaining its rise as a peer competitor required more than economic growth and technological innovation. It required sovereignty. By observing how control over networks and infrastructures had translated into strategic power for the United States, Chinese policymakers concluded that remaining dependent on external systems would leave the country perpetually vulnerable. The logical response was to pursue a model of cyber sovereignty, embedding territorial logics into digital governance and developing direct control over infrastructures. In this sense, China's strategy reflects not simply a defensive posture, but a recognition that infrastructural control constitutes the very foundation upon which geopolitical parity in the digital age must be built. These initiatives signal a recognition that cyberspace is not a realm separated from geopolitics, but rather a central arena of geopolitical contestation. What was once described as a post-territorial order has thus evolved into a space where infrastructures are weaponized, jurisdictional boundaries are reasserted, and territorial strategies are embedded in the governance of the digital domain.

The purpose of this chapter is thus to analyze these dynamics through the case study of U.S.-China competition. By examining how both states embed territorial logics into cyberspace governance, the chapter seeks to assess the extent to which contemporary technological rivalry is structured by geography, infrastructural dependencies, and the territorial strategies that underpin the projection of cyber power.

A methodological clarification regarding the choice of the case study is in order. The United States and China are examined here not because they embody opposite models of cyberspace governance − democratic versus authoritarian − as suggested by much of the existing literature (see for instance Long 2023; Neuberger 2025), but because they constitute critical instances of states that combine both the capability and the intention to govern cyberspace infrastructures. Unlike smaller or less digitally integrated actors, both powers exercise direct influence over global digital infrastructures, articulate explicit national strategies for cyberspace, and employ those strategies as instruments of geopolitical competition. Their selection is not motivated by a concern for statistical representativeness, but rather by their paradigmatic value. As Flyvbjerg (2006, 232) convincingly argues, *paradigmatic cases* serve as prototypes that make the fundamental features of a phenomenon more visible, thereby generating conceptual and theoretical insights that extend beyond the case itself. This role of paradigmatic cases can be compared to what Kuhn (1987) described as "exemplars" in the natural sciences: concrete models or reference points that guide practice and understanding within a broader field of inquiry. Building on this perspective, it is important to note that strategies of case selection are not mutually exclusive. A single case can simultaneously be extreme, critical, and

paradigmatic, and it is precisely this overlap that provides such cases with exceptional analytical richness, allowing them to yield multiple perspectives and complementary insights. In this sense, the United States and China are treated here as paradigmatic cases of how territorial logics are embedded in cyberspace governance, illuminating structural dynamics that transcend the two countries themselves.

This choice, as just anticipated, departs deliberately from the conventional narrative that juxtaposes "democratic" and "authoritarian" cyberspaces. According to this framing, the United States is typically presented as the defender of an open, liberal, and market-driven internet, while China is depicted as the architect of a sovereign, closed, and state-controlled cyberspace (Mueller 2010; Polyakova & Meserole 2019). While such distinctions capture important differences − especially in the domestic sphere, where the relationship between state authority, corporate power, and citizens' rights diverges significantly − they risk obscuring a deeper structural reality: that the two powers converge substantially in their approach to the international and infrastructural dimensions of cyberspace governance. This decision is consistent with a realist understanding of international relations. Realist scholarship has long emphasized that the primary driver of state behavior lies not in regime type but in the structural pressures of the anarchic international system. As Waltz (1979) famously argued, the distribution of capabilities and the imperative of survival compel all states − democratic or authoritarian alike − to act according to similar strategic logics. Mearsheimer (2001) further reinforced this point by observing that democracies are no less prone to power maximization than autocracies when confronted with security imperatives. From this perspective, treating the United States and China reflects a theoretical position in which strategic imperatives outweigh domestic political differences, leading both powers to adopt comparable strategies of infrastructural control and cyber power projection.

At the global level, in fact, both the United States and China pursue strategies of infrastructural sovereignty, forms of data localization, and supply-chain control. Both resist foreign ownership of their critical infrastructures, encourage the re-shoring of strategic assets, and deploy infrastructural leverage in contexts of geopolitical rivalry. The main divergence lies in the institutional modalities through which these objectives are pursued. In China, the state directly supervises and disciplines major technology firms, integrating them into a broader authoritarian governance framework (Creemers 2017). In the United States, by contrast, the relationship between government and industry is less overtly hierarchical and is mediated primarily through partnerships and regulatory mechanisms rather than direct command. Yet, this distinction should not be overstated. As Zuboff (2019) and others have observed, American technology companies operate within a dense and intricate web of state influence. This is visible both in highly publicized episodes − such as Mark Zuckerberg's

testimony before the U.S. Senate − and in more subtle but pervasive dynamics like the phenomenon of *revolving doors* (Ghosh 2019), whereby elites circulate continuously between federal administrations and major firms such as Google, Microsoft, Amazon, and SpaceX. These mechanisms ensure a persistent alignment between corporate priorities and national strategic objectives. In times of crisis, war, or regulatory tension, technology companies have consistently adjusted their practices to comply with national security directives, demonstrating that their autonomy is structurally constrained. Thus, although the domestic arrangements differ, state-centric authoritarian oversight in China versus public-private entanglement in the United States, the outcomes at the international level are strikingly similar. Both powers − and this is the main thesis of this chapter − embed sovereign territorial logics into cyberspace governance by asserting jurisdiction over infrastructures, minimizing external dependencies, and projecting cyber power beyond their borders through infrastructure supply and control. The comparative value of their analysis therefore lies not in their alleged opposition, but in the convergence it reveals: two distinct political systems producing comparable practices of infrastructural sovereignty and digital territorialization. For these reasons the United States and China are treated here as paradigmatic cases of infrastructural sovereignty in cyberspace. Studying them sheds light on the broader structural dynamics by which states, regardless of regime type, embed territorial and spatial logics into the governance of the digital domain.

The analysis that follows is guided by the central question of this chapter: *to what extent does the pursuit of cyber power by major states translate into territorial and spatial strategies of cyberspace governance?* To answer this, the chapter develops a conceptual framework that translates the abstract idea of "territorial and spatial logics" into observable implications. These implications − ranging from the reshoring of infrastructures, to the resistance to foreign control, to supply of technology and infrastructure − provide the criteria by which the cases of the United States and China are assessed. By tracing these practices across both contexts, the chapter aims to demonstrate that the geopolitics of cyberspace is inseparable from geography, territory, and infrastructural strategies. For the purposes of this section, the expressions "territorial logics", "territorial strategies", and "territoriality" are used interchangeably to denote the ways in which states seek to assert spatial control and sovereignty over cyberspace through infrastructures, jurisdictional authority, and practices of spatial governance.

The central hypothesis here is that major powers, in their pursuit of cyber power, systematically resort to territorial and spatial strategies in cyberspace. These strategies, such as reshoring or friendshoring critical infrastructures, restricting foreign control, and supply ICT infrastructure, constitute observable practices through which power is exercised in the digital domain. Their recurrence

indicates that cyberspace is not a post-territorial environment, but one in which geography and spatial logics continue to shape state behavior. If corroborated by the empirical analysis of the United States and China, this hypothesis would also reinforce realist insights in international relations that posits that the pursuit of power is a constant across regime types, driven by the structural pressures of the anarchic international system. From this perspective, examining two powers often portrayed as political opposites allow us to assess whether their pursuit of cyber power converges on similar strategies. Such convergence would demonstrate that structural constraints play the decisive role in shaping how states govern cyberspace and project influence through digital infrastructures.

To evaluate this claim, the chapter employs, as said, observable implications as a tool for connecting abstract theoretical concepts with empirical evidence. As King, Keohane, and Verba (1994, pp. 28–29) have argued, theories are meaningful only insofar as they generate implications that can be observed in the empirical world. Observable implications function as bridge between theory and data: they specify what we should expect to find if the theoretical argument is correct. George and Bennett (2005) similarly stress that formulating such implications is indispensable to case study research, as it provides the criteria for identifying relevant evidence and for assessing whether theoretical expectations hold in practice. Thus, it is these observable implications that will guide the data collection, and that will help distinguish relevant from irrelevant facts.

Dimension	If territorial logics are embedded we would expect…	If territorial logics are absent we would expect…	Indicators / Evidence
1. Reshoring & Localization	States re-shore data centers, cloud services, and critical supply chains; adopt data localization laws; restrict foreign hosting of sensitive data.	States prioritize efficiency and cost; rely heavily on foreign infrastructure and globalized supply chains without strategic concerns.	Data localization laws; national cloud services; reshoring of critical supply chains; public subsidies for domestic hosting; relocation of data/assets from foreign to domestic facilities.
2. Resistance to Foreign Control	States block or regulate foreign ownership/operation of submarine cables, IXPs, data centers; prefer national or allied firms.	States allow foreign companies broad access to domestic infrastructure if economically advantageous.	Bans or restrictions of foreign services or infrastructures; prohibition of foreign control of key infrastructure; joint ventures only with national majority stake.
3. Supply of Technology and Infrastructure	States actively export digital infrastructures (submarine cables, 5G networks, cloud services, satellites) to third countries, seeking to establish spheres of influence and reduce rival access. Infrastructure supply becomes a tool of geopolitical alignment and dependency creation.	States allow global market competition to determine infrastructure provision abroad, without strategic selection of partners or exclusion of adversaries. Influence over third countries' digital ecosystems remains limited.	U.S.-backed Clean Network Initiative; bans on Huawei/ZTE in allied states; financing of submarine cables by U.S. (Google, Meta) or Chinese (Huawei Marine, China Unicom) firms; promotion of cloud/data centers in strategic regions; memoranda of understanding and digital partnerships framed as part of geopolitical alliances.

Figure 4 - Observable Implications of Territorial Logics in Cyberspace

Figure 4 summarizes the observable implications that translate the abstract notion of territoriality in cyberspace into empirical expectations. Three dimensions are highlighted. First, reshoring and localization, where territorial strategies are expressed in efforts to repatriate data centers, cloud services, and supply chains, while their absence is reflected in the prioritization of efficiency and reliance on foreign infrastructures. Second, resistance to foreign control, where territoriality appears in restrictions on foreign ownership and operation of infrastructures such as submarine cables, IXPs, and data centers, rather than adopting a permissive approach aimed at economic advantage. Third, supply of technology and infrastructure, where territorial strategies manifest in efforts by states to expand their sphere of influence through the export of digital infrastructures, platforms, and technological ecosystems, while simultaneously excluding their strategic competitors. In this perspective, cyberspace governance is not limited to domestic reshoring or defensive measures but extends outward, as powers seek to shape regional and global markets by offering financing, standards, and equipment to allied or dependent states. By contrast, in the absence of territorial logics, states would allow technology diffusion to follow market dynamics, tolerating competitor firms' presence in their own territory and abroad. Each of these dimensions is linked to concrete indicators − such as data localization laws, restrictions of foreign providers, and sanctions or infrastructural blockades − that allow us to trace whether and how territoriality is expressed in practice

The operationalization will be as follows. A coding rule will be used to specify dimension-specific necessary and sufficient indicators and assigns a trichotomous score (0 = absent; 1 = capacity/intent; 2 = territorial practice). For reshoring/localization, the necessary condition is the presence of binding authorities that re-embed critical ICT assets under domestic or allied jurisdiction; the sufficient condition is an implemented reduction of extra-bloc dependence (e.g., new in-jurisdiction capacity coming online, mandated in-jurisdiction processing of sensitive data). For resistance to foreign control, the necessary condition is a screening and control regime that explicitly covers core nodes of the national digital ecosystem; the sufficient condition is an enforced decision that changes control in practice (e.g., a blocked project or a denial/conditioning of operating rights). For external supply/projection, the necessary condition is the availability of state-backed outward instruments (export finance, development lending, diplomatic frameworks, or coordinated standards strategies); the sufficient condition is executed overseas digital infrastructure. Falsifiers − for example, permissive cross-border handling of sensitive data despite localization mandates, continued rival operation of core nodes after documented security externalities, or systematic non-execution of pledged projects − override any positive evidence and revert the code to 0. This design distinguishes declaratory authority from implemented practice, allows comparison across the different dimensions,

and supports a transparent, testable method consistent with established process-tracing approaches (Van Evera 1997, pp. 55–67; Bennett & Checkel 2015, pp. 17–20, 30).

This will allow to evaluate in all three dimensions whether and how the United States and China are implementing territorial practice and strategies to govern digital infrastructures and pursue cyber power. It is also important to clarify the epistemic status of the empirical analysis developed in this chapter. The structured comparison of the United States and China is designed primarily as an exploratory assessment of how territorial strategies manifest in practice, rather than as a definitive test producing final empirical confirmation. The evidence assembled here, drawn from policy documents, legal instruments, regulatory measures, and publicly observable initiatives, allows the chapter to trace patterns of convergence and to evaluate whether the specified observable implications are plausibly present across the two cases. Yet the analysis necessarily faces obvious limits. Policy domains evolve rapidly, many decisions and implementation details remain partially opaque or classified, and the available material captures a time-bounded "snapshot" rather than a closed universe of actions. For these reasons, the chapter should be read as providing a systematic, transparent baseline that substantiates the plausibility and relevance of the territoriality framework, identifies recurrent mechanisms and practices, and generates empirically grounded expectations for further research, rather than as delivering exhaustive measurement or definitive causal claims.

Before going further it is however necessary to carefully discuss the concept of *cyber power*, since it constitutes one of the analytical instruments through which this chapter will assess the strategic behaviour of states. Just as debates on power have long occupied a central place in international relations theory, the extension of those debates into the digital realm has generated a wide range of definitions, analytical frameworks, and controversies. Clarifying how cyber power is to be understood is therefore essential for both conceptual precision and methodological coherence.

In the broader field of political science, power has traditionally been conceived either as the possession of resources or as the ability to shape outcomes and influence the behaviour of others. Robert Dahl's (1957) classical formulation defined power as a relational concept: «A has power over B to the extent that A can get B to do something that B would not otherwise do». Later contributions, such as Barnett and Duvall (2005), broadened this view by distinguishing between different forms of power − compulsory, institutional, structural, and productive − highlighting that power can operate not only through direct coercion but also through the shaping of structures, norms, and discourses. These general debates provide the conceptual background against which cyber power must be situated. The emergence of cyberspace as a domain of political and strategic activity led to early attempts to apply these insights to the digital sphere. Kuehl (2009) defined cyber power as «the ability

to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power». Joseph Nye (2010), whose work on soft and hard power had already transformed debates in international relations, offered a similar definition: «the ability to obtain preferred outcomes by producing effects within cyberspace and by using cyber-enabled means». These formulations are deliberately broad, stressing that cyber power is relational and outcome-oriented, not merely a matter of technological assets or capabilities. Despite this broad consensus, the literature has developed competing interpretations regarding the scope and boundaries of cyber power. A narrow conception, common in policy debates and security studies, equates cyber power with the operational capacity to conduct cyber operations, whether offensive (espionage, disruption, sabotage) or defensive (protection, resilience, deterrence) (see for instance: Libicki 2009; Rid 2013; Locatelli 2013; Lilli 2021). From this perspective, cyber power is analogous to military power in the digital domain: it is measured by the sophistication of malware arsenals, the size of cyber commands, and the effectiveness of defense systems. Such an approach, while analytically clear, risks underestimating the broader political and economic dimensions of power in cyberspace. By contrast, a broader conception extends the notion of cyber power beyond operations to include governance, norms, and infrastructures. This work wants to emphasize that cyber power derives not only from the ability to launch cyberattacks but also from the authority to regulate access, to shape the rules of use, and to determine how information flows are structured even through physical architecture, as we saw in chapter II. In this view, power encompasses the ability to set technical standards, dominate platforms, and control the legal frameworks that govern digital interactions. A state that influences the direction of global internet governance institutions or compels corporations to comply with national directives is exercising cyber power even without launching a single cyberattack.

Between these two poles lies a growing recognition that cyber power is inherently multidimensional. It encompasses at least three levels: (1) operational − the conduct of cyber operations in peacetime and conflict; (2) institutional − the shaping of rules, norms, and standards that govern cyberspace; and (3) structural − the ability to manage dependencies, exploit vulnerabilities, and shape the environment in which digital interactions occur. While not all authors agree on terminology, there is a shared acknowledgement that cyber power cannot be reduced to a single dimension without losing sight of its complexity. A key implication of these debates is methodological. If cyber power is defined too narrowly, e.g. restricted to cyberattacks and defensive measures, it risks missing important forms of influence that are exercised through governance and infrastructural positioning. If defined too broadly, folding into it all aspects of digital economy and society, it risks becoming indistinguishable from general state power. The analytical challenge, therefore, is to adopt a definition that is sufficiently broad to capture the multiple dimensions of cyber power while sufficiently precise to

guide empirical inquiry. For the purposes of this chapter, and in order to avoid tautology, *cyber power* is understood in general terms as the capacity of a state to produce preferred outcomes in and through cyberspace, whether by offensive, defensive, regulatory or other means. This deliberately open definition does not assume *a priori* which mechanisms are the most decisive. Rather, it provides the analytical flexibility to examine empirically how different states pursue cyber power, and to assess whether territorial and spatial strategies constitute a central pathway through which cyber power is projected.

Reshoring, Localization and the Geopolitics of the Digital Supply Chain

The first dimension of territorial strategies in cyberspace governance is expressed through the retrenchment of infrastructures, supply chains, and critical technological capabilities. Whereas the globalization of the late twentieth century was premised on the dispersal of production and the erosion of territorial boundaries, the current phase of great power rivalry has restored the centrality of territory and sovereign control. Both the United States and China, though operating within distinct institutional settings, have embraced the logic that the ability to exercise authority over digital infrastructures and supply chains within their territorial orbit is indispensable to safeguarding autonomy and sustaining geopolitical competition. This marks a deliberate reversal of the earlier reliance on globalized interdependence: production and technological capabilities are no longer viewed primarily through the lens of efficiency, but rather through that of strategic location and jurisdictional control. In this sense, reshoring and the imposition of territorial data and infrastructure requirements mark a renewed assertion of sovereignty, as states either repatriate infrastructures physically or compel them to operate under their own legal authority or within allied spheres of control.

In the United States, the reorientation of digital and technological supply chains gathered momentum in the wake of mounting concerns about systemic dependencies on China, exacerbated by the disruptions of the Covid-19 pandemic. These concerns crystallized in the early 2020s, when Washington decisively shifted away from the liberal orthodoxy of globalized efficiency toward a security-driven industrial policy. A pivotal turning point was Executive Order 14017 on *America's Supply Chains* (The White House 2021), which mandated a comprehensive review of U.S. vulnerabilities in semiconductors, batteries, pharmaceuticals, and critical minerals. The report underscored that efficiency alone could no longer justify reliance on adversarial states for essential technologies, and instead reframed resilience and national security as paramount criteria in supply chain design (DOC & DHS, 2022). Treasury Secretary Janet Yellen's articulation of the "friend-shoring" doctrine in 2022 gave discursive clarity to this new orientation (DOT 2023). Globalization was no longer conceived as a universal web of interdependence but as a selective partnership among

trusted allies. The objective however was not autarky, but the relocation of sensitive supply chains into reliable jurisdictions so as to mitigate geopolitical risks while still retaining some benefits of international integration.

As Haglund (2024) has shown, this logic has deeper roots than commonly acknowledged. Already during the Second World War, Washington experimented with what he terms "amigo shoring": a plan to mobilize hemispheric partners to secure critical resources against German influence. The Inter-American Trading Corporation envisioned by the Roosevelt administration would have centralized the purchase and marketing of Latin American exports, shielding them from Nazi manipulation through trade and currency tactics. Although short-lived, this experiment marked an important Washington's attempt to take the security risk out of interdependence by, to use Haglund's (2024) words, «keeping multilateralism alive but on a slimmed-down geographical basis, so that the gains from trade structured according to the principle of comparative advantage might be directed more toward the cohort of America's friends (however defined), and away from its adversaries». The revival, in some sense, of this strategic repertoire in the twenty-first century reflects a broader transformation of U.S. grand strategy, in which geopolitics has displaced market rationality as the guiding principle of production. National Security Advisor Jake Sullivan (as cited in Haglund 2024) captured the essence of this shift in a landmark 2023 policy address. While avoiding Yellen's exact metaphor of friend-shoring, he emphasized that Washington's turn toward industrial policy was not a retreat behind protectionist barriers:

> «Our objective is not autarky – it's resilience and security in our supply chains. Now, building our domestic capacity is the starting point. But the effort extends beyond our borders. And this brings me to the second step in our strategy: working with our partners to ensure they are building capacity, resilience, and inclusiveness, too. Our message to them has been consistent: We will unapologetically pursue our industrial strategy at home – but we are unambiguously committed to not leaving our friends behind. We want them to join us. In fact, we need them to join us».

Sullivan's remarks capture how profoundly U.S. policy has shifted from the 1990s-2010s, when globalization and the "Washington Consensus" were celebrated as the zenith of economic rationality. Today, market efficiency has given way to resilience and sovereignty as guiding principles (on this see Chapter I). This reorientation no longer imagines a borderless global economy, but instead maps supply chains onto a landscape of national borders and trusted allies while excluding rivals. In this sense, "friend-shoring" introduces a spatial logic that assigns political meaning to territory: some places – physical spaces – become safe havens of cooperation, others sites of strategic risk. The return of such friend-enemy distinctions signals the reassertion of geo-politics at the very core of global

governance, with supply chains transformed into instruments of national security and infrastructural power.

The discursive shift toward *friend-shoring* found its most tangible expression in the institutionalization of a new U.S. industrial policy. Having reframed globalization as a geography of allies and adversaries, Washington moved to anchor this strategy in concrete legislative and financial instruments. The goal was not only to reduce exposure to Chinese-controlled supply chains but also to cultivate a resilient ecosystem of production under U.S. jurisdiction and within the orbit of trusted partners. This dual ambition − repatriating strategic capabilities at home while embedding allied economies into shared technological architectures − signaled the material codification of friend-shoring. The CHIPS and Science Act of 2022 (Congress 2022) represents the legislative centerpiece of Washington's attempt to reassert sovereign control over the material foundations of the digital economy. It is not simply a subsidy scheme, but the institutionalization of a new strategic doctrine in which technological infrastructures are treated as national security assets rather than neutral instruments of commerce. With a funding envelope of $52.7 billion, the Act combines direct incentives for semiconductor manufacturing (approximately $39 billion), research and development investments ($11 billion), and tax credits for private capital expenditures. The creation of the National Semiconductor Technology Center and the National Advanced Packaging Manufacturing Program signals a deliberate effort to rebuild not only production capacity but also the entire ecosystem of innovation, training, and standard-setting around semiconductors (Arcuri 2022). Unlike earlier industrial policies, which were often defensive or reactive, the CHIPS Act operates proactively: it seeks to restructure global supply chains by anchoring their most sophisticated segments within U.S. territory and allied jurisdictions. The Act's geopolitical design is evident in the so-called *national security guardrails* provisions (on this see also: Shivakumar et al. 2023). Companies benefitting from federal subsidies are barred from expanding or upgrading semiconductor capacity in «countries of concern» (Shivakumar et al. 2023), a designation aimed squarely at China (even though they include also Iran, Russia, and North Korea), for a period of at least ten years. In practice, this amounts to a legal codification of technological bifurcation: while firms like Intel, TSMC, Samsung, and Micron are encouraged to expand U.S. facilities with generous public support, they are simultaneously discouraged from deepening their presence in rival jurisdictions. This restriction is particularly salient in relation to China, which represents not only a major hub for global semiconductor production but also the largest single market for consumption of chips across multiple industries. For stakeholders, the implications are profound: compliance with the CHIPS Act guardrails could entail the forfeiture of billions of dollars in potential revenues and sunk investments in China, a market that has historically accounted for as much as one-third of global semiconductor demand. (Lovely 2023). This

linkage between domestic investment and external restriction reveals how the United States has weaponized its position in the global semiconductor ecosystem. On one hand, it is re-embedding the most critical infrastructures within secure borders; on the other, it is actively denying competitors access to those same infrastructures, thereby converting interdependence into a source of strategic leverage. The magnitude of implementation illustrates the structural nature of this shift.

Two years after the passage of the CHIPS and Science Act, the Biden-Harris Administration highlighted the extraordinary scale of investment and industrial transformation it had triggered (White House 2024). Since 2021, more than $395 billion in semiconductor and electronics-related investments have been announced, accompanied by the creation of tens of thousands of new jobs across the United States. The Department of Commerce's CHIPS Incentives Program has already signed preliminary agreements with fifteen companies in fifteen states, mobilizing over $30 billion in direct funding and $25 billion in loans, while leveraging hundreds of billions in private capital. These initiatives are not confined to the narrow promotion of chip fabrication, but they are embedded within a broader strategy aimed at restoring U.S. leadership in semiconductor manufacturing, expanding advanced packaging facilities, and positioning the United States to produce nearly 30 percent of global leading-edge chips by 2032, up from less than ten percent in 2021. Crucially, federal funding under the CHIPS Act has been tied not only to industrial investment but also to labor provisions, child-care requirements, and regional workforce development hubs, thereby linking the revival of high-tech production to the social and economic renewal of the nation. This integration of industrial policy with community-based measures projects an image of resilience, stability, and inclusive growth, qualities historically associated with the image of the "American way of life". In this sense, the CHIPS Act transcends the narrow category of industrial strategy. It constitutes a deliberate geopolitical project: one that re-anchors advanced manufacturing within U.S. territory, reasserts infrastructural sovereignty, and signals to allies and rivals alike that Washington is prepared to bear significant fiscal costs to secure supply chains and reinforce its technological primacy. Moreover, It complements the export controls imposed in October 2022 and tightened in 2023, which restricted China's access to high-performance chips and advanced lithography equipment. Thus, taken together, subsidies and controls form a double-edge sword: one side fosters domestic and allied innovation; the other constrains the technological upgrading of adversaries.

This synthesis marks a decisive rupture with the neoliberal orthodoxy that long governed global markets, where efficiency and cost minimization were prioritized over resilience and sovereignty, and where even competitors could be reframed as partners in a vision of "positive-sum" interdependence. By contrast, the CHIPS Act codifies an unambiguous geopolitical and geoeconomic logic: production

must be anchored in spaces subject to U.S. legal and political authority, while rivals are deliberately excluded from the commanding heights of the digital economy. More than an industrial initiative, it is a geopolitical statement that the age of hyper-globalization has ended, and that the spatial organization of production will henceforth mirror the map of strategic rivalries and alignments.

China's trajectory parallels and precedes that of the United States in recognizing infrastructural dependence as a strategic liability, but it has been articulated on different discursive bases. In fact, the narrative here was centered on *cyber sovereignty* and national rejuvenation. Since the early 2000s, Chinese policymakers have consistently framed control over digital infrastructures as integral to state sovereignty, linking it directly to both regime stability and developmental ambitions (Creemers 2017). As Deibert et al. (2010) already observed in their work *Access Controlled*, China's model of cyberspace governance has long emphasized the indivisible connection between infrastructures, political order, and geopolitical security. This logic was made visible at the infrastructural level through the construction of what has become known as the "Great Firewall of China" (GFW), launched in 2002 (Na 2024, p. 5). Over the following decades, Beijing devoted extensive resources to building one of the most sophisticated filtering systems in the world. As Deibert et al. (2010, pp. 466–506) note, the state undertook to «limit access to any content that might potentially undermine state control or social stability» by combining strict supervision of domestic media, delegated liability for online content providers, and the promotion of state-led narratives in online debate. The Great Firewall exemplifies how technical architectures can be mobilized as instruments of political sovereignty. Rather than relying on a single method of restriction, it operates through a layered system of control that reshapes the very geography of information flows. One layer consists of Domain Name System (DNS) tampering, where requests to resolve the address of a banned website are deliberately corrupted: users attempting to access such domains are redirected to false or empty addresses, making the site appear unreachable. Another layer involves Internet Protocol (IP) blocking, which prevents connections to servers whose addresses have been blacklisted, thereby cutting off access at the level of the network's basic routing system. These techniques, while common in various national filtering regimes, are supplemented in China by a particularly distinctive and intrusive practice: TCP reset filtering. Here, the content of data packets traveling through the network is inspected in real time. When the system detects politically sensitive keywords − whether in the message header or in its body it injects forged TCP reset packets into the stream. Because TCP is designed to terminate connections when such reset signals are received, the result is the immediate disruption of the communication, regardless of where the original content is hosted. In effect, this system transformed the Chinese internet into a bounded informational enclave: a national space shielded from unwanted external flows and governed through continuous state monitoring.

Far from being an *ad hoc* measure of censorship, the Great Firewall has served as a paradigmatic infrastructure of cyber sovereignty. It illustrates how the Chinese government materialized the principle that cyberspace, like land, sea, or airspace, must be subject to the territorial authority of the state. By embedding jurisdictional boundaries directly into the architecture of the internet backbone, China prefigured the broader strategic. This perspective was further crystallized in Xi Jinping's landmark speech at the 2015 World Internet Conference in Wuzhen, where he declared that «respecting cyber sovereignty» was one of the necessary pillar of international order in the digital age (Xi 2015).

This orientation was in fact already formulated the same year in May through the launch of *the Made in China 2025* strategy, which explicitly tied industrial modernization to national security. The plan described manufacturing as the «mainstay of the national economy, the basis on which the nation is established, an instrument of rejuvenation, and the foundation of a world power» stressing that without a strong manufacturing sector «there will be no country and no nation» (State Council 2025). It acknowledged China's vulnerabilities in «key and core technologies» and the «high dependence on foreign countries» for advanced equipment, calling for breakthroughs in strategic sectors such as integrated circuits, robotics, aerospace, high-speed rail, and new-generation information technologies. In this sense, *Made in China 2025* transformed longstanding concerns about technological dependence into a concrete roadmap, aiming not merely at economic upgrading but at securing sovereignty in the digital and industrial economy. By setting targets for China to become largely self-sufficient in advanced technologies and to emerge as a global leader in high-tech industries, *Made in China 2025* directly challenged the technological dominance of established powers such as the United States. It signaled, in fact, Beijing's intention to restructure global value chains in ways that reduced reliance on Western firms, while simultaneously projecting Chinese standards, products and platforms abroad. The ambition to cultivate "national champions" capable of competing on a global scale underscored that industrial policy was being mobilized as a tool of state power (Balestrieri and Balestrieri 2019). The U.S. response − ranging from tariffs during the Trump administration to bipartisan support for domestic reshoring initiatives like the CHIPS and Science Act that we just analyzed − reveals exactly how *Made in China 2025* was interpreted, namely not only as an economic plan but as a strategic threat to American primacy. In this way, the initiative showed clearly the overlap between industrial modernization and international rivalry, positioning technological sovereignty as a central battlefield in twenty-first-century geopolitics.

Another important step in this direction, so to see if the dimensions of territoriality is central in the Chinese institutional, legal framework and political framework around cyberspace and its

infrastructure, is to analyze the Cybersecurity Law of the People's Republic of China, adopted in November 2016 and entered into force on 2017. The law's opening provisions clearly articulate its intent: it was «formulated in order to ensure cybersecurity; safeguard cyberspace sovereignty and national security, and social and public interests; [and] promote the healthy development of the informatization of the economy and society» (Cybersecurity Law, 2017, Art. 1). By placing sovereignty at the center of its rationale, the law positioned digital infrastructures not as neutral instruments of economic modernization but as components of the state's territorial authority and national security apparatus. This territorial dimension was explicitly enshrined in the law's scope: it applies to «the construction, operation, maintenance, and use of networks, as well as to cybersecurity supervision and management within the mainland territory of the People's Republic of China» (Art. 2). In other words, cyberspace was redefined as a bounded domain, subject to the same spatial logic that governs physical territory. The internet, often idealized in the West as a borderless realm, was instead mapped and constrained onto China's territorial boundaries, transformed into a sovereign enclave where infrastructures and data must remain within the purview of state control. The law further consolidated this territorial logic through an expansive definition of state responsibility. Article 5 specifies that the state shall take measures to monitor, prevent, and handle cybersecurity risks and threats arising both «within and without the mainland territory» of China. This dual formulation underlines two critical dimensions: on the one hand, cyberspace is a domestic domain to be policed as rigorously as land or airspace; on the other, it is also a frontier through which external threats can penetrate, demanding proactive defense at and beyond the border. Perhaps the most consequential provision, however, was the introduction of data localization requirements. Article 37 stipulates that «operators of critical information infrastructure» must store personal information and «important data» collected within China inside the country's borders, and that any cross-border transfer of such data must undergo a state-conducted security assessment. This measure not only reasserted jurisdictional sovereignty over data flows but also transformed the geography of the digital economy: infrastructures and platforms operating in China could no longer treat data as a globally fungible resource, but instead had to align their architectures with the territorial imperatives of the Chinese state.

It is clear that this "territorialization" of cyberspace in China was not the result of a single legislative act but of a broader strategic convergence between industrial planning and legal codification. The *Made in China 2025* strategy, released in 2015, had already stressed the need to expand domestic data centers, cloud infrastructures, and indigenous information technologies as part of a push for technological self-reliance. By framing digital infrastructures as both economic assets and security imperatives, the plan made clear that the accumulation and processing of data could not remain

dependent on foreign providers or be dispersed across global jurisdictions. The 2017 *Cybersecurity Law* translated this strategic vision into binding legal obligations. On the one hand, *Made in China 2025* mobilized resources to build the physical backbone of sovereignty through new data centers, domestic cloud services, and a strengthened ICT supply chain; on the other, the *Cybersecurity Law* ensured that these infrastructures operated firmly under the authority of the Chinese state.

An additional step in consolidating China's vision of cyber sovereignty was taken with the adoption of the Data Security Law (DSL) in June 2021, which came into effect in September of the same year. Whereas the 2017 Cybersecurity Law had already established data localization requirements for «critical information infrastructure operators», the DSL broadened the scope by treating data itself as a strategic national resource. Article 1 states that the law was enacted «to regulate data processing activities, ensure data security, promote data development and use, protect the lawful rights and interests of individuals and organizations, and safeguard state sovereignty, security, and development interests» (DSL 2021, Art. 1). By explicitly linking data governance to sovereignty and national security, the DSL marked a further institutionalization of territorial logics in cyberspace. The law introduced a classification system distinguishing between «ordinary», «important», and «core» data, with the latter two categories subject to heightened scrutiny. Cross-border transfers of such data must undergo state-led security assessments (DSL 2021, Arts. 21–25), thereby placing the circulation of information flows firmly under government oversight. In this sense, the DSL transformed the geography of data management: digital platforms and firms operating in China could no longer treat information as a fungible commodity circulating freely across jurisdictions, but were compelled to align their practices with China's territorial and security priorities.

All these steps unequivocally reflect Beijing's determination to bind technological development to sovereign control. Industrial strategies provided the material infrastructure, while legal codification ensured that data remained subject to Chinese jurisdiction. In this way, the DSL reinforced the principle that sovereignty in cyberspace is not an abstract claim but a concrete regime of spatial regulation, embedding territoriality into the very circulation of digital information.

Taken together, the American and Chinese trajectories in this first dimension confirm that cyber power is increasingly grounded in territorial strategies. The United States has sought to re-embed production through friend-shoring and the CHIPS Act, while China has pursued technological self-reliance and legally codified data sovereignty through measures such as *Made in China 2025*, the Cybersecurity Law, and the Data Security Law. Despite their institutional differences, both powers converge on the recognition that infrastructures and data cannot be left to the contingencies of global markets: they must instead be secured within sovereign or allied jurisdictions. This convergence provides empirical

support for the argument that the retrenchment of supply chains and infrastructures is not merely an economic adjustment, but a geopolitical strategy through which states seek to transform territorial control into a source of cyber power.

Resistance and Projection: The Dual Logic of Territoriality in Global Digital Infrastructures

The second and third dimension of territorial strategies in cyberspace concern, respectively, the resistance to foreign control over critical infrastructures and the proactive export of such infrastructures abroad. Analytically, these phenomena are distinct: the first relates to defensive measures aimed at preventing external actors from dominating national digital ecosystems, while the second reflects an outward projection of influence through the provision of connectivity, platforms, and technological architectures to third countries. Yet, they are also intimately connected. The very need to ban, restrict, or regulate foreign infrastructures presupposes the expansionist drive of external powers, just as the attempt to export cables, data centers, or 5G networks to allied or dependent states is meaningful only insofar as rivals might do the same. For this reason, resistance and supply should be considered as two sides of the same geopolitical dynamic: the contestation of infrastructural power in cyberspace. This dual process has become visible in multiple arenas, from U.S.-led campaigns to exclude Huawei from 5G networks and block Chinese participation in transpacific cable projects, to Beijing's promotion of its own connectivity solutions across Africa, Latin America, and Southeast Asia. Whether through defensive prohibitions or proactive infrastructural diplomacy, these two powers are increasingly redefining the geography of digital interdependence, shaping not only their own territorial sovereignty but also the alignment of other countries within competing technological blocs.

A particularly significant case in the geostrategic dynamics of digital infrastructures is the controversy surrounding the Chinese companies Huawei and ZTE. This should be read in the broader anxieties of the United States about losing technological primacy in the transition to fifth-generation mobile networks and as Balestrieri and Balestrieri (2019, 94) observe, Washington perceived 5G not merely as another step in telecommunications, but as the very "open sesame" – the magical phrase in the story of *Ali Baba and the Forty Thieves* − of the digital revolution: the indispensable infrastructure for smart cities, the Internet of Things, artificial intelligence applications, and the interfaces that will define the future of human-machine interaction.

When Deloitte's 2018 report revealed that China had already achieved a striking lead in the density of 5G-ready infrastructure − 14.1 sites per 10,000 inhabitants compared to only 4.7 in the United

States − the sense of vulnerability deepened. In spatial terms the disparity was even more pronounced: 5.3 sites per ten square miles in China against a mere 0.4 in the United States (Deloitte 2018, 5). As the report stressed, «Since 2015, China outspent the United States by approximately $24 billion in wireless communications [..] Looking forward […] China and other countries may be creating a 5G tsunami, making it near impossible to catch up» (Deloitte 2018, 3). These figures appeared to confirm that American firms risked being overtaken at the infrastructural foundations of the next digital economy by state-supported Chinese champions. Security anxieties, however, were not limited to industrial capacity. Already in 2012, the U.S. House of Representatives Permanent Select Committee on Intelligence had issued a stark warning that Huawei and ZTE «cannot be trusted to be free of foreign state influence» and that their equipment could be used to «undermine core U.S. national-security interests» (House Intelligence Committee 2012, vi). The same year, the U.S.-China Economic and Security Review Commission emphasized that China's commercial IT sector maintained close ties with the People's Liberation Army, creating «a potential vector for state-sponsored or state-directed penetrations of the supply chains for microelectronics supporting U.S. military [and] civilian government» (2012, 10). These assessments consolidated the perception that the risks of Chinese 5G extended well beyond commerce: they struck at the heart of sovereignty and security.

As Balestrieri and Balestrieri (2019, 95–96) synthesize, American concerns coalesced around three interrelated dimensions. First, the persistence of what Washington saw as predatory practices: "copycat" strategies and forced technology transfer in joint ventures, regarded as a form of state-sanctioned intellectual property theft. Second, the specter of cyber-espionage, reinforced by congressional and commission reports pointing to Huawei and ZTE as potential vectors of state surveillance. Third, the strategic risk embedded in the 5G supply chain itself: whoever controlled the critical nodes of this infrastructure could condition, delay, or even block entire rival industries dependent on digital connectivity.

In response to these concerns, Washington progressively moved from warnings and reports to the adoption of binding legislative and regulatory measures. A turning point came with the 2019 *National Defense Authorization Act* (NDAA), which explicitly prohibited federal agencies and contractors from procuring equipment and services from Huawei, ZTE, and a handful of other Chinese firms designated as security threats (NDAA 2019, 6). This legal prohibition institutionalized the earlier suspicions voiced by Congress and security commissions, transforming them into enforceable restrictions across the federal apparatus. The Federal Communications Commission (FCC) subsequently reinforced this trajectory by classifying Huawei and ZTE as national security risks in

2020, thereby excluding them from the pool of firms eligible for subsidies to expand broadband infrastructure in rural America (FCC 2020). Together, these measures not only constrained Chinese participation in the domestic market but also signaled to private operators that reliance on such vendors entailed regulatory and financial penalties. At the international level, the Trump administration launched the *Clean Network* initiative in 2020, an explicit campaign to coordinate with allies and partners to exclude Huawei equipment from their 5G rollouts. Through a combination of diplomatic pressure, intelligence sharing, and promises of alternative financing, Washington sought to persuade countries such as the United Kingdom, Australia, and Japan to adopt restrictions similar to its own. As reported by Coy and Mathieson (2020) on Bloomberg, the initiative was described by senior officials as the equivalent of George Kennan's *Long Telegram* at the beginning of the Cold War, in which it appeared a first articulation of a comprehensive containment strategy against the Soviet Union. In this analogy, Huawei and other Chinese firms were cast as vectors of authoritarian expansion, while the Clean Network framed the defense of "trusted" digital infrastructures as a collective task for allied democracies. Although the degree of compliance varied across regions, the campaign revealed how infrastructural choices were no longer left to market efficiency alone but were redefined as matters of alliance cohesion and geopolitical alignment, another political line had been drawn on the planisphere.

In parallel, U.S. authorities expanded the scope of investment screening and export controls. The Committee on Foreign Investment in the United States (CFIUS) and the interagency Team Telecom increasingly scrutinized Chinese involvement in strategic projects, ranging from data centers to subsea cable landings on American shores. A prominent example was the *Pacific Light Cable Network*, a project initially designed to connect California to Hong Kong. In 2020, Team Telecom formally recommended that the Federal Communications Commission (FCC) deny the application for a direct connection to Hong Kong, citing «unacceptable national security risks to the United States' telecommunications infrastructure» (U.S. Department of Justice 2020).

Beyond restrictive measures, Washington also pursued a proactive strategy of infrastructural projection aimed at providing allies and partners with alternatives to Chinese vendors. This effort took multiple forms. At the industrial level, U.S. officials consistently promoted trusted suppliers such as the Scandinavian Nokia, Ericsson, and the South Korean Samsung as substitutes for Huawei in 5G rollouts (Coy and Mathieson 2020). While none of these companies are American, their integration into U.S.-led alliances underscored that what was at stake was less national ownership than alignment with a geopolitical bloc. By backing these alternatives, the United States sought to reassure partners that rejecting Huawei would not result in technological isolation but would instead

anchor them in a broader ecosystem of "trusted" connectivity. This proactive logic extended well beyond Washington's closest allies in Europe. Conscious that the contest over digital infrastructures was global in scope, U.S. policymakers directed attention also to Africa and Latin America, regions where Chinese firms had secured dominant positions through bundled loans, concessional financing, and turnkey projects (see Hillman 2022). Here, Washington sought to rebalance the playing field by mobilizing its own financial instruments. The U.S. International Development Finance Corporation (DFC) and the Export-Import Bank (Exim Bank) were mandated to extend loans and guarantees for telecommunications infrastructures. In 2020, for instance, the DFC announced support for a 5G rollout in Ethiopia, explicitly framed as an alternative to reliance on Chinese vendors (DFC 2020). Likewise, Exim Bank listed telecommunications among the priorities of its "Transformational Exports Program", conceived to reduce dependency on Chinese credit and equipment by underwriting projects involving U.S.-aligned suppliers (Exim Bank 2020).

In parallel with these financial instruments, Washington also placed growing emphasis on the geostrategic role of undersea cables. This was made explicit in the *Joint Statement on the Security and Resilience of Undersea Cables* (U.S. Department of State 2024a), which underscored that the integrity of these infrastructures is essential to the stability of the global digital economy and must therefore be protected against risks of espionage, sabotage, or excessive dependence on strategic competitors. The statement also emphasized the importance of diversifying suppliers and ensuring that new systems are developed in cooperation with trusted partners, thereby embedding political alignments into the very architecture of digital connectivity. This approach materialized in concrete initiatives, particularly in regions where Chinese actors had consolidated a dominant presence. In Latin America, Washington celebrated for instance the inauguration of the first subsea cable directly linking Chile with Australia, a Google project welcomed by the U.S. as a milestone in fostering «secure and resilient connectivity» between democratic partners (U.S. Department of State 2024b). By supporting alternative routes of interconnection, the United States signaled its determination to provide regional partners with options beyond Chinese-backed infrastructures and to anchor them into a U.S.-aligned technological sphere. In Africa, this strategic competition overlapped with large-scale projects such as Google's *Equiano* cable and Meta's *2Africa* system. While designed as commercial ventures, these initiatives can also be read − as Balestrieri and Balestrieri (2019, 105) suggest − in terms of a neocolonialism, binding the continent's digital future to American technology companies while simultaneously distancing its networks from Chinese providers. From this perspective, this projects were not only channels of connectivity but also instruments of geopolitical alignment, shaping long-term dependencies and reconfiguring Africa's position within competing technological network.

Standard-setting added a further layer to this outward projection. Through institutions such as the National Institute of Standards and Technology (NIST), participation in the 3rd Generation Partnership Project (3GPP), the Quad framework, and transatlantic dialogues, Washington consistently emphasized the need to embed security and trust into technical standards. This logic was first articulated in the *National Strategy to Secure 5G* (The White House 2020), which made U.S. leadership in international standard-setting organizations a central line of effort to guarantee that next-generation networks would reflect "trusted vendor" principles. The subsequent *Implementation Plan* coordinated by NTIA (2021) translated this vision into agency-level tasks, from increasing U.S. participation in standards development organizations to fostering security benchmarks that implicitly excluded untrusted suppliers. The priority given to standard-setting was later expanded in the *U.S. Government National Standards Strategy for Critical and Emerging Technologies* (The White House 2023), which explicitly linked participation in international standards bodies to safeguarding national security and maintaining technological leadership. As this Strategy put it this dimension is of fundamental importance since in the eyes of the White House:

> Strategic competitors are actively seeking to influence international standards development, particularly for CET, to advance their military-industrial policies and autocratic objectives, including blocking the free flow of information and slowing innovation in other countries, by tilting what should be a neutral playing field to their own advantage. The United States must renew our commitment to the rules-based and private sector-led approach to standards development, and complement the innovative power of the private sector with strategic government and economic policies, public engagements, and investments in CET. By supporting our unrivaled innovation ecosystem and related international standards development as part of a modern industrial strategy, we can ensure that CET are developed and deployed in ways that benefit not only the United States but all who seek to promote and advance technological progress. (The White House 2023).

In July 2024, the White House and NIST released an *Implementation Roadmap* for the NSSCET, aimed at mobilizing resources to increase allied coordination, prevent undue influence from strategic competitors, and strengthen U.S. presence in key organizations (NIST 2024; White House 2024). This document made clear that standards are not neutral technical conventions but instruments of geopolitical alignment: by investing in sustained participation, coordinating with allies, and excluding high-risk actors, Washington sought to ensure that the technical protocols governing critical and emerging technologies would embody political values of security, trust, and transparency. In this sense, the promotion of "trusted" standards should be understood less as a technical exercise of interoperability and more as a strategic effort to shape the architecture of global markets, creating

lock-in effects that bind partners to a U.S.-aligned ecosystem while structurally constraining the spread of Chinese alternatives. As Balestrieri and Balestrieri (2024, 107) note «If technology cements empires, as religion did in the sixteenth century, standards are the dividing line that distinguishes and binds technological professions of faith», especially since shifting suppliers after adopting one standard regime entails prohibitive costs. By codifying trust and resilience as criteria in standards, the United States sought to universalize its strategic preferences, ensuring that partners in Africa, Latin America, and Europe would converge on frameworks incompatible with Chinese vendors. Taken together, the U.S. approach to infrastructural sovereignty reveals a dual logic. On the one hand, Washington sought to insulate its domestic digital ecosystem through investment screening, export controls, and restrictions on high-risk suppliers. On the other, it projected its influence outward by financing alternatives, promoting trusted vendors, embedding his security criteria into international standards, and encouraging (or forcing) allies to align their infrastructural choices with U.S. strategic preferences. This duality underscores that resistance and projection are not separate trajectories, but mutually reinforcing dimensions that U.S. adopted to implement their cyber power. The overall outcome was the consolidation of a U.S.-led technological bloc, evoking maybe in more nuanced form the geopolitical divides of the Cold War, where infrastructural choices became markers of alliance and strategic alignment rather than mere matters of market efficiency.

On China's side, beyond the already discussed measures of data localization and cybersecurity, Beijing has long relied on institutional arrangements that structurally constrain the role of external actors. Foreign companies operating in sensitive sectors such as cloud computing, telecommunications, and data services are required to do so through joint ventures with domestic partners, ensuring that ownership, management, and ultimately jurisdictional authority remain aligned with Chinese sovereignty (State Council 2016, Art. 6; NDRC & MOFCOM 2021). Microsoft's Azure and Amazon Web Services, for instance, are operated in compliance with Chinese regulations, using data centers located within China (see for example: Microsoft 2023). Similarly, the *Measures for Cybersecurity Review* empower the Cyberspace Administration of China to block acquisitions, procurement contracts, or listings abroad if deemed to endanger national security (CSET 2021). Together, these mechanisms prevent foreign providers from exercising autonomous control over the digital foundations of the Chinese economy, subordinating their market presence to state oversight and domestic corporate intermediaries.

However, China's strategy in cyberspace cannot be reduced to domestic measures of data localization and restrictions on foreign control. While these policies ensure that critical infrastructures remain under sovereign authority and ensure that critical networks and data remain insulated from the "rest"

of the global network, Beijing – following the path of laid by the United States in their quest for creating a globalized liberal world − has also pursued an external agenda aimed at reshaping global digital connectivity. This outward projection finds its institutional expression in the famous Digital Silk Road (DSR). The first official step in this direction appeared in the 2015 policy document *Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road*, which called for the development of an *Information Silk Road* through cooperation in cross-border optical cables, satellite networks, and information sharing (NDRC, MFA & MOFCOM 2015). Two years later, this agenda was formalized with the proper launch of the DSR at the 2017 Belt and Road Forum, where China announced the *Initiative for Belt and Road Digital Economy International Cooperation* and signed memoranda of understanding several countries to promote collaboration in cloud computing, big data, artificial intelligence, and the Internet of Things. To recall Chinese president Xi Jinpin: «We should […] intensify cooperation in frontier areas such as digital economy, artificial intelligence, nanotechnology and quantum computing, and advance the development of big data, cloud computing and smart cities so as to turn them into a digital silk road of the 21st century» (Xi 2017).

Since then, the DSR has evolved into a central pillar of the Belt and Road Initiative. According to the 2023 White Paper *The Belt and Road Initiative: A Key Pillar of the Global Community of Shared Future*, by the end of 2022 China had concluded formal cooperation agreements in the digital domain with seventeen states, alongside numerous frameworks for e-commerce and digital governance (State Council Information Office 2023). These institutional commitments demonstrate that the DSR is not a rhetorical supplement to the Belt and Road but a carefully articulated strategy of infrastructural statecraft. Through it, Beijing extends the principle of cyber sovereignty beyond its territorial borders, embedding Chinese technologies, platforms, and standards into the infrastructures of partner countries. In this way, the Digital Silk Road constitutes the external complement to China's consolidation of a separate (from the American one) cyberspace, transforming cables, cloud services, and standards into instruments of geopolitical influence, pursuing the creation of a different center of the network. In this regards, one of the most tangible element of this strategy lies in the construction and financing of subsea cable systems. By laying and managing cables that connect Asia, Africa, Europe, and South America, China reduces its dependence on foreign carriers while embedding its own presence into the arteries of global connectivity. As Hillman (2021) has argued, this path recalls the logics of Britain's *All-Red Routes* (seen in Chapter II) in the late nineteenth century. Just as the British Empire sought to construct a cable network that touched only imperial territories in order to minimize vulnerability to disruption, China is seeking to assemble a high-capacity, high-speed network that bypasses Western-controlled chokepoints. The analogy underscores that these

infrastructures are not neutral conduits of information, but territorial instruments through which states reshape the geography of global communications.

The institutional vehicle for this expansion was Huawei Marine, created in 2008 through a joint venture with the U.K.-based Global Marine (Partington 2012). The company's development illustrates the characteristic features of Chinese infrastructural project: initial reliance on foreign expertise, sustained learning through joint ventures, and the gradual acquisition of independent capabilities, underwritten by state financing. Within its first decade, Huawei Marine participated in more than one hundred projects, laying sufficient cable to encircle the globe and consolidating China's position as an emerging power in the subsea domain. After its acquisition by Hengtong Group in 2019, the rebranded HMN Technologies became the world's fourth-largest cable producer, with ambitions of achieving full end-to-end control over manufacturing, installation, and repair. Several flagship projects reveal both the scale and the strategic orientation of China's cable diplomacy (see Deruda 2024). The South Atlantic Inter Link (SAIL), completed in 2018, was the first direct connection between South America and Africa. Despite weak commercial demand, the project was realized through a package of state-backed loans, ownership stakes by China Unicom, and government-to-government agreements with Cameroon. In strategic terms, the cable provided China with a transatlantic link that circumvented the United States, while offering partner states an alternative to U.S.-dominated networks. Similarly, the Pakistan-East Africa-Connecting Europe (PEACE) cable links Gwadar Port − flagship of the China-Pakistan Economic Corridor − to Djibouti and Europe. Its route intersects with sites of major Chinese political and military investment, including Beijing's first overseas military base in Djibouti, thereby further demonstrating the overlap between digital infrastructures and broader geopolitical footprints. These cases highlight a dual logic. On the one hand, the projects respond to partner states' demand for connectivity and development finance, providing short-term economic incentives. On the other hand, they embed Chinese technology, financing, and governance standards into the infrastructures of host countries, creating long-term dependencies on infrastructure and standards that extend Beijing's influence well beyond its borders. As Hillman notes, «shunned by the West, Huawei would connect the rest» (Hillman 2021, 109): having been excluded from Western markets, Chinese firms redirected their efforts toward the Global South, where financial packages and political backing could more readily translate into strategic presence, thus generating the alarmed response that we briefly analyzed before by the United States. Naturally, China's technological expansion does not unfold only beneath the oceans but it also manifests above the surface, in the rapid globalization of cloud services and smart infrastructures, which together extend the reach of the Digital Silk Road into partner states' economic and governance systems. This development represents the creation of a new "network periphery", in Hillman's (2021)

terms: whereas China's traditional connectivity points to the global internet were located beyond its borders and often in geopolitically sensitive areas, its companies are now constructing alternative nodes in emerging markets where Beijing's influence is stronger. Alibaba Cloud, Huawei Cloud, and Tencent Cloud stand at the forefront of this effort. Domestically, these companies have already consolidated a dominant position − Alibaba controlled nearly half of China's market by 2020 and became the world's fourth-largest cloud provider, while Tencent pledged $70 billion in cloud and AI investments over five years, and Huawei claimed to be providing services in over 140 countries (on these see Hillman 2021, 115-120). Internationally, however, their expansion has targeted regions that remain underserved by U.S. and European incumbents, especially Southeast Asia, the Middle East, Africa, and Latin America. These markets offer fewer barriers to entry and often welcome Chinese concessional financing, which is frequently bundled with the export of cloud and ICT services. Alibaba has positioned itself as a "bridge into China", leveraging the constraints of the Great Firewall as a competitive advantage for firms seeking reliable connections with the Chinese mainland. It has invested heavily in Southeast Asia, opening data centers in Indonesia and Singapore and committing $1 billion to developer training and start-up support across the region. Huawei Cloud, meanwhile, has pursued a more aggressive government-focused strategy, providing cloud platforms for sensitive functions such as health systems, social security records, and even electoral management in developing countries. Public announcements indicate that Huawei's cloud services are used by at least fifteen African governments and the African Union, with active data centers in South Africa, Kenya, and Nigeria. The Middle East has also become another crucial frontier. Chinese firms have secured contracts in Saudi Arabia and the United Arab Emirates to host governmental data, presenting these projects as drivers of "digital transformation" while embedding Chinese standards into the technological backbone of state institutions (Polyakova & Meserole 2019). Closely linked to the cloud expansion is the export of smart city and surveillance systems, marketed under the "Safe City" brand by Huawei, ZTE, Hikvision, and Dahua. These packages integrate surveillance cameras, biometric systems, and AI-powered analytics and have been deployed in more than sixty countries, often financed under the DSR (Feldstein 2019). While officially promoted as modernization tools, they often reinforce state surveillance capacities and institutionalize Chinese technical standards. As DeNardis (2014) has argued, control over intermediaries in the information ecosystem produces structural forms of influence. Through the combined expansion of cloud infrastructures and smart urban systems, Chinese firms increasingly embed themselves within the everyday functioning of foreign states, shaping not only technological choices but also the institutional frameworks of governance. This dual strategy illustrates that the external supply of Chinese digital technologies is not simply a commercial endeavor but an exercise in infrastructural geopolitics. It operates through

a territorial logic aimed at decoupling from existing U.S.-centered networks while simultaneously reconstituting new nodes of centrality in which Chinese platforms, standards, and governance practices become structurally indispensable.

Country	Dimension	Necessary	Sufficient	Falsifier	Code	Evidence	Mechanism
United States	Reshoring / Localization	Yes	Yes	No	2	EO 14017; CHIPS guardrails; funded capacity build-out; export controls.	Juris. leverage; supply chain choke points
United States	Resistance to Foreign Control	Yes	Yes	No	2	NDAA ban; FCC high-risk designations; CFIUS/Team Telecom; PLCN HK denial rec.	Juris. leverage; standards framing
United States	External Supply / Projection	Yes	Yes	No	2	Clean Network; DFC/Exim; Chile–Australia cable; Equiano/2Africa; standards strategy.	Standards lock-in; alt. routes
China	Reshoring / Localization	Yes	Yes	No	2	Cybersecurity Law; Data Security Law; Great Firewall control of flows.	Juris. leverage
China	Resistance to Foreign Control	Yes	Yes	No	2	JV/ownership constraints; Cybersecurity Review; foreign clouds via domestic partners.	Juris. leverage; op. constraints
China	External Supply / Projection	Yes	Yes	No	2	Digital Silk Road; SAIL & PEACE cables; gov. cloud; Safe City exports.	Standards/profile diffusion; alt. routes

Figure 2 - Coding Territoriality

Applying the necessary-sufficient coding to the evidence collected in this work, all three dimensions are coded as territorial practice (2) for both the United States and China. In each case, the analysis documents the requisite authority (laws, regulatory powers, financing/standards instruments) together with at least one outcome that materially alters dependencies, access, or control (domestic capacity

build-outs and enforced exclusions for the United States; binding localization and operational constraints on foreign providers for China; executed overseas cables, datacenters, and governance packages for both). No falsifiers emerge from the material analyzed. Substantively, a code of 2 does not imply autarky but it indicates that territorial strategies are operational, with observable effects on the allocation of infrastructural control, data jurisdiction, and standards adoption. These findings therefore support the chapter's central claim: despite institutional differences, the pursuit of cyber power converges on territorial strategies of governance that weaponize infrastructure, jurisdiction, and standards as durable instruments of state influence.

Conclusions

This chapter set out to test whether major powers translate the pursuit of cyber power into territorial and spatial strategies of governance. The comparative evidence examined on the United States and China, organized around the three analyzed dimensions of observable implications of (i) reshoring and localization, (ii) resistance to foreign control, and (iii) the external supply of technologies and infrastructures, supports a clear conclusion. Despite their distinct domestic institutions and vocabularies, both powers enact functionally specular strategies: they re-embed production and data under sovereign or allied jurisdiction; they harden their cores against rival ownership and leverage; and they project infrastructural capabilities outward to structure dependencies beyond their borders. In other words, regime type does not map onto divergent infrastructural practices, but on the contrary what emerges instead is a common spatial and territorial strategy for cyberspace.

The significance of these finding extends beyond the empirical comparison. They invite us to reconsider how power is constituted in the digital age. The evidence suggests, first, that the very terms of the long-standing debate about "Internet fragmentation" (see for example Mueller 2017) are misplaced. Fragmentation is not a looming possibility, nor a matter of political preference, but an accomplished fact. The territorialization of cyberspace is no longer speculative: infrastructures, data, and platforms are already being reorganized along sovereign lines and within geopolitical blocs. To speak of fragmentation as a future risk is therefore to obscure what is already a structural condition of global connectivity. Second, the comparative analysis reveals that cyber power is not exhausted by the operational dimension of attacks and defenses. Its foundations are infrastructural. States secure influence not only by developing offensive arsenals or defensive shields, but by embedding themselves in the material systems through which digital life unfolds: submarine cables, data centers, cloud platforms, and standards-setting processes. These infrastructures are not passive enablers; they are sites where authority is exercised and where dependencies are structured. To control them is to possess a form of power that is less visible than cyber operations but ultimately more enduring,

because it conditions the very environment in which others must act. Third, the rivalry between the United States and China shows that these infrastructural strategies are acquiring clear geographical contours. The territorialization of cyberspace is drawing lines on the map. Some regions already fall within consolidated spheres of influence, while others remain contested. Emerging markets in Africa, Latin America, and parts of Southeast Asia have become frontier zones, where alternative infrastructures and financing models compete for primacy. What is at stake in these arenas is not only economic opportunity but the inscription of long-term dependencies and alignments into the material fabric of connectivity.

Bibliography

Arcuri, G. (2022, January 31). The CHIPS for America Act: Why It Is Necessary and What It Does. Center for Strategic and International Studies (CSIS).

Bennett, A., & Checkel, J. T. (Eds.). (2015). *Process tracing: From metaphor to analytic tool*. Cambridge University Press.

Balestrieri, F., & Balestrieri, L. (2019). Guerra digitale – Il 5G e lo scontro tra Stati Uniti e Cina per il dominio tecnologico. LUISS University Press.

Balestrieri, F., & Balestrieri, M. (2024). Tecnologie dell'impero: AI, quantum computing, 6G e la nuova geopolitica del potere. LUISS University Press.

Barnett, M., & Duvall, R. (2005). Power in international politics. International Organization, 59(1), 39–75.

Center for Security and Emerging Technology. (2021, January 25). Measures for cybersecurity reviews (Translation of Chinese regulation issued April 13, 2020). Georgetown University.

Congress (2022). CHIPS and Science Act of 2022, Pub. L. No. 117-167, 136 Stat. 1492.

Creemers, R. (2017). Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. Journal of Contemporary China, 26(103), 85–100.

Dahl, R. A. (1957). The concept of power. Behavioral Science, 2(3), 201–215.

Data Security Law (DLS). 2021. Translation: Data Security Law of the People's Republic of China (Effective September 1, 2021). Stanford University.

Deibert, R. et al., 2010. Access Controlled The Shaping of Power, Rights, and Rule in Cyberspace. The MIT Press.

DeNardis, L. (2014). The global war for internet governance. Yale University Press.

Deruda, A. (2024). Geopolitica digitale: La competizione globale per il controllo della Rete. Carocci.

DOC & DHS - U.S. Department of Commerce & U.S. Department of Homeland Security. (2022). Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry.

DOT - U.S. Department of the Treasury. (2023). Remarks by Secretary of the Treasury Janet L. Yellen on the Biden Administration's economic approach toward the Indo-Pacific

Export–Import Bank of the United States (Exim Bank) (2020). Transformational Exports Program Report to Congress. Washington, DC.

FCC (2020). FCC Designates Huawei and ZTE as National Security Threats. Public Notice, June 30, 2020.

Feldstein, S. (2019). The global expansion of AI surveillance. Carnegie Endowment for International Peace.

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

Friedman, T. L., & Ramonet, I. (1999, Fall). Dueling globalizations. Foreign Policy.

George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. MIT Press.

Ghosh, S. (2019, December 29). Obama's "favorite books of 2019" list includes a title that slammed his administration's incestuous relationship with Google. Business Insider.

Haglund, D. G. (2024, August 14). Amigo shoring (1940): Washington's first experiment with "friend shoring" and what it tells us about geo-economic strategy. Comparative Strategy.

King, G., Keohane, R. O., & Verba, S. (1994). Designing social inquiry: Scientific inference in qualitative research. Princeton University Press.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. In F. Kramer, S. Starr, & L. Wentz (Eds.), Cyberpower and national security (pp. 24–42). National Defense University Press.

Kuhn, T. S. (1987). What are scientific revolutions? In L. Kruger, L. J. Daston, & M. Heidelberger (Eds.), The probabilistic revolution, Vol. 1: Ideas in history (pp. 7-22). Cambridge, MA: MIT Press.

Libicki, M. C. (2009). Cyberdeterrence and cyberwar. RAND Corporation.

Lilli, E. (2021). Redefining deterrence in cyberspace: Private sector contribution to national strategies of cyber deterrence. Contemporary Security Policy, 42(2), 163–188.

Locatelli, A. (2013). The offense/defense balance in cyberspace (Analysis No. 203). ISPI – Istituto per gli Studi di Politica Internazionale.

Long, M. L. (2023). Information warfare in the depths: An analysis of global undersea cable networks. Proceedings, 149(5), 1,443. U.S. Naval Institute.

Lovely, M. E. (2023). US CHIPS Act threatens to hollow out Asian semiconductor industry. East Asia Forum.

Mearsheimer, J. J. (2001). The tragedy of great power politics. New York, NY: W. W. Norton & Company.

Microsoft. (2023, dicembre 13). Microsoft Azure operated by 21Vianet: Overview of operations. Microsoft Learn.

Mueller, M. (2017). Will the internet fragment? Sovereignty, globalization and cyberspace. Polity Press.

Mueller, M. L. (2010). Networks and states: The global politics of Internet governance. MIT Press.

Na, Y. (2024). The Chinese Internet. Routledge.

National Development and Reform Commission (NDRC) & Ministry of Commerce (MOFCOM). (2021, December 27). Special Administrative Measures (Negative List) for Foreign Investment Access (2021 Edition). Beijing.

National Development and Reform Commission (NDRC), Ministry of Foreign Affairs (MFA), & Ministry of Commerce (MOFCOM). (2015, March). Vision and actions on jointly building Silk Road Economic Belt and 21st-Century Maritime Silk Road. State Council of the People's Republic of China.

National Institute of Standards and Technology (NIST). (2024). Implementation roadmap for the U.S. Government National Standards Strategy for Critical and Emerging Technologies (NSSCET). U.S. Department of Commerce.

National Telecommunications and Information Administration (NTIA). (2021). Implementation plan for the national strategy to secure 5G. U.S. Department of Commerce.

NDAA (2019). John S. McCain National Defense Authorization Act for Fiscal Year 2019. Public Law 115-232

Neuberger, A. (2025). China Is Winning the Cyberwar. America Needs a new Strategy of Deterrence. Foreign Affairs, 104(5).

Nye, J. S. (2010). Cyber power. Harvard Kennedy School, Belfer Center for Science and International Affairs.

Polyakova, A., & Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models. Brookings Institution, Foreign Policy Report.

Shivakumar, S., Wessner, C., & Howell, T. (2023, November 7). “Guardrails” on CHIPS Act funding to restrict investments in China may restrict participation in CHIPS Act incentives. Center for Strategic and International Studies (CSIS).

State Council Information Office of the People’s Republic of China. (2023, October 10). The Belt and Road Initiative: A key pillar of the global community of shared future [White paper]. Beijing.

State Council of the People's Republic of China. (2015, May). Made in China 2025. State Council. Retrieved from translation by Georgetown CSET

State Council of the People’s Republic of China. (2016, February 6). Administrative Provisions on Foreign-Invested Telecommunications Enterprises (Revised). Beijing. English translation available via Ministry of Commerce (MOFCOM).

The White House (2021). Executive Order 14017: America’s Supply Chains. CISA.

The White House (2023). U.S. Government National Standards Strategy for Critical and Emerging Technologies (NSSCET). National Institute of Standards and Technology.

The White House. (2020). National strategy to secure 5G.

The White House. (2024). Fact sheet: Advancing the U.S. Government National Standards Strategy for Critical and Emerging Technologies.

The White House. (2024). Fact sheet: Two years after the CHIPS and Science Act, Biden-Harris Administration celebrates historic achievements in bringing semiconductor supply chains home, creating jobs, supporting innovation, and protecting national security.

U.S. China Economic and Security Review Commission. (2012). Occupying the information high ground: Chinese capabilities for computer network operations and cyber espionage (Prepared by Northrop Grumman Corporation).

U.S. Department of Justice (2020). Team Telecom Recommends that the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States. Office of Public Affairs.

U.S. Department of State (2024a). Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World.

U.S. Department of State (2024b). Welcoming the First Subsea Cable Between South America and the Indo-Pacific Region.

U.S. House of Representatives Permanent Select Committee on Intelligence. (2012). Investigative report on the U.S. national security issues posed by Chinese telecommunications companies Huawei and ZTE. U.S. Government Printing Office.

Van Evera, Stephen. 1997. Guide to Methods for Students of Political Science. Ithaca, NY: Cornell University Press

Waltz, K. N. (1979). Theory of international politics. Reading, MA: Addison-Wesley.

Xi, J. (2015, December 16). Remarks by H.E. Xi Jinping, President of the People's Republic of China, at the opening ceremony of the Second World Internet Conference [Speech]. World Internet Conference. Amazon.

Xi, J. (2017, May 14). Work together to build the Silk Road Economic Belt and the 21st Century Maritime Silk Road [Keynote speech at the Opening Ceremony of the Belt and Road Forum for International Cooperation, Beijing]

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. Public Affairs.

Conclusions

This dissertation set out from two guiding questions, that have structured the inquiry from beginning to end. The first asked how geographical factors shape the spatial distribution of cyberspace infrastructures, while the second examined to what extent the pursuit of cyber power by major states translates into territorial and spatial strategies of governance. The answers that emerge are mutually reinforcing and converge on a central claim: the digital realm rests upon, and is strategically governed through, a material and territorial architecture. Far from dissolving geography, the expansion of cyberspace has intensified the salience of location, topography, chokepoints, and jurisdiction. Internet's apparent immateriality gives way, on inspection, to a hard skeleton of cables, landing stations, data centers, transmission corridors, energy linkages, and regulatory boundaries; and as states recognize the leverage conferred by those structures, they adopt policies that re-embed data, production, and standards within sovereign or allied domains while projecting infrastructural influence across borders. Cyberspace is not an ether above the earth; it is routed through seabeds, coasts, energy geographies, and metropolitan demand basins, and it is increasingly inscribed by law and policy that treat these routes and nodes as matters of high strategy. This dissertation shows it in three moves: it reconstructs the shift from a liberal imaginary of a borderless web to a contested, securitized, and territorialized digital order; it demonstrates empirically that connectivity infrastructures concentrate spatially and reproduce hierarchies; and it documents how major powers − despite institutional differences and contrasting vocabularies − deploy functionally similar repertoires to localize control and structure dependencies beyond their borders. Together, these elements sustain the conclusion that digital power today is fundamentally geographical and territorial in both structure and practice.

The first part of the argument proceeds by recovering a trajectory that is at once historical and conceptual. The liberal imaginary of the 1990s − of a borderless web, self-regulated by markets and voluntary norms − was never merely descriptive; it carried a political wager about the self-stabilizing virtues of interdependence. That wager has steadily lost credibility as actors have learned, often through crisis, that the same interconnections which promised efficiency and openness also transmit risk, diffuse coercion, and create structural asymmetries. The shift is not reducible to any single shock or doctrinal turn; it is through the cumulative recognition of political actors that networks can never be neutral channels and that infrastructures are not merely technical supports but strategic assets. The contemporary picture is therefore the inverse of the original utopia: states assert jurisdiction over the

physical layer (landing stations, cable routes, data centers), legislate over data localization and cross-border transfers, scrutinize supply chains for strategic choke points, and use standard-setting to project authority into the operational core of the network. The result is a re-territorialization of cyberspace that is neither rhetorical nor temporary; it is embedded in law, investment, and the siting of assets. The empirical part then demonstrates that the cloud, far from floating above geography, but rests and depends on it. The mapped distribution of submarine cables and landing points follows regularities that are intelligible in spatial terms: bathymetry and seabed conditions, access to littorals with established maritime and commercial infrastructures, and the gravitational pull of coastal gateway cities that already concentrate trade, finance, and population. Cables converge along a limited set of corridors and chokepoints, inscribing historical hierarchies into contemporary fiber routes and reproducing positional advantages for a small number of states and firms that occupy hub or brokerage positions. The terrestrial anchors of the network − data centers − are equally patterned. They cluster where energy is reliable and relatively cheap, where ambient temperatures reduce cooling costs, and where latency to dense demand basins can be compressed. Statistical results, while presenting a clear indication that climate and population have a positive effect in predicting the positioning of a datacenter at global scale, also indicate that exposure to natural hazards does not, in itself, exert a systematic deterrent effect on siting − a finding that may appear counterintuitive but that instead reflects how operators actively manage environmental risk by combining engineering redundancies, insurance markets, and contractual allocation of liabilities. These patterns do not simply illustrate an infrastructural geography; they condition power. The capacity to observe, route, slow, or sever flows is not evenly distributed. It follows the topologies that geography make possible and that policies ratify. The cloud, viewed from this angle, is a profoundly territorial artifact.

Having established that the digital skeleton is spatially structured, the final analytical step shows that great powers act accordingly. The comparative evidence on the United States and China brings into view strategies that are specular in function despite different institutional vocabularies. Both actors re-embed critical segments of production and data within sovereign or trusted jurisdictions; both harden their cores against rival control by tightening screening of foreign ownership in strategic sectors and by designing legal shields against extraterritorial discovery or seizure; both invest in the external provision of technology and infrastructure − such as submarine cables, cloud regions, platform ecosystems − so as to write durable dependencies into the connectivity choices of others. What changes is not the logic but the idiom: one speaks the language of openness and trusted supply chains, the other of cyber sovereignty and secure controllability. The outcome, however, is convergent: a world in which the fragmentation of cyberspace is no longer a hypothetical risk but an accomplished fact, albeit one that remains interlinked by selective gateways and negotiated standards.

In this landscape, infrastructural control is not ancillary to cyber power; it is constitutive, because it shapes the very environment within which all other actors must operate.

Contribution to the literature

This dissertation contributes to three strands of scholarship − strategic studies on cyberspace and cyber power, the international relations literature on great-power behavior, and neo-classical geopolitics − by bringing geography back to the center of explanation and by supplying an empirical strategy capable of measuring its effects. In a field that has produced sophisticated accounts of doctrines, capabilities, and coercion in the digital domain, systematic, large-N evidence on how geographic and geostrategic factors shape the *infrastructural* layer of cyberspace remains surprisingly scarce. The thesis addresses this gap by showing, with historical reconstruction, GIS mapping, and network metrics, that submarine cables, landing stations, and data centers follow patterned spatial logics − climate geographies, metropolitan demand basins, and legacy chokepoints − that concentrate connectivity and, with it, positional power. This empirical move matters theoretically: it demonstrates that what often appears as a placeless, purely "virtual" order is in fact materially embedded and unevenly distributed across space, and that these material asymmetries condition the exercise of influence online as much as (and sometimes more than) software-level innovation or operational tradecraft.

On the question that has animated much recent debate on whether cyberspace equalizes power or multiplies it − the dissertation advances a clarifying framework that disaggregates *cyber power* into three interrelated dimensions. Operational power captures episodic capabilities to disrupt, exfiltrate, deceive, or degrade informatic systems. Institutional power captures the capacity to shape the rules, norms, and technical standards that structure interaction − what is routable, inspectable, auditable, or lawful. Structural (or infrastructural) power captures the ability to manage dependencies, exploit vulnerabilities, and configure the environment in which digital interactions occur by owning, siting, and governing the places where flows must pass or rest. Lowered entry costs undeniably broaden access to operational power: a modestly resourced actor can acquire or rent the tools to conduct intrusions and information operations – the hacker's way of war as Libicki's termed it. Yet this very accessibility often obscures the enduring concentration of institutional and infrastructural power, which remain the preserve of large states and a handful of firms (usually well aligned with great powers) because they require deep capital, specialized talent, standard-setting participation, and sovereign legal reach over physical assets. By distinguishing these dimensions and tracing how positional advantages at the infrastructural layer feed into institutional rule-making and, in turn, shape the effectiveness and limits of operational action, the dissertation reframes the equalizer-multiplier

debate as an issue of scope conditions: cyberspace levels the *operational* playing field at the margins, while entrenching *institutional* and *structural* hierarchies at the core.

A second contribution speaks to the literature on great-power politics. Comparative analysis of the United States and China shows that regime type − though consequential in rhetoric, legal form, and domestic legitimation − does not produce fundamentally divergent *infrastructural* repertoires in this domain. Both powers pursue functionally similar strategies: reshoring and localization of critical production and data; screening and insulation against foreign control of strategic nodes; and outward projection through the financing, construction, and governance of external infrastructures and standards. The finding thus nuances claims that liberal and authoritarian orders necessarily translate into antithetical approaches to the global digital economy. It suggests instead that the geostrategic salience of communications technologies and data infrastructures induces convergence on a territorial logic: where the network touches ground − cable landings, IXPs, data farm, backhaul corridors − states of very different regime type behave similarly because that is where sovereignty can be asserted, dependencies configured, and leverage accumulated. In doing so, the dissertation adds granularity to theories of weaponized interdependence by showing that convertibility of network centrality into coercion turns on *where* control is anchored and *how* redundancy is engineered, not merely on abstract position within a graph.

Finally, the project contributes to neo-classical geopolitics by demonstrating that geography, topography, resource endowments, and positional advantages remain indispensable to explaining power even in the most "immaterial" of domains. Without discounting the importance of ideational and cultural factors that gained prominence in the 1990s, the evidence here shows that proximity, regionality, and physical lines of communication retain analytic bite. In theoretical terms, geography works not as a background "setting" but through mechanisms that structure incentives and capabilities. Distance imposes frictions that technology can compress but not erase: latency, error rates, and the cost and stability of energy scale with separation and with the number of conversions and crossings involved. Positionality matters because flows are not evenly distributed; actors and sites located at the intersection of multiple routes accumulate centrality and brokerage functions that can be translated into surveillance, and, *in extremis*, interdiction. Jurisdictional embedding converts location into authority: wherever assets touch ground, they become legible to specific legal orders, which in turn condition access to data, remediation obligations, and standards compliance. Path dependence then locks these configurations in place: early investments, agglomeration effects, and sunk coordination costs make corridors sticky and hubs self-reinforcing, raising the barrier to strategic rewiring. Together, these mechanisms generate the uneven topologies that define contemporary

cyberspace and make chokepoints and gateways durable structural features rather than historical accidents. These spatial mechanisms operate across scales. Locally, land-use regimes, utility interdependencies, and municipal permitting set the feasibility frontier for new nodes. Regionally, the distribution of demand and complementary infrastructures (energy mixes, terrestrial backbones, skilled labor) shape where dense computational and interconnection clusters can form. Transoceanically, route geometry and the allocation of jurisdiction along corridors condition redundancy, repair options, and the convertibility of centrality into leverage. Crucially, the mechanisms interact: positional advantage without jurisdictional reach yields limited authority; jurisdiction without centrality yields limited influence; reductions in technological friction amplify rather than dissolve the payoff to scale and agglomeration, thereby intensifying the politics of position. As a result, strategies that appear purely "digital" − platform governance, standard-setting, or data localization − are in fact inseparable from choices about where assets sit, which legal orders bind them, and how easily traffic can be rerouted around them.

Reframing cyberspace through this geopolitical lens is an analytic correction, not a metaphor. It redirects attention from placeless abstractions to constraints and affordances that make some strategies feasible and others fragile, and it clarifies why operational feats by weaker actors rarely translate into lasting influence absent institutional and infrastructural position. It also reconnects contemporary to the Anglo-American classical geopolitical tradition that foregrounded position, proximity, and lines of communication as enduring determinants of power, and that remains valid both analytically and geostrategically when recast for an infrastructural century.

Limits and Future research

The most immediate limitation is the scope of the infrastructural layers analyzed. By design, the empirical core concentrates on submarine cables and data centers. These are indeed the backbone of international connectivity, but the global network is multiplex. Satellite constellations (and their ground segments), long-haul terrestrial fiber within continents, Internet exchange points (IXPs), content-delivery and edge-computing nodes, and cloud introduce additional elements that can re-weight leverage in ways the cable-data center dyad cannot capture. For example, IXPs and private peering can localize traffic that would otherwise traverse international backbones; cloud on-ramps can shift dependence from physical corridors to platform-level contracts; and low-Earth-orbit satellites may, in specific geographies, change latency and resilience trade-offs even if they do not displace fiber's capacity advantages. A fuller account requires integrating these layers into a coherent, multi-layer network representation rather than treating them as ancillary context.

A second limitation concerns data completeness and measurement error. As anticipated in chapter II Publicly available inventories of cables, landings, and facilities remain incomplete, uneven across regions, and − because of commercial confidentiality and national security − selectively opaque. Exact routes are often generalized; capacity and utilization are variably reported; ownership and control structures can be nested in consortia and special-purpose vehicles that are difficult to untangle; and datacenter registries tend to overcount planned projects while undercounting private, unmapped sites. Geocoding introduces additional error: facility coordinates can be imprecise; and matching across heterogeneous sources risks both duplicates and omissions. These imperfections do not invalidate pattern detection, but they widen uncertainty bands around estimates of centrality, exposure, and redundancy. Future work should pursue systematic data fusion (combining operator disclosures, regulatory filings and commercial datasets), and make uncertainty explicit through sensitivity analysis and multiple-imputation strategies rather than treating point estimates as precise.

Temporal design is a third constraint. All analyses here are cross-sectional or near-contemporaneous snapshots. Yet infrastructure is dynamic: cables are upgraded, rerouted, or retired; protection measures are added after failures; datacenter footprints migrate with energy markets, climate policy, and local incentives; and hazard profiles evolve with environmental change. A longitudinal cartography − panel datasets linking infrastructure changes to policy shocks, energy price regimes, green policies or exogenous events − would allow the identification of path dependency and the timing and mechanism of change of these infrastructures. It would also improve causal leverage. Event-study designs around cable cuts, the opening of new landings, major cloud-region inaugurations, or regulatory shocks (localization mandates, screening laws) could estimate how traffic patterns, interconnection prices, and positional centrality adjust over time.

The comparative frame constitutes a fourth limitation. Focusing on the United States and China clarified great-power repertoires but risks overgeneralization. Regime type, industrial policy traditions, alliance networks, and capital-market structures vary in ways that may shape infrastructural strategy elsewhere. Moreover, within each case, the analysis relies heavily on public doctrine and policy documents; elite interviews, firm-level strategy archives, and regulatory case files would deepen the analysis and reduce the risk of rhetorical over-read. Incorporating middle-power and small-state strategies would also test propositions about brokerage, neutrality, and digital non-alignment, and would illuminate how states without great-power balance nonetheless accumulate positional leverage.

Private-sector agency is a fifth, and crucial, gap. Cloud providers, content platforms, submarine cable consortia, carrier, and fiber operators often decide where to place nodes, how to peer, and when to

retire capacity. Their strategies mediate or magnify state aims, but they are motivated by contractual economics, latency-sensitive workload distribution, tax regimes, and internal risk models. A political economy of the cloud − ownership networks, capital expenditure cycles, peering and transit contracts, service-level agreements, and exit costs − would specify channels through which corporate decisions translate into geopolitical constraints or opportunities. It would also surface distributional effects: how market concentration shapes resilience, pricing power, and the diffusion of security standards.

These limitations do not overturn the central claims; they indicate where additional leverage can be gained. The core point − that geography and territoriality structures the digital order materially and politically − remains valid on the evidence assembled here, yet it is precisely because it holds that it makes sense to push further. A multi-layer, longitudinal, mechanism-driven research design − combining richer datasets, event-study and quasi-experimental identification, alternative network metrics, and closer integration of corporate strategy and regulatory process − would narrow uncertainty and extend the argument across cases and time. In parallel, the project's GIS cartography should be iteratively improved: expanding coverage to additional layers (IXPs, edge nodes, terrestrial backbones, satellite ground segments), refining geocoding and capacity estimates, harmonizing heterogeneous sources through systematic data fusion, and making uncertainty explicit via sensitivity analysis. The goal is a living cartography that functions as an increasingly accurate heuristic instrument, one that not only visualizes the spatial skeleton of connectivity but helps generate and test hypotheses about leverage, vulnerability, and policy effects. On the qualitative side, deeper process tracing is warranted to illuminate the sequences through which infrastructural choices translate into institutional outcomes: triangulating public doctrine with elite interviews, regulatory files, firm archives, and standards-body proceedings would sharpen causal inference about how states and corporations convert positional advantages into rule-making authority and coercive capacity. Taken together, these extensions would transform a persuasive snapshot into a durable, generalizable, and practically useful account of how geography continues to structure power in the digital age.

Policy Recommendations and Future Scenarios

Recognizing network centrality as a source of power in cyberspace entails more than acknowledging that some actors sit at the crossroads of global flows. It requires treating centrality as a strategic asset that can be cultivated, protected, and, when necessary, temporarily relinquished. States at or near the core − able to function as hubs, set *de facto* standards, and act as indispensable intermediaries − convert positional advantages into rule-making authority, agenda-setting capacity, and informational leverage. The United States illustrate this dynamic through long-standing control of key routes, platforms, and forums; China's strategy has been to assemble an alternative hub architecture capable

of mediating the connectivity of third countries. Yet centrality is a double-edged asset. Hyper connection magnifies exposure to cascades: outages, software defects, targeted attacks, and coercive pressure propagate more rapidly and widely through cores precisely because of their indispensability. Power in cyberspace cannot therefore be equated with connectivity alone; it is the product of connectivity plus resilience.

For policy, two lines of effort follow. First, engineer redundancy where topology concentrates risk. This means financing genuinely disjoint cable paths and inland backhauls; prioritizing dual landings on distinct coastal morphologies; hardening critical crossings; and formalizing restoration through pre-negotiated mutual-aid and repair-vessel access. Because private incentives under-provide redundancy on commercially marginal routes, public de-risking (guarantees, concessional finance) is warranted where single-edge failure would otherwise cascade. Second, prepare to operate critical infrastructures in a segmented or rapidly air-gappable posture. The objective is not permanent isolation but the ability to reconfigure quickly to an "islanded" mode when external compromise is suspected, preserving core functionality while containing propagation. In practice this entails architectural and procedural measures: network designs that support fast, well-scoped disconnection of hospital, defense, and industrial-control segments; local fail-safe services and data caches to sustain operations during isolation; out-of-band communications for command continuity; pre-authorized "break-glass" credentials and sovereign public key infrastructure that can function in offline mode; and routine exercises that rehearse the switch from normal interconnection to degraded but safe autonomy. Legal and regulatory frameworks should codify islanding playbooks (triggers, authorities, maximum isolation windows, restoration criteria) and align liability so that operators are incentivized to disconnect promptly when risk thresholds are crossed. In short, prioritize graceful degradation over fragile seamlessness: keep systems interoperable in peacetime, but ensure they can disconnect cleanly and operate safely in crisis, limiting damage from external intrusions without turning temporary safeguards into permanent fragmentation.

Strategic robustness supplements these measures with selective islanding: the legal and technical ability to segment and stabilize critical sub-networks during acute stress without compromising long-term openness. This requires pre-agreed playbooks with operators and allies (triggers, authorities, sunset clauses), periodic exercises, and harmonized emergency powers to avoid decision-latency compounding network latency. For middle and small powers, a pragmatic diplomacy of infrastructure is available: cultivate credible neutrality at IXPs and landing sites; welcome multi-vendor consortia under transparent rules; pair cloud procurement with exit clauses and interoperability tests; and pool

bargaining power through regional development banks to finance redundancy that single markets cannot justify. Such brokerage strategies convert position into voice without hard alignment.

As for the likely trajectory of the future of cyberspace, the evidence points to a polycentric, semi-sovereign patchwork rather than a single borderless commons. Interconnection will persist, but through selective gateways shaped by territorial strategies, industrial policy, and standards blocs. Three scenarios are not mutually exclusive and may co-evolve. A bloc-consolidation scenario hardens clusters around U.S. and China-anchored ecosystems, with partial interoperability managed by treaty-like agreements on routing security and data transfer. A brokered intermediation scenario leaves space for European Union, India, Japan, Gulf and ASEAN coalitions to act as balancing hubs, advancing "trusted connectivity" through finance and standards that knit rival systems at the edges. A layered substitution scenario introduces incremental flexibility – for instance low earth orbit satellites constellations − mitigating (but not eliminating) dependence on specific chokepoints. Resilience rather than seamlessness becomes the governing norm: networks are designed to degrade gracefully under stress and to recover quickly, with redundancy and governance substituted for naïve assumptions of frictionless integration. None of this implies technological autarky. The policy problem is to optimize exposure: it should remain sufficiently central to shape rules and reap scale economies, while embedding enough redundancy, procedural safeguards, and emergency authorities to absorb shocks and resist coercion. Realism, rather than pessimism, should guide this outlook. The strategic actor of the next decade will be judged not only by how much traffic it carries or how many regions it hosts, but by how well it can toggle between openness and insulation when circumstances demand, preserving interoperability in normal times and protecting core functions in crisis, without turning temporary safeguards into permanent fragmentation.