UNIVERSITY OF COPENHAGEN
FACULTY OF LAW

PhD Thesis

Marie Thøgersen

Ruling the Cloud

A Critique of International Cyber Law

Supervisors: Astrid Kjeldgaard-Pedersen (primary) & Marc Schack

Submitted on March 8, 2025

RULING THE CLOUD

RULING THE CLOUD

A Critique of International Cyber Law

PhD Thesis

Marie Thøgersen
Faculty of Law
University of Copenhagen

University of Copenhagen, 2025
Supervisors: Astrid Kjeldgaard Pedersen & Marc Schack
PhD defense: 2 June 2025
Assessment Committee: Mikkel Jarle Christensen, Miriam Bak McKenna, Ntina Tzouvala

CONTENTS

PREFACE

I was trained as a doctrinal lawyer. When I began law school at Aarhus University in 2015, I found a certain satisfaction in legal reasoning – it allowed me to reach seemingly meaningful conclusions about the world without the methodological struggles that preoccupied other disciplines. I don't remember ever being introduced to the limitations of the positivist methodology throughout my legal education. Law, as it was taught to me, appeared as a neutral system of rules, self-contained and logically coherent.

When I embarked on my PhD journey in January 2022, I carried this formalist optimism into my research. My initial research project was conceived as a study of how longstanding norms of international law could be applied in the digital era. I was curious about how international legal principles, once developed in an analog world, could be extended to regulate 'cyberspace'. But as I immersed myself in the field of international cyber law, I began noticing deep inconsistencies. Certain legal precedents were interpreted in ways that to me clearly contradicted their underlying logic, yet these interpretations became accepted in legal scholarship simply because states seemed to follow them. When I one day shared these concerns (which were, at this point, merely of a methodological nature) with a colleague, she responded pragmatically that I shouldn't worry too much about that; if states accept the doctrine, then this is simply how the law is.

I was perplexed. If coherent legal reasoning was only true until it was overruled by state power, then formalist rigor was insufficient to produce meaningful conclusions. Obviously, my colleague's assertion was correct in doctrinal terms. But where did that leave me as a legal scholar? I realized my inability to explain why some interpretations of law 'stick' while others do not within my positivist methodological toolbox. This realization led me to read *From Apology to Utopia*. Like many doctrinally trained legal scholars encountering the work of Martti Koskenniemi for the first time, I experienced something that can best be described as a loss of innocence. His argument – that international law is structurally indeterminate and operates in a constant oscillation between apology and utopia – felt like a moment of disillusionment. There was, for me, no way back to legal positivism after this. I could no longer see international law as a self-contained system of rules – the international legal language had revealed itself as an indeterminate system that is meaningless in abstraction from underlying social forces.

This emerging awareness soon became brutally reinforced. In the aftermath of October 7, 2023, Israel launched its full-scale destruction of Gaza – a devastating escalation of decades of genocidal violence against the Palestinian people. Every day since then, I have watched how the international legal language in which I had been trained – its categories, its doctrines, its institutions – became tools for legitimation of this brutal violence. It became devastatingly clear how international law's indeterminacy was not merely a theoretical insight – it was a tool of power.

This shift in perspective led me to the deeper question: if international law is structurally indeterminate, then why do certain interpretations ultimately become authoritative? I became increasingly convinced that to understand how legal interpretations manage to 'stick' despite the indeterminate nature of international law, a purely structuralist critique of international law was insufficient. I thus found myself, quoting Marx, 'in the embarrassing position of having to discuss what is known as material interests.'[1] It was in other words necessary to root the operations of international law in the material reality to make sense of them. The study of international cyber law became, for me, a case study in the legal developments occurring despite the structural indeterminacy of international law. This dissertation is the result of that intellectual journey.

I am grateful to my supervisors, Astrid Kjeldgaard-Pedersen and Marc Schack, for their steady support and guidance throughout this process. Their encouragement to follow my curiosity and carve my own research path has been invaluable. I also want to thank Barrie Sander for his rigorous engagement with my work at my evaluation seminar, which truly became a turning point in the writing process.

An essential precondition for conducting research is the existence of an adequate institutional framework. I have been fortunate to carry out my PhD fellowship at a time when the Faculty of Law at the University of Copenhagen was supported by an incredible administrative staff, which did not only maintain efficiency but also remained responsive to the local conditions of the faculty and created a welcoming environment, thus ensuring the ideal conditions for the academic activities of the faculty. I am especially grateful to Lilli Streymnes for welcoming me on some cold January morning during Covid, making me immediately feel at home at the faculty despite the rather odd circumstances prescribed by the lockdown.

[1] Karl Marx, 'Preface', in *A Contribution to the Critique of Political Economy*, 1859.

Thanks to everyone at iCourts for intriguing discussions, generous feedback, much-needed after-work beers, and stimulating retreats. And especially thanks to Ula Alexandra Kos, Ergün Cakal, Thorbjørn Waal Lundsgaard and Pernille Kloster for keeping me in great company in the corner office. I have thoroughly enjoyed sharing our ups and downs throughout the journey. Also a special thanks to Joseph Bernasol and Jenny Orlando-Salling for the support and solidarity throughout the last tough months.

Several people have provided thorough feedback on previous drafts of parts of this dissertation. Caroline Bertram, Erick Guapizaca Jiménez, Andrew Milne, Henning Lahmann, Joseph Bernasol, Andreas Piperedes, Carl Wilén, and Charlotte Cator have each taken time to engage with my work, not only helping me make significant improvements but also making this writing journey feel less solitary. I am also thankful to Carlos Orjuela and Rishabh Bajoria for accompanying me through the first thrilling yet somewhat terrifying steps of reading *Capital*. Above all, I am deeply grateful to Søren Mau for his unwavering and unconditional support throughout this process, intellectually and emotionally. A better partner for a writing journey does simply not exist.

A central challenge in writing this dissertation has been the lack of existing critical scholarship on international cyber law with which I could bring my work in dialogue. At times, this meant working in isolation, oscillating between profound uncertainty about the overall justification of the project and a feeling that there was just too much to say. But this also presented an opportunity: to engage with untouched questions about international law's operations in the digital age. While this dissertation opens many new questions, it should not be perceived as an attempt to offer any final answers. Rather, it attempts to sketch the crude contours of a rethinking of a dominant narrative. I hope that my scholarly colleagues will interpret any limitations and blind-spots as an invitation to join me in this important task.

PROLOGUE: IN PROXIMITY TO SILICON VALLEY

On November 10, 2016, Brian J. Egan, State Department Legal Adviser of the United States, delivered a speech at Berkeley School of Law – just across the Bay from Silicon Valley, the global epicenter of the tech industry.[2] Egan acknowledged how the location was a 'fitting place' for the topic of the speech: 'the importance of international law and stability in cyberspace'. Silicon Valley was, he contended, 'home to many of the world's largest and most innovative information technology companies.' The remarkable reach of the Internet, and the ever-growing number of connections between computers and other networked devices, were delivering 'significant economic, social, and political benefits to individuals and societies around the world.'

But as the frequent occurrence of malicious cross-border cyber activities were increasingly threatening these benefits, international law came to play an essential role in 'maintain[ing] cyber stability in order to preserve the continued benefits of connectivity.' The premise was clear: conflict arises, and international law becomes relevant, when the *stability* of digital infrastructures is at risk. With this framing, Egan proceeded to discuss how specific international legal norms apply to cyberspace.

The symbolism of Egan's speech is unmistakable: By charting the international rules governing in cyberspace from such close proximity to the epicenter of the multi-trillion-dollar tech industry, Egan deliberately chose the perspective of the winners of high-tech capitalism.

---

[2] Brian J. Egan, 'International Law and Stability in Cyberspace' (Berkeley School of Law, 10 November 2016).

It would probably be an unfounded claim of causality to assert that Egan's speech (or, for that matter Harold Koh's speech on the same matter four years earlier[3]) served as the trigger of the process that followed. However, the fact remains that in the years following Egan's visit to Berkeley School of Law, other states followed the American example. One by one, states have continuously published their views on how general international legal norms regulate information technologies. As of March 2025, 33 states and two regional organizations have published their views. Within international legal academia, the unilateral positions of states have been taken as modern expressions of customary international law, in which the two constitutive elements, state practice and *opinio juris,* are conveniently merged into one concise, easily digestible document. Unsurprisingly, mainstream international legal scholarship has been quick to respond with a vast body of research on *international cyber law*. In this dissertation, I interrogate this process as an unprecedented mode of international law-making and ask: *Why is international cyber law developing as it is?*

The answer, I argue, lies not within the doctrines of international law, but in the material realities of the digital landscape – and in the role of states in protecting it. Egan's location in proximity to Silicon Valley thus ultimately tells us more about international law than his more substantial remarks that followed. His engagement with international law is rooted in the perspective of those who design and control the digital landscape, profiting immensely from societies' increasing dependence on digital infrastructures. Presumably, nowhere in the world is the technophile optimism as unambiguous as from within Egan's proximity to Silicon Valley.

While international cyber law is increasingly taking shape to facilitate the constant expansion of digital infrastructures and protect them from external intrusions, the field disregards the risks faced by other social groups. It disregards how information technologies have become essential tools in a spatial restructuring of global production that is causing inequality, uncertainty and suffering for most of the world. This restructuring has worsened the conditions for the working class, which is exposed to unprecedented regimes of surveillance and new forms of vulnerability. Meanwhile, ever more aspects of life are being increasingly commodified, and ecological crises are deteriorating.

---

[3] Harold Hongju Koh, 'International Law in Cyberspace' (USCYBERCOM Inter-Agency Legal Conference, Ft Meade, 18 September 2012).

Once we look beyond the dominant, technophile narratives being promoted by the winners of the 'information society' and begin to see the digital landscape as a political terrain of conflict and struggles, then the emerging field of international cyber law reappears before us as a tool of power.

As I will argue in this dissertation, the consolidation of international cyber law is deeply tied to the global expansion of capitalism and the protection of the digital infrastructures that sustain it. Egan's speech, delivered just across bay from the rulers of the 'information society', was thus not just a neutral restatement of international cyber law – it was a declaration that those who shape the technology, shape the rules.

INTRODUCTION

Over the past 50 years, information technologies have profoundly transformed the world in the image of their designers. Automation has driven down labor costs while increasing profits, and the standardization and centralization of control over production and circulation have intensified global competition among workers as well as among companies. Digital infrastructures have accelerated capital flows, enabling financial markets to increase profits with minimal reliance on labor. In the contemporary data economy, ever more aspects of life are inputs for capital. Meanwhile, working class life is becoming ever more precarious, and an ecological crisis is unfolding. Yet, the technologies that have made possible these profound restructurings have also brought new vulnerabilities: Capital accumulation is now inextricably dependent on the stability and reliability of digital systems. In response, states are seeking to protect digital infrastructures through international law, resulting in the emergence of a new legal field: International cyber law.

This dissertation examines the nascent yet rapidly growing field of international cyber law through a Marxist lens. It challenges a popular narrative that international cyber law has simply emerged as the result of some neutral interpretative endeavor to apply extant law to new technologies. Instead, it argues that the emergence of the field must be understood as an expression of the role of the state-system in the reproduction of the social relations of capitalism out of which the digital landscape has emerged. Capitalist states operate through international law to protect and legitimize digital infrastructures that facilitate continuous capital accumulation while depoliticizing their profound social, economic, and ecological consequences. The dissertation examines how international law protects a digital landscape constructed and promoted by a high-tech elite – and how it might be contested.

International cyber law is a recent field of international law – emerging within the last 15 years in response to the growing societal dependencies on digital infrastructures. The field is concerned with key aspects of international law governing cyber operations, which we may provisionally define as external intrusions, interruptions, or disturbances of digital systems. While the crude contours of the field are now settled, the precise legal norms governing cyberspace are still being actively shaped. Existing scholarship on international cyber law has been dominated by positivist approaches to law, asking how existing rules of international law are identified, interpreted, and applied to the new reality of information technologies. These scholars are all addressing different aspects of the same overarching question: *How does international law regulate cyberspace?* They share a commitment to coming as close as possible to describing the law *as it is.* A variety of argumentative techniques are deployed in this endeavor, which are all centered on the search for consensus in the unilateral positions of states for the eventual, ultimate clarification of ambiguities as to the understanding of the international rules governing cyberspace.[4]

This dissertation traces the debates of positivist scholarship on the field, but distinguishes itself from the above scholarship by asking a fundamentally different question: *Why is international cyber law developing as it is?* This question relies on a rejection of a central assumption underlying existing scholarship of the field: the assumption that international law makes up a determinate system of rules. If international law was determinate, then no 'development' would be taking place, and the 'why'-question would be meaningless. As has long been established in critical international legal scholarship, the doctrinal legal methodology is indeterminate: State practice is both the legal source and the object of regulation. Every individual practice therefore has the potential to either verify an existing rule, be the seed for a new rule, or be a

[4] Amongst many others, Jeffrey Biller, 'The Strategic Use of Ransomware Operations as a Method of Warfare', *International Law Studies* 100, no. 1 (2023): 486; Sean Watts and Theodore T. Richard, 'Baseline Territorial Sovereignty and Cyberspace', *Lewis & Clark Law Review*, 2018, 809; Kevin Jon Heller, 'In Defense of Pure Sovereignty in Cyberspace', *International Law Studies* 97, no. 1 (2021); Wolff Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace', *International Law Studies* 89, no. 1 (2013); Michael Schmitt, 'Grey Zones in the International Law of Cyberspace', *Yale Journal of International Law*, 2018.

violation of a rule.[5] The doctrinal framework is incapable of explaining why a given practice has a given destiny – that is, why some practice turns into law, and other practice turns into violations thereof. To escape this circularity, the legal argument must either point to a utopian vision or to the practice of states, thus either pointing beyond doctrine or remaining within apologetic circularity.[6] I elaborate on the logical shortcomings of the positivist scholarship of the field of international cyber law in chapter one. For now, I want to merely raise the point that if I am correct to assert that international law is structurally indeterminate – that is, it contains no criteria for explaining why certain practices and ideas become law – then the dynamics shaping international cyber law must be external to doctrine.

This proposition is especially striking with regard to international *cyber* law for two reasons. *First*, the technological landscape to which international law is being applied contains profound, conflicting interests. Over the past 50 years, information technologies have scrupulously changed the world in the interest of their designers. Information technologies have, *inter alia*, reduced labor time and increased profits, making much of the work-force superfluous to the economy and weakening workers' collective bargaining power; intensified global labor competition, reinforcing inequalities between the Global North and the Global South; and empowered the financial sector to accelerate capital accumulation with a minimum of labor. By all these means, the working class is facing increasing uncertainty and new regimes of surveillance, and ever more aspects of human life are being commodified. The information technology landscape is thus by no means a natural, automatic realization of some predestined and universally beneficial end. It is a domain of conflict and contestation.

The *second* reason why the indeterminacy of international law is especially striking in the context of international cyber law relates to the process through this legal field is developing. The process of 'clarifying' the cyber-specific application of general international legal norms follows an unprecedented mode of what we might call international law-making. Through

---

[5] I have borrowed this metaphor from Anthea Elizabeth Roberts, 'Traditional and Modern Approaches to Customary International Law: A Reconciliation', *American Journal of International Law* 95, no. 4 (2001): 757–91.

[6] Martti Koskenniemi, *From Apology to Utopia: The Structure of International Legal Argument* (Cambridge: Cambridge University Press, 2005); Fleur Johns, 'Critical International Legal Theory', in *International Legal Theory: Foundations and Frontiers*, ed. Jeffrey L. Dunoff and Mark A. Pollack (Cambridge: Cambridge University Press, 2022), 135.

unilateral position papers, states are publicly expressing their views on the scope and content of general rules of international law in the context of 'cyberspace'. States are thereby deliberately and overtly shaping the contours of a new international legal field.

Given the high stakes of the rapidly changing technological landscape and the unprecedented mode of international law-making, a critical examination of the emerging field of international cyber law is urgently needed. This dissertation is an attempt at doing just that. By approaching the field of international cyber law through a Marxist lens, I study the practices and ideas that are crystallizing into 'law' as historically specific ideas that are neither natural nor uncontestable. Rooting the dominant ideas in the social relations of capitalism out of which the information technology landscape has emerged, I explain legal developments as a reflection of the role of the state-system in the reproduction of global capitalism.

State of the Art

To my knowledge, only a handful of scholars have addressed the nascent field of international cyber law from positions that challenge the basic presuppositions underlying legal positivism. These contributions have mostly been article-length interrogations of the debates surrounding the doctrine of sovereignty in cyberspace. Henning Lahmann has brought important nuances to the mainstream narrative on the legal nature of sovereignty in cyberspace through a critical analysis of the legal discourse around sovereignty, even if he ultimately recurs to doctrine in his conclusion.[7] Milton L. Mueller has further contextualized the contemporary debates on the doctrine of sovereignty, linking the conceptual debate over cyber-sovereignty to real-world geopolitical struggles over the governance of the internet.[8] However, he leaves the broader information technology landscape largely unexplored and disregards the ties between the internet and the broader dynamics of global capitalism. A few scholars have further contributed to the establishment of a critical research agenda on international cyber law by elucidating the contemporary information technology landscape and debates

[7] Henning Lahmann, 'On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace', *Duke Journal of Comparative & International Law* 32, no. 1 (2022): 61–107.
[8] Milton Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace* (Cambridge, MA: MIT Press, 2009); Milton Mueller, 'Against Sovereignty in Cyberspace', *International Studies Review* 22, no. 4 (2020): 779–801; Milton Mueller, *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace* (London: Polity Press, 2017).

on digital sovereignty through a colonial lens.[9] While a few critical interventions have thus emerged in recent years, a critical research agenda is only beginning to see the light of day. No scholarship has yet sought to root the very operations of the field in the social relations of capitalism. Beyond the field of international cyber law, technological developments have increasingly been examined through critical legal lenses, most notably new materialist and post-humanist perspectives.[10] However, both in their theoretical foundations and objects of inquiry, these approaches remain conceptually distant from the objectives of this dissertation. As it stands, critical scholarship on international cyber law remains sparse - and Marxism has been altogether absent.

The absence of Marxist inquiry into the field of international cyber law is striking, because the field sits at the intersection of two disciplines that both have rich Marxist traditions: *Law* and *technology*. Various streams of Marxist legal scholarship have long sought to elucidate law's (and specifically, international law's) intrinsic connections to capitalism. Moreover, not only has technology always been a central theme in Marxist scholarship – but the study of *information technology* as a mode of power within capitalism has also been gaining increasing scholarly interest. While international cyber law thus remains untouched ground within Marxist and broader critical literature, this dissertation is positioned on the shoulders of two well-established and rich intellectual traditions. In the following, I provide a brief recapitulation of central scholarly streams within these two traditions relevant to my argument.

Beginning with Marxist literature on law, it is notable that Karl Marx's own writings on law are relatively sparse and sporadic, despite his educational background in jurisprudence. Although he began a critique of Hegel's *Philosophy of Right*, he never completed it. Marx recognized that criticizing law required first criticizing the state, and criticizing the state, in turn, required a critique of political economy. As a result, he never comprehensively addressed the subject of law during his lifetime. Generations of

---

[9] Renata Ávila Pinto, 'Digital Sovereignty or Digital Colonialism?', *Sur - International Journal on Human Rights*, no. 27 (2018); Cong Wanshu, 'Contesting Freedom of Information: Capitalism, Development, and the Third World', *Asian Journal of International Law* 13, no. 1 (2023): 46–75.

[10] Emily Jones, *Feminist Theory and International Law: Posthuman Perspectives* (Routledge, 2023); Matilda Arvidsson and Emily Jones, *International Law and Posthuman Theory* (London: Taylor & Francis, 2024).

scholars since have drawn on his general insights into history and political economy to bear on the role of law in society.[11] Amongst them, an inevitable intellectual source is Soviet legal scholar Evgeniĭ Pashukanis. Pashukanis's attempt at formulating a general Marxist theory of the legal form has been highly influential and subject to renewed interest in recent years. Focusing on the most basic, abstract juridic concepts – equally applicable to any branch of law – Pashukanis aims to explain the legal form in the most general sense.[12]

Throughout the 1980s, the reckoning of the non-materialization of the promises of socialist revolution led to a temporary decline in the prominence of Marxist thinking. The area of law was no exception to this general tendency. Legal scholars who had previously found engagements with Marxist writings productive changed their focus.[13] Instead of attempting to show law's contingency on historically specific modes of production, structuralist and post-structuralist scholarship attempted to decode the properties of legal doctrine from within law itself, challenging the proposition underlying legal doctrine that law could be understood as a rationally integrated scheme within which one right answer to any legal question could be discovered by the qualified jurist.[14] One of the most prominent contributions to international legal theory throughout this period is Martti Koskenniemi's *From Apology to Utopia*, which demonstrates the structural indeterminacy of international law through a dissection of the structure of the international legal argument. Koskenniemi's exposition of the liberal paradox inherent in international legal discourse is both rigorous and compelling, remaining a strong starting point for critical interrogations with law. However, as was the case of most of this wave of notoriously anti-Marxist scholarship, Koskenniemi's structurally founded critique gives us little sense of the systemic

[11] Kanad Bagchi, 'Marxism and the Cognitive Turn in International Law – Exploring an Uneasy Relationship', *Amsterdam Law School Research Paper No. 2024-42*, 2024.

[12] Evgeniĭ Bronislavovich Pashukanis, *Law and Marxism: A General Theory*, ed. C. J. Arthur (London: Ink Links, 1978).

[13] Johns, 'Critical International Legal Theory', 145.

[14] Johns, 'Critical International Legal Theory'. See also Roberto Mangabeira Unger, *The Critical Legal Studies Movement: Another Time, a Greater Task* (London & New York: Verso, 2015).

subordinations empowered and enabled by international legal discourse.[15] His framework thus leaves open the question of what real conditions determine the eventual occurrence of regularities in what we come to accept as the 'content' of international law (in the language of Koskenniemi, substantial determinacy).

The last couple of decades have witnessed a revival in the interest for Marxist legal scholarship, manifesting the tradition as an invaluable intellectual resource for rooting the liberal paradox in international law in historically specific material conditions. Various streams of Marxist international legal scholarship have emerged in this revival. These contributions do not represent a cohesive, uniform set of prescriptions.[16] Beyond two key themes – historicity and materiality – Marxist legal thought remains varied and fragmented, encompassing a wide range of ideas.[17] One stream has emerged out of the Pashukanian tradition, seeking to show how the legal form is intrinsically connected to capitalism. China Miéville's influential volume, *Between Equal Rights,* stands the most important contribution within this tradition. Combining Koskenniemi's structuralist account of the indeterminacy of international law with a Pashukanian theory of the legal form, he argues that the 'content' of international law is defined by the state with the coercive power to back its interpretation by force.[18] Another stream of scholarship has sought to show the role played by international law in the historical transformation of non-capitalist societies into the image of capitalist modernity, focusing on how the central doctrines of international law – its rules on trade and commerce, the doctrine of territory, sovereignty, and statehood, has been central to an imperialist project of Western domination and

[15] China Miéville, *Between Equal Rights: A Marxist Theory of International Law* (Chicago: Haymarket Books, 2006), 53–54; Ntina Tzouvala, *Capitalism As Civilisation: A History of International Law*, 1st ed. (Cambridge: Cambridge University Press, 2020), 35.

[16] Kanad Bagchi, 'Marxist Approaches to International Law: An Outline', *Max Planck Institute for Comparative Public Law & International Law (MPIL) Research Paper No. 2022-16, Forthcoming in: OpenRewi Textbook on Public International Law*, 2022; Susan Marks, ed., 'Introduction', in *International Law on the Left: Re-Examining Marxist Legacies* (Cambridge: Cambridge University Press, 2008).

[17] For an informative overview, see Bagchi, 'Marxist Approaches to International Law'.

[18] Miéville, *Between Equal Rights: A Marxist Theory of International Law*.

expansion of the capitalist mode of production.[19] A third stream of Marxist legal scholarship has focused on the class struggles underlying international law, analyzing international law as a terrain of global class antagonisms in which legal structures sustain the subjugation of the global proletariat.[20] A fourth stream of scholarship has focused on the ideological role of international law, amongst whom Susan Marks stands as the most prominent representative.[21] While varied in focus and methodology, these diverse contributions share a fundamental commitment to demystifying international law and exposing its entanglement with the material structures of capitalism. This dissertation is primarily informed by the first two streams of Marxist legal scholarship, drawing on the Pashukanian tradition to interrogate the legal form's intrinsic link to capitalism and engaging with historical materialist accounts of how international law has facilitated the expansion of the capitalist mode of production. These perspectives provide a critical foundation for the arguments that follow.

Let me now turn from Marxist legal scholarship to the second important theoretical foundation of this dissertation. *Technology* is a key theme in Marxist literature as well as critical literature more broadly. Traditional Marxist conceptions of technology have been characterized by a tendency towards technology determinism, neglecting the power of human agency to control technological development and instead considering technical means to be

---

[19] Bagchi, 'Marxist Approaches to International Law', 4–5; Bagchi, 'Marxism and the Cognitive Turn in International Law – Exploring an Uneasy Relationship'; Tzouvala, *Capitalism As Civilisation*; Matilda Arvidsson and Miriam Bak McKenna, 'The Turn to History in International Law and the Sources Doctrine: Critical Approaches and Methodological Imaginaries', *Leiden Journal of International Law* 33, no. 1 (2020): 37–56.

[20] B.S. Chimni, 'International Institutions Today: An Imperial Global State in the Making', *European Journal of International Law* 15, no. 1 (2004): 1–37; Akbar Rasulov, '"The Nameless Rapture of the Struggle": Towards a Marxist Class-Theoretic Approach to International Law', *Finnish Yearbook of International Law* 19 (2008): 243–94; Mai Taha, 'Reading "Class" in International Law: The Labor Question in Interwar Egypt', *Social & Legal Studies* 25, no. 5 (2016): 567–89; B.S. Chimni, *International Law and World Order: A Critique of Contemporary Approaches*, 2nd ed. (Cambridge: Cambridge University Press, 2017).

[21] Susan Marks, *The Riddle of All Constitutions: International Law, Democracy, and the Critique of Ideology* (Oxford: Oxford University Press, 2003). See also Shirley V. Scott, 'International Law as Ideology: Theorizing the Relationship between International Law and International Politics', *European Journal of International Law* 5, no. 3 (1994): 313–25.

neutral insofar as they merely fulfill natural needs.[22] In this view, information technologies are seen as an inevitable result of humanity's progressive development. Ironically, this neutralization of technology is prevalent in Marxist determinism and liberal instrumentalism alike.[23] The determinist technology view has the implication of moving technologies away from political controversy: if technological development is merely a realization of a destined future, then its direction cannot reasonably be contested.[24] As various scholars have shown, such technology determinism is not only flawed – it is also essentially anti-Marxist. It fails to see how technologies are historically specific, and insofar as history is a social product, so are technologies reflections of the mode of production at a given time. Marx was indeed attentive to the historical specificity of technologies. In *Capital,* he describes how instruments of labor of a given society at a given time reflect the economic formations of society.[25] There is thus no universally given direction of technological developments. An insistence that technologies are contestable and reversable should be at the center of the Marxist study of technologies.

The historically specific nature of technologies has been recognized by constructivist technology scholars, who have analyzed technological developments as an innovative design process, the course of which different actors have the ability to influence.[26] These scholars emphasize how a wide variety of social groups counts as actors that may have the power to influence the design process. Corporations, technicians, politicians, and bureaucrats are all involved to one degree or another. They meet in the design process where

---

[22] Andrew Feenberg, *Questioning Technology* (London, United Kingdom: Taylor & Francis Group, 1999), 9; Gavin Mueller, *Breaking Things at Work: The Luddites Are Right About Why You Hate Your Job* (London & New York: Verso, 2021), 4.

[23] Chapter IV of this dissertation shows how prevalence of liberal instrumentalism within the field of international cyber law. See also James N. Rosenau, 'Information Technologies and the Skills, Networks, and Structures That Sustain World Affairs', in *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, by J. P. Singh and James N. Rosenau (Albany: SUNY Press, 2002).

[24] Feenberg, *Questioning Technology*, 2; Daniel R. McCarthy, *Power, Information Technology, and International Relations Theory* (London: Palgrave Macmillan, 2015).

[25] Karl Marx, *Capital: A Critique of Political Economy. Volume One*, Penguin Classics (London: Penguin in association with New Left Review, 1990), 286.

[26] Feenberg, *Questioning Technology*; McCarthy, *Power, Information Technology, and International Relations Theory*.

they wield their influence by proffering or withholding resources, assigning purposes to new devices, fitting them into prevailing technical arrangements to their own benefit, imposing new uses on existing technical means, and so on. The interests of the involved actors come to be expressed in the technologies they participate in designing.[27] While constructivist technology scholars accurately capture how technologies reflect the interests of those positioned to influence the design process, they often underestimate how the central axis of the power relations by which the innovative process is formed are defined by the mode of production of a given society.[28] Under capitalism, the creative power to control and design the innovative process ultimately follows the logics of capital. The necessary resources to undertake technological developments thus lie in the hands of capitalists who own the means of production – and of states, which have become dependent upon economic growth for their own existence and functioning.[29] In contrast, the working class, which has no access to the means of production, has no power to influence the innovative process.[30] Within this broad framing, a wealth of scholarship has elucidated various aspects of the development of information technologies since the emergence of digital computers in the 1950s.[31]

---

[27] Feenberg, *Questioning Technology*, 10–11.

[28] McCarthy, *Power, Information Technology, and International Relations Theory*, 55.

[29] McCarthy, 58–59; William Clare Roberts, 'What Was Primitive Accumulation? Reconstructing the Origin of a Critical Concept', *European Journal of Political Theory* 19, no. 4 (2020): 533; Mariana Mazzucato, *The Entrepreneurial State: Debunking Public vs. Private Sector Myths* (London: Anthem Press, 2015).

[30] McCarthy, *Power, Information Technology, and International Relations Theory*, 58–59.

[31] Amongst others, see David F. Noble, *Forces of Production* (Transaction Publishers, 1984); Shoshana Zuboff, *In the Age of the Smart Machine: The Future of Work and Power* (London: Heinemann, 1988); Nick Dyer-Witheford, 'Cyber-Marx: Cycles and Circuits of Struggle in High-Technology Capitalism', *Canadian Journal of Communication* 25, no. 3 (2000); Nick Dyer-Witheford, 'Empire, Immaterial Labor, the New Combinations, and the Global Worker', *Rethinking Marxism* 13, no. 3–4 (2001): 70–80; Nick Dyer-Witheford, *Cyber-Proletariat: Global Labour in the Digital Vortex* (London: Pluto Press, 2015); Charmaine Chua et al., 'Introduction: Turbulent Circulation: Building a Critical Engagement with Logistics', *Environment and Planning D: Society and Space* 36, no. 4 (2018): 617–29; Martin Danyluk, 'Capital's Logistical Fix: Accumulation, Globalization, and the Survival of Capitalism', *Environment and Planning D: Society and Space* 36, no. 4 (2018): 630–47; Mueller, *Breaking Things at Work*; Deborah Cowen, *The Deadly Life of Logistics: Mapping Violence in Global Trade* (Minneapolis: University of Minnesota Press, 2014); Nick Srnicek, *Platform Capitalism* (New York City: John Wiley & Sons,

Through a synthesis of the central insights from these streams of research on various aspects of the information technology landscape, I explore how the information technology landscape of today has emerged and taken shape.

These bodies of critical literature on law and technology make up the scholarly cornerstones of this dissertation. As I will show, law and technology each represent a distinct mode of power, which are intertwined in the field of international cyber law in a way that makes the ideas of the field seem obvious and uncontestable. Yet, one additional body of literature is important to this dissertation and deserves mentioning here: Critical security studies. As I will show, the evolving concept of cybersecurity has been central to the delineation of the field of international cyber law, making particular concerns seem universal. Critical security studies have long illuminated how there is nothing natural or inevitable about notions of security.[32] Following the Copenhagen School, security has a performative character – that is, it does not only describe the world but can also transform social reality.[33] As such, the concept of (cyber)security does not simply represent a a natural and uncontestable category; it is 'built on a series of political and epistemological choices that define what is considered security.'[34] In the context of cyberspace, Hansen and Rosenbaum have argued that the securitization of cyberspace works to 'prevent it from being politicized in that it is precisely through rational, technical discourse that securitization may "hide" its own political roots.'[35] But importantly, and in contrast to much of the prevalent scholarship on (cyber)securitization emerging from the tradition of the Copenhagen School, I root the emergence and development of

---

2016); Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019* (London: Profile Books, 2019); Nick Couldry and Ulises A. Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford: Stanford University Press, 2019); Cory Doctorow, *The Internet Con: How to Seize the Means of Computation* (London & New York: Verso, 2023).

[32] Mark Neocleous, *Critique of Security* (Edinburgh: Edinburgh University Press, 2008).

[33] Thierry Balzacq, Sarah Léonard, and Jan Ruzicka, '"Securitization" Revisited: Theory and Cases', *International Relations* 30, no. 4 (2016): 495.

[34] Keith Krause and Michael C. Williams, 'Broadening the Agenda of Security Studies: Politics and Methods', *Mershon International Studies Review* 40, no. 2 (1996): 234.

[35] Lene Hansen and Helen Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly* 53, no. 4 (2009): 1168.

ideas in the material conditions, thus insisting that ideas do not precede material reality and that the analysis of the former is only meaningful when rooted in the latter.[36] I thus follow Marc Neocleous in seeing the critique of security as 'part and parcel of a wider critique of power'.[37]

Security represents a third mode of power which is intertwined with law and technology in the field of international cyber law, making up an intricate ideological operation that is hardly contestable from any singular perspective. To break down the field – its 'self-evident views and spontaneously arising notions'– it is necessary to explore how international law, information technology, and cybersecurity are interwoven.[38] I aim to do just that by bringing insights all three disciplines – law, technology, and security – into conversation. By dissecting the doctrinal debates through which ideas about information technology are being (re)produced as international law, and by rooting these ideas in the social relations of capitalism, I aim to expose how international law works through cybersecurity to sustain global capitalism in the digital era.

The Field of International Cyber Law

The task ahead of me is to unmask the field of international cyber law. But before doing so, it is necessary to clarify what I mean by 'international cyber law.' The field is not a fixed, codified body of legal rules; rather, it is an ongoing process in which states, legal scholars, and international institutions are developing rules that govern digital technologies. Unlike other areas of law that have developed through treaties or longstanding state practice, international cyber law has emerged within a couple of decades mainly through unilateral position papers articulating their interpretations of how international law applies to cyberspace. As of this writing, some-30 states and two regional organizations have contributed to this process. These positions, alongside negotiations in international fora such as the United Nations Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG), quasi-legal scholarship like the two Tallinn Manuals

[36] See for example Hansen and Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School'; Tobias Liebetrau, 'Problematising EU Cybersecurity: Exploring How the Single Market Functions as a Security Practice', *Journal of Common Market Studies* 62, no. 3 (2024): 705–24.

[37] Neocleous, *Critique of Security*, 5.

[38] Michael Heinrich, *An Introduction to the Three Volumes of Karl Marx's Capital* (New York City: NYU Press, 2004), 35.

developed by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), and positivist legal scholarship engaging in questions as to how international law applies in cyberspace form the core of what I understand as international cyber law.

Despite these characteristics, international cyber law is not generally treated as a distinct legal field. Many scholars insist on referring to it instead as 'international law applicable to cyberspace', a seemingly minor textual nuance that in fact has substantial implications: the latter phrase suggests that 'cyberspace' is not a separate legal domain detached from other domains, and that information technology is therefore simply regulated by *existing rules* of international law.[39] The process taking place, then, is not a political process, but a process through which existing law is applied to a new set of technologies. Although uncertainties and ambiguities exist, they are merely a reflection of law's occasional lack of clarity in combination with the novelty of technological innovations.

However, this view fails to account for the actual process by which certain interpretations of law become dominant while others are sidelined. As I will argue in chapter one, no law-application exists that can be distinguished from law-creation – and thus, from politics. Through this perspective, it is hardly possible to draw any disciplinary lines between separate areas of law on the basis of any legal systematicity. The field of international cyber law is therefore first and foremost distinguishable by its procedural nature. We have already seen how the process of international cyber law distinguishes itself from other modes of international law-making. In the following, I provide some further reflections on how the scholarly field of international cyber law distinguishes itself from other areas of international law.

While I will not be interrogating the economy of the scholarly landscape as part of this study, it is remarkable that the field distinguishes itself from other areas of international law by its economical foundation: Many states are allocating resources for the academic production of research within this field and related ones, such as artificial intelligence, often through partnerships between National Defenses, Military Research Organizations, and publish universities (I know of such collaborations in Denmark, The Netherlands, Canada, and Norway). For the sake of transparency, here is perhaps

[39] See Dapo Akande, Antonio Coco, and Talita de Souza Dias, 'Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies', *International Law Studies* 99, no. 1 (2022).

a good place to inform that this also applies to the present PhD project. Thus, my PhD fellowship is related to the InterMil research project, a collaboration between the University of Copenhagen and the Royal Danish Defence College which, based on funding from the Ministry of Defence, 'provides research-based public-sector consultancy within the field of military studies' and 'examines questions of international law of particular relevance for the Danish Defence and Danish decision makers.'[40] I do not mean to imply that research carried out with support from national defense budgets are lacking 'impartiality' (a critique that would imply a belief in the existence of a neutral or apolitical position). Rather, I want to make the perhaps banal point that research that asks a particular type of questions – what Robert Cox calls 'problem-solving questions' – has other kinds of access to funding, which may explain the dominance of particular types of questions being asked rather than others.[41]

International law does not only consist of texts, but also of numerous rituals performed by persons that fulfill particular roles in designated places. Judges, diplomats, state officials, and lawyers 'perform' international law in courtrooms, embassies, and international fora.[42] However, when I delimit the object of this interrogation to the texts of the field, it serves a particular purpose, namely, to keep the object of interrogation as close as possible to that which is accepted by the scholars belonging to the field of international cyber law. Positivist legal scholars are, as we will see in chapter one, concerned with textual legal sources.[43] Despite 'state *practice*' being a central source in international legal doctrine, the positivist scholarship of the field of international cyber law tends to focus mainly on textual expressions of such practice. In particular, they take states' unilateral, written positions on international cyber law as indicative of state practice and *opinion juris* at once, merged into one concise document. They analyze the written records of negotiations in international fora such as the United States General Assembly and the precedents of international courts. When I choose to 'stick to the papers', as Darryl Li puts it, it reflects an endeavor to focus the analysis on

[40] iCourts, 'International Law & Military Operations (InterMil)' (University of Copenhagen, 7 August 2020), https://jura.ku.dk/icourts/research/intermil/.

[41] Robert W. Cox, 'Social Forces, States and World Orders: Beyond International Relations Theory', *Millennium* 10, no. 2 (1981): 126–55.

[42] Tzouvala, *Capitalism As Civilisation*, 18.

[43] Arvidsson and McKenna, 'The Turn to History in International Law and the Sources Doctrine'.

the sources that are usually identified as relevant by the positivist scholarship of the field. This choice fits with the methodology undertaken: my critical (re)reading of the field aims to expose the logics inherent in the field itself, rather than holding them up against some external logic.[44] As such, I am interested in the (re)production of ideas as law *within the field*. I provide some methodological reflections in the following section.

Critique as a Method

Marx once described his method as 'a critical exposé of the system of the bourgeois economy. It is at once an exposé and, by the same token, a critique of the system.'[45] Such a task requires a thorough interrogation of the categories, assumptions, and logics underlying the system, rather than a rejection of them. The same applies to the Marxist study of law; following Pashukanis, 'if the critique of bourgeois jurisprudence must follow the example of Marx's critique of bourgeois political economy, the critique must, above all, 'venture into enemy territory.'[46] Rather than throwing away the generalizations and abstractions deployed by the jurists of the field, we must *analyze* these categories to 'demonstrate their true significance'.[47]

In that endeavor, I am conscious to remain within the sources accepted in international legal doctrine.[48] Following Darryl Li, the legal form enables certain narrative content.[49] The critical task lies in a symptomatic reading of the texts of the field, that is, a reading that is concerned with understanding the underlying presuppositions that shape dominant ideas.[50] The critical task is not so much to show that the field of international cyber law is mistaken, but rather to trace dominant narratives back to their hidden presuppositions, expose their emergence and root it in the material conditions.

---

[44] Darryl Li, 'How to Read a Case: Ethnographic Lawyering, Conspiracy, and the Origins of Al Qaeda', *American Anthropologist* 125, no. 3 (2023): 561.

[45] Karl Marx, 'Letter to Ferdinand Lassalle, February 22, 1858', in *Marx & Engels Collected Works Volume 40: Letters 1856-1859* (International Publishers, 1975), 270.

[46] Pashukanis, *Law and Marxism*, 64.

[47] Pashukanis, 64.

[48] For a discussion of the role of sources in critical international legal scholarship, see Arvidsson and McKenna, 'The Turn to History in International Law and the Sources Doctrine'.

[49] Li, 'How to Read a Case', 563.

[50] Louis Althusser, *Reading Capital: The Complete Edition* (London & New York: Verso, 2016).

My analytical approach thus begins with a critical examination of the most recent texts in the field of international cyber law in which I identify its dominant narratives. I trace these narratives back in history to identify the presuppositions on which they rely. I thereby seek to expose the logics underlying the field – in other words, to expose the distinction between what the field aims to explain (the ambiguities and uncertainties that are acknowledged within the field) and what is accepted as so self-evident that it does not need to be explained at all (the narratives of who and what is needs protection).[51]

The prescribed methodology for critically (re)reading the texts of the field involves working backwards from the present. Beginning with the dominant ideas of the field of international cyber law as of today, I trace them back in time to uncover the presuppositions on which they rely and their underlying logics. However, the systematicity with which an investigation is carried out and conclusions are reached is not always the most logical order in which to structure and present an argument. Instead of structuring the three chapters (chapters four to six) that scrutinize the emergence of international cyber law in accordance with the methodology taken, I present them as a story of the emergence and development of key ideas of the field of international cyber law. Chapter four explores the emergence and evolution of the notion of cybersecurity from the end 1980s and until today. Chapter five examines the gradual emergence of international legal discourse within the field, which was from the beginning delineated around rationalities inherited from the dominant notion of cybersecurity. Chapter six zooms in on a question that remains overtly ambiguous today: the question of digital sovereignty. This structure means that the rationale behind my choice of textual material to include may not appear clear at the outset. This arguable weakness is a reflection of the fact that I present this part of my analysis in the reverse order of how I carried it out. With that caveat, I hope that my reading will ultimately make sense as a coherent narrative that traces the stream of ideational development and influence across the four decades under examination, while rooting these ideas in the social relations of capitalism out of which the digital landscape has emerged.

Throughout this dissertation, I speak of ideology, ideas, and discourses. Following a long tradition of ideology critique, I use the term *ideology* to refer

[51] Heinrich, *An Introduction to the Three Volumes of Karl Marx's Capital*, 34.

to the ways in which ideas sustain relations of domination.[52] Ideas should here be conceived in a broad sense, including conscious as well as unconscious thoughts, images, narratives, myths, utterances, and texts 'through which significance is generated, conveyed, received and appropriated'.[53] In close connection to ideas, I use the word 'discourse' in an overlapping, but slightly more narrow meaning to describe the visible expression of ideas.

My aim is not merely to challenge the naturalness of the dominant ideas of the field by exposing the presuppositions and logics on which they have been constructed, but more importantly, to explain why particular ideas have emerged at a particular time in history. The existence of an idea tells us nothing about *why* that idea came to dominate in this field at that time, and with what implications. It follows from this notion that we can only make sense of international cyber law by rooting the ideas of the field in historically specific social relations. This notion serves as an important theoretical foundation and structuring principle for this dissertation.

To move beyond empty deconstruction, I root the logics of the field in the social relations of capitalism and the role of states in their reproduction, examining how dominant ideas respond to particular conditions. An interrogation of the emergence of the information technology landscape is therefore a necessary component to the analysis. Through a synthesis of literature on the emergence and development of information technologies, I examine how increasingly sophisticated information technologies have emerged as responses to the needs of capitalism which, since the stagnation of the 1970s, has consistently tended towards crises and stagnation.

I am conscious that an examination of the information technology landscape in its multifaceted entirety might appear like a ridiculously broad task, unavoidably leading to some degree of reductionism. However, this dissertation is about a particular field of international law and not primarily about the technologies to which it applies. It follows from this that the delineation of my engagement with the technological reality must follow the delineation drawn by the field of international cyber law. Since the field of international

---

[52] Terry Eagleton, *Ideology: An Introduction* (London & New York: Verso, 1991); Jan Rehmann, *Theories of Ideology: The Powers of Alienation and Subjection* (Chicago: Haymarket Books, 2013); Louis Althusser, *On The Reproduction Of Capitalism: Ideology And Ideological State Apparatuses* (London & New York: Verso, 2014).

[53] John Brookshire Thompson, *Ideology and Modern Culture: Critical Social Theory in the Era of Mass Communication* (Stanford: Stanford University Press, 1990), 56; Marks, *The Riddle of All Constitutions*, 10–11.

cyber law is concerned with information technologies in a broad sense, my interrogation of the information technology landscape must be equally broad. I aim to accomplish the task by providing careful sketch of a complex and manifold evolution without pretending comprehensiveness. Such a sketch will allow us to root international cyber law in the information technology landscape as it has emerged out of the social relations of capitalism.

Capitalism: A Brief Primer

Neither international law nor information technologies can be understood in isolation from the fundamental social structures of the society we all live in. As I will argue throughout this dissertation, the legal form is historically specific to capitalism, and the content of international law reflects the role of the state-system in contemporary global capitalism. Information technologies have emerged in the context of capitalist social relations, in response to the imperatives of capital. This is not to suggest that capitalism explains everything; rather, capitalism operates alongside and interacts with other social forces. Why, then, should capitalism be given analytical priority? As the dominant mode of production of our time, capitalism organizes everyone's access to the resources necessary for their reproduction. The logics of capital define what everyone must do to survive. Before delving into the substantive interrogation of international cyber law in the chapters ahead, it is therefore necessary to provide a brief primer on capitalism, the capitalist mode of production, and the key categories and social relations that define this economic system.

Capitalism is a mode of production in which the production and exchange of commodities with a view to generating profit dominates economic activity. This process is best understood by following Marx's method of abstraction in *Capital* and starting with the commodity. A commodity is a thing which satisfies a certain human need (that is, it has a *use value*), and which is being produced or acquired to be exchanged on the market (that is, it has an *exchange value*). Importantly, the exchange value of a commodity is not determined by its use value. It is determined by the socially necessary labor time that goes into the production of the commodity. The socially necessary labor-time denotes the 'labour-time required to produce any use-value under the conditions of production normal for a given society and with the average degree of skill and intensity of labour prevalent in that society.'[54]

[54] Marx, *Capital: A Critique of Political Economy. Volume One*, 129.

Commodities possess an exchange value because they express an identical social substance, human labor. Their objective character as values is therefore *purely social*.[55] While commodities thus appear as an 'extremely obvious, trivial thing', Marx's analysis 'brings out that it is a very strange thing':[56] The commodity-form reifies the social characteristics of human labor as natural characteristics of the products of labor themselves, as the 'socio-natural properties of these things.'[57]

Commodities are brought to the market by their owners, where they are generally exchanged for other commodities with an equal exchange value. Money functions as a universal equivalent that facilitates exchange. What Marx calls 'simple circulation', that is, the exchange of commodities mediated by money (in other words, selling and buying), can be represented by the formula C-M-C, where C signifies commodity and M signifies money. This formula expresses the role of market transactions for most people: a commodity, for example their labor power, is sold for a sum of money (a wage), which is then used to buy the commodities people need.

As Marx demonstrates in a detailed dialectical derivation of concepts, this 'simple circulation' is in fact 'a mere form of appearance of some deeper process lying behind it, even resulting from it and producing', namely *capital*.[58] Marx defines capital as the process M-C-M', that is, a purchase followed by a sale that results in a larger sum of money than the original sum. In other words, the commodity form only becomes the general social form of the products of labor when the economy as a whole is governed by money and commodities circulating as capital, i.e. a market economy. A market economy is necessarily a *capitalist* economy governed by profitability.

Whereas workers engage in market transactions in the form of C-M-C, that is, by selling their labor power in order to be able to buy the use values they need, capitalists engage in market transaction with the aim of augmenting value, i.e. making a profit (C-M-C'). A crucial question in Marx's critique of the political economy is where this profit comes from. Profit cannot arise from the circulation of commodities alone.[59] If money is used to buy a commodity, and that commodity is sold, it will not generally result in a

---

[55] Marx, 138.

[56] Marx, 163.

[57] Marx, 165.

[58] Karl Marx, *Marx & Engels Collected Works Volume 29: Marx 1857-61* (New York: International Publishers, 1987), 482.

[59] Marx, *Capital: A Critique of Political Economy. Volume One*, 268.

higher magnitude of money than the original sum. Marx explains how the availability of labor power – and thus, the existence of classes – is a necessary presupposition for profit:

> [O]ur friend the money-owner must be lucky enough to find within the sphere of circulation, on the market, a commodity whose use-value possesses the peculiar property of being a source of value, whose actual consumption is therefore itself an objectification of labour, hence a creation of value. The possessor of money does find such a special commodity on the market: the capacity for labour, in other words labour-power.[60]

Just like any other commodity, the exchange value of labor power is determined by the socially necessary labor time for its production (and reproduction).[61] As such, the price of labor time is determined by the average of labor that goes into its production (and reproduction). The most foundational form of capital occurs in the production process: the capitalist buys raw materials and labor power, which are brought together with the means of production, resulting in a commodity that the capitalist brings to the market and sells for more money than they originally spent. Capital is therefore not a thing but a process; namely, the process of putting money into circulation to make more money.[62]

It follows from this that the existence of humans selling labor power as a commodity is the presupposition of capitalist production. This, in turn, presupposes a system of class domination. In contrast to the apologetic liberal fantasy, there is ample historical evidence that people all over the world have resisted becoming market dependent.[63] Historically, the process of so-called primitive accumulation was vital to establishing the preconditions for capitalism. Through the violent dispossession of the majority of people from the means of their own subsistence, people became forced to sell their labor power to capitalists to ensure their own survival. A central feature of

---

[60] Marx, 270.

[61] Marx, 274.

[62] Marx, 247–57; David Harvey, 'The Enigma of Capital and the Crisis This Time', in *Business as Usual: The Roots of the Global Financial Meltdown*, ed. Craig Calhoun and Georgi Derluguian (New York City: New York University Press, 2011), 89–112.

[63] Ellen Meiksins Wood, *The Origin of Capitalism* (New York City: Monthly Review Press, 1999); Robert Brenner, *Property and Progress: The Historical Origins and Social Foundations of Self-Sustaining Growth* (London & New York: Verso, 2009).

capitalist society is therefore that the majority of the people do not have immediate access to the means of production, forcing them to sell the only commodity in their possession – their labor power – to those who own and control the means of production, *i.e.* the capitalist class. In exchange for a wage, workers produce commodities, which the capitalist brings to the market to exchange for more money than they initially put into the production process.

Central to the capitalist mode of production is therefore the establishment and reproduction of a particular set of social relations. The social relations that define capitalism can be divided into two sets: *vertical* relations between the exploited class and the exploiting class (a relationship of dependence), and *horizontal* relations among the members of these classes themselves (a relationship of competition).[64] Together, these relations make up the foundations of the capitalist economy.[65] The state has traditionally been seen to play an important role in the capitalist system. The formal separation of states from the capitalist class allows states to ensure stable and reliable property relations, ultimately with extra-economic force, at arm's-length from capital. The state functions as an institution 'standing above the self-destructive competition of individual capitals, to ensure that such competition did not compromise the expanded reproduction of capital.'[66] States are, in turn, dependent upon economic growth for their own existence and functioning.[67]

The capitalist economy compels everyone to follow particular logics. In the vertical relations between workers and capitalist, the worker is forced to sell their labor power to survive. In the horizontal relations between capitalists, companies must follow the laws of the market, which entails putting profit above all other considerations.[68] The capitalist system has a built-in strive for growth, fitting with the conventional wisdom that for a 'healthy' capitalism to operate, a certain level of economic growth is necessary.[69]

---

[64] Brenner, *Property and Progress*, 58; Søren Mau, *Mute Compulsion: A Marxist Theory of the Economic Power of Capital* (London & New York: Verso, 2023), 123.

[65] Costas Lapavitsas, *Profiting Without Producing: How Finance Exploits Us All* (London & New York: Verso, 2014), 4.

[66] Simon Clarke, ed., *The State Debate* (London: Palgrave Macmillan, 1991), 11.

[67] Roberts, 'What Was Primitive Accumulation?', 533.

[68] Ellen Meiksins Wood, *Empire of Capital*, 2nd ed. (London & New York: Verso, 2005), 10–11.

[69] Harvey, 'The Enigma of Capital and the Crisis This Time'.

States, in turn, must pursue such policies that sustain and support the capitalist system to ensure a sufficient level of growth.

These basic propositions are crucial points of reference throughout this dissertation. As I aim to show, the different modes of power that are intertwined in the field of international cyber law – law, technology, and security – are operationalized to sustain capitalism in an era where the capitalist economy spans the entire world. The information technology landscape has emerged out of the social relations of capitalism, reflecting capitalists' imperative to constantly seek out new venues for profit. In their international relations, states seek to sustain the social relations of capitalism by protecting the stable property relations on which these relations depend. States further seek to facilitate capital's continuous expansion, thus sustaining capital accumulation to uphold satisfying growth rates. These dynamics finds expression in the emerging content of international cyber law.

Tangibility and Intangibility

The technological developments at the center of international cyber law are characterized by a profound tension between tangibility and intangibility, reflected in many of the interpretative dilemmas in which states are currently finding themselves. The title of this dissertation seeks to capture this tension: The word 'cloud' is well-known both as a metaphor for the internet and as a model for computer data storage in which data is said to be located on a cloud somewhere. In the meteorological meaning of the word, a cloud is at once a real, physical phenomenon, appearing before us as visible objects, and at the same time a somewhat intangible phenomenon. The 'new' meaning of the word underscores how the digital appears before us as a real, yet intangible world detached from the 'physical' world – while at the same time, it does indeed have a physical location. Whereas digital content is always located on a cloud somewhere, the geography of the cloud is not decisive for who might see it, access it, and control it. This tension between tangibility and intangibility of the information technology landscape is central to its success. However, as I will show throughout this dissertation, it also results in sometimes contradictory imperatives for capitalist states in their endeavors to develop rules governing this digital reality: The need to ensure stability and reliability in the digital landscape, while facilitating and sustaining the global flows of capital. The tension between tangibility and intangibility is reflected in the vocabulary deployed within the field of international

cyber law – and, by extension, in the vocabulary deployed this dissertation. A few reflections on this vocabulary are therefore in place.

One term that I use frequently is *information technology*. A literal reading of the word *information technology* suggests that were here dealing with an incredibly broad term: Any type of tool deployable for the processing, storing, dissemination, or other type of handling of information would be included in the term. Ever since humans have had written language, different tools have been deployed for information purposes. Humans have manufactured tools for counting and calculating since ancient times such as the abacus and early mechanical clocks. In the 1600s, more complex instruments began to emerge, including the slide rule and mechanical calculators. By the early 1800s, the Industrial Revolution led to the development of mass-produced calculators like the arithmometer, along with innovations such as the punch card. However, when most people use the term 'information technology' today, they certainly do not think of the abacus; they conceive the word in a much narrower sense. A dictionary definition suggests that the term 'information technology' refers to 'the technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data',[70] thus delineating the technology applied by the term to the type of handling of information that involves the use of computer systems, software, and network. In this dissertation, I use the term to refer to digital computer technologies that works to process, store, retrieve, transmit, or in any other way handle information, including data (and metadata). I use the word digital technologies synonymously with information technologies.

Another related word central to this dissertation demands a few reflections: The word *cyberspace*. Despite its retro-futuristic sound, cyberspace has become the common term used to refer to the information technology landscape within the field of international cyber law. Originating in science fiction, the term was widely embraced by the pioneer internet users of the 1990s. The *cyberspace* metaphor first migrated into legal discourse via the work of academic commentators who advanced exceptionalist arguments about the special nature of internet-based activities that, they argued, could consequently not be seen as subject to existing legal regulation.[71] While the

[70] 'Definition of Information Technology', in *Merriam-Webster Online Dictionary*, 13 September 2024.

[71] David R. Johnson and David G. Post, 'Law and Borders - the Rise of Law in Cyberspace', *Stanford Law Review*, no. 48 (1997); Henry H. Jr. Perritt, 'Cyberspace and

exceptionalist arguments were eventually losing ground in positivist legal debates, the metaphor survived in mainstream discourse.

The metaphor's notion of spatiality effectively captures the social experience of the internet, often described with metaphors such as virtual room, world, or domain – and experienced as such by its users.[72] To specify, to the person in Sidney, Australia, who carries daily conversations with a friend in Lima, Peru, it has little relevance for their social experience that the information is located on a cloud in Iowa, United States. The spatial metaphor also captures another important feature of the information technology landscape: The existence of a realm beyond the tangible technology tools that this space is made up of – an intangible reality beyond the tangible components of a computer, a server, a wire, or a grid.[73]

Many of the ambiguities arising within the field of international cyber law thus arise from different ways of dealing with this 'something more' beyond the tangible technology tools. As we dive into the tension between the tangibility of information technologies and the intangibility of cyberspace, a dilemma unfolds. *On one hand*, the intangibility of cyberspace suggests the breaking down of spatial barriers – the existence of a borderless domain free from rules and restrictions. *On the other hand*, the existence of tangible properties under the control of their owners existing withing the jurisdictions of states. We are therefore dealing with an ambiguous spatiality: cyberspace is everywhere and nowhere – it is tangible and intangible at the same time. As we will see, this ambiguous spatiality reflects a broader ambiguity in the role of states in contemporary capitalism, which comes to be reflected in international cyber law.

Structure

Apart from the prologue and this short introduction, the dissertation consists of seven chapters followed by a conclusion and an epilogue. In ***chapter one***, I interrogate existing scholarly efforts of the field of international cyber law with the aim of demonstrating what I will argue to be their

---

State Sovereignty', *Journal of International Legal Studies* 3, no. 2 (1997): 155–204; Heather McGregor, 'Law on a Boundless Frontier: The Internet and International Law', *Kentucky Law Journal* 88, no. 4 (2000): 967–86.

[72] Julie E. Cohen, 'Cyberspace as/and Space', *Columbia Law Review* 107, no. 1 (2007): 210–56.

[73] For a critique of a tendency within the field of international cyber law to focus on tangibility of cyberspace, see Mueller, 'Against Sovereignty in Cyberspace'.

methodological shortcomings. On this basis, I turn in ***chapter two*** to Marxist legal theory to expand on the critique of the field through a Marxist lens and to build a framework through which we can approach the current process of making international cyber law. In ***chapter three***, I examine how the information technology landscape has emerged out of the social relations of capitalism. Challenging a prominent view that technology evolves independently of social and political forces, I argue that the most groundbreaking technological inventions have emerged in response to the crisis of stagnation in the 1970s and has ever since been developed to promote global capital accumulation at the costs of increasing inequality and exploitation. In ***chapter four***, I make a turn from the material reality to the ideational sphere, examining how the concept of cybersecurity has emerged and evolved in the relation between states. In ***chapter five***, I examine the emergence of the idea that 'cyberspace' is regulated by international law. I explore how the legal discourse on cyberspace has changed from exceptionality to unexceptionality and discuss how we can root this change in the relations between states and their role in sustaining the social relations of capitalism. In ***chapter six***, I zoom in on one of the legal doctrines that remain ambiguous within the field of international cyber law - the doctrine of sovereignty. I analyze the doctrinal debates surrounding the doctrine as a case-study of how a Marxist lens may help us understand the remaining ambiguities within the field of international cyber law. In the final chapter of the dissertation, ***chapter seven***, I move beyond the deconstructive endeavor of the previous chapters and look at past, present, and imaginary attempts at exercising resistance against contemporary digital infrastructures and constructing an alternative digital landscape.

CHAPTER I
LIMITS TO LEGAL POSITIVISM

A wealth of scholarship has already been written on the topic of international law and information technology. This scholarship has been dominated by positivist, or so-called doctrinal, approaches to international law. The scholars belonging to this tradition are all seeking to address different aspects of the same overarching question: *How does international law apply in cyberspace?* This question presumes that law can be distinguished from the social relations that it regulates – that law can be understood and theorized as a determinate, autonomous system of rules.

My inquiry is different: I ask *why* international cyber law develops as it does. The two questions – the *how*-question and the *why*-question – may appear closely related and mutually reinforcing. Perhaps, the *why*-question may seem like an innocent quest for further detail, for additional explanation of state-of-the-art. This is not wrong per se. However, the *why*-question does more than that. It carries an inherently critical intention. Asking *why* law develops as it does is premised on the rejection of the fundamental presupposition underlying the methodology of the field of international cyber law: the presupposition that international law can be understood and theorized as a determinate, autonomous system of rules.

To grasp the importance of the *why*-question, we must first recognize this implicit critique of the positivist scholarship asking the *how*-question. This requires a deeper dive into the positivist methodology and its shortcomings. As such, before embarking on my interrogation of the *why*-question, it is necessary to scrutinize the methodology underlying existing scholarly efforts

of the field of international cyber law. That endeavor is the purpose of this chapter.

My key claim is that the methodology of positivist international cyber law scholarship impedes it from grasping the dynamics shaping law's content. I argue that the positivist legal methodology confines legal scholars in an endless, circular endeavor to capture a reality that is constantly evolving according to logics that are entirely external to doctrine. It is therefore impossible to understand the emergence of regularities in what gets accepted as international cyber law within their methodological framework. In other words, I provide a methodological critique of the positivist scholarship of the field. I further argue that the inability to explain regularities within a positivist legal framework compels us to build a methodological framework that explains how and why certain ideas come to dominate and why these ideas take the form of law.

Positivism as an Analytic Metaphor

Despite the nascent character of international cyber law, the list of scholars working in the field is already long. I thus write this chapter well aware of the danger of making myself guilty of excessively crude simplifications, disregarding the inevitable varieties existing within any scholarly field. Regardless of that risk, I think that it is fair to hold on to the assertion that existing scholarship shares some common methodological characteristics. Existing scholarship on international cyber law is thus characterized by relying on a particular set of assumptions about international law, which I argue to be captured in the notion of 'positivism'. I use the term positivism as an umbrella term to describe a variety of approaches to international law that focus on describing the law as it is with reference to formal criteria, (seemingly) independently of moral or ethical considerations. For positivists, international law is no more or less than the rules to which states have consented through treaties and custom.[1] Through the act of *interpretation*, they strive to identify what international law *is*. Borrowing from Andrea Bianchi:

> The ultimate object of the game of interpretation is to persuade one's audience that his or her own interpretation of the law is the correct

[1] Steven R. Ratner and Anne-Marie Slaughter, 'Appraising the Methods of International Law: A Prospectus for Readers', in *The Methods of International Law*, Studies in Transnational Legal Policy ; No. 36 (Washington, D.C: American Society of International Law, 2004), 5.

> one. In other words, the winner is he or she who succeeds in securing adherence to his or her own interpretation.[2]

Positivists thus believe in the existence of a correct interpretative result that can be identified by the competent legal expert through the reliance on a set of authoritative interpretative techniques.

This does not *per se* mean that positivists are blind to the existence of a social reality, nor that they are blind to the existence of ambiguous rules. They may emphasize how their reliance on a positivist methodology 'does not necessarily imply subscribing to the view that there is only one correct answer to any legal problem'[3] or how 'international law is by nature a dynamic creature', the content of which thus 'evolve[s] over time in response to transformation of the … environment in which it applies.'[4] However, such acknowledgments often only come up in theoretical debates, in response to methodological criticism, or in discussions of the law of the future – *lex ferenda*. Thereby, they seem to consider the absence of definite answers a marginal problem that does not impact the overall validity of their methodology. These occasional acknowledgements of the existence of a social reality are thus not integrated into their analysis with any systematicity. Instead, positivist scholars may assert that law, *in many cases*, indeed does 'provide guidance regarding what to do or not to do'.[5] Despite the awareness of a social reality and the existence of several possible answers to a legal question, they thus appear to believe that this reality is theoretically distinguishable from the reality of *law* to such an extent that it is possible to examine the latter as an autonomous force.

Throughout this dissertation, I use the notion of legal positivism as an analytic metaphor for the wealth of scholarly attempts to answer different aspects of the overarching question of how international law applies in

---

[2] Andrea Bianchi, ed., *Interpretation in International Law* (Oxford: Oxford University Press, 2015), 36.

[3] Bruno Simma and Andreas L. Paulus, 'The Responsibility of Individuals for Human Rights Abuses in Internal Conflicts: A Positivist View', *The American Journal of International Law* 93, no. 2 (1999): 307.

[4] Michael Schmitt, 'The Law of Cyber Warfare: Quo Vadis?', SSRN Scholarly Paper (Rochester, NY, 2013), 271.

[5] Simma and Paulus, 'The Responsibility of Individuals for Human Rights Abuses in Internal Conflicts', 307.

cyberspace. In the following, I provide a more elaborate characterization of legal positivism and show its methodological shortcomings.

Characteristics of Positivism

This section examines the basic presuppositions on which the positivist methodology relies, showing how they are reflected in common argumentative techniques deployed in the scholarship on international cyber law. While the object of my interrogation is the field of international cyber law, the points that I make in this chapter are not specific to this particular area of international law. They are rather reflections of fundamental problems that have been demonstrated thoroughly elsewhere on a general level.[6] However, I aim to identify the prevalence of these problems in the scholarship of the field of international cyber law and thus illuminate the implications of these general insights for the specific area of international law with which I am concerned.

First, on the most fundamental level, the positivist methodology is based on the presupposition of the coexistence of free, sovereign and equal states. The presupposition reflects an idea that the starting point of the development of legal commitments is a reality in which sovereign states confront each other as free and equal entities. From this starting point of peaceful coexistence, international legal obligations imply a restriction of states' sovereignty based on their consent. Every legal norm is thus derivable from sovereign states' free will, while simultaneously implying a restriction of that will. The assumption of an abstract individuality – the absence of a preexisting hierarchy – is thus fundamental to the philosophical foundation on which positivism relies.[7] International law, in other words, consists of obligations to which they have voluntarily consented towards each other. As I will show throughout this section, the positivist methodology is entirely structured around this presupposition; its ways of generating knowledge are all centered on identifying the obligations that sovereign states have consented to undertake. An illustrative example of the presupposition that international law is derived from the consent of sovereign states in the context of international cyber law scholarship is Heintschel von Heinegg's argument that 'there may be a need for a consensual adaptation [of international law]

[6] See Koskenniemi, *From Apology to Utopia*; Lawrence B. Solum, 'On the Indeterminacy Crisis: Critiquing Critical Dogma', *University of Chicago Law Review* 54, no. 2 (1987): 462–503.

[7] Koskenniemi, *From Apology to Utopia*, 94–95.

to the specific characteristics of cyberspace.'[8] Another example is Kevin Jon Heller's observation that '[s]ignificant differences … remain concerning how international law applies to cyberspace, because States have been unable to agree on what kinds of cyber operations international law prohibits.'[9] Michael Schmitt similarly argues that states drive the evolutionary process of interpreting and applying international law to cyberspace, as 'international law represents consensus among states as to the rules of the game that govern their interactions.'[10] The task for international legal scholars, then, is to identify the common will of sovereign states to determine the specific commitment to which they have consented.

The presupposition of equality between sovereign states is not only problematic because the abstract equality shields over their material inequality (a point that I will elaborate on in chapter two). Already on an abstract, conceptual level, the assumption suffers from the fundamental problem that two entities cannot be both free and equal at the same time. Once the respective wills of the two entities collide, the will of one entity must inevitably be put aside in favor of the will of the other entity. This problem becomes clearer as we dive into the positivist techniques for identifying extant legal norms. However, it is important to note that the problem arises already from this very fundamental presupposition.

The consent of sovereign states is, in itself, a poor input for doctrinal analysis; to examine what states have consented to, it is necessary with a more specific unit of analysis. This brings us to the second presupposition underlying the positivist methodology: the presupposition that legal sources express the will of sovereign states, and that it is thus possible to determine international law's content be resorting to these sources. The classic doctrine of sources was developed in the 19th century and later codified in Article 38(1) of the Statute of the International Court of Justice. Following Mathilda Arvidsson and Miriam Bak McKenna, the doctrine 'entrenches international legal discourse and argumentation in the historical and contemporary behaviour, will and interests of States.'[11] The doctrine of sources thus appears as a key tool for identifying the specific obligations to which states have

[8] Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace', 123–24.

[9] Heller, 'In Defense of Pure Sovereignty in Cyberspace', 1433.

[10] Schmitt, 'The Law of Cyber Warfare', 272.

[11] Arvidsson and McKenna, 'The Turn to History in International Law and the Sources Doctrine', 5.

willingly committed. In the context of international cyber law, this idea is explicated by Schmitt who asserts:

> States consent [to international law] either by opting into treaty regimes or by engaging in practices out of a sense of legal obligation (opinio juris) that, combined with similar practice by other states, eventually crystallizes into customary international law.[12]

In this common view, the sources of international law reflect the consent of states to this or that specific commitment. As is reflected in Schmitt's assertion, the two central sources of international law are conventions and customary international law. Since no conventions currently regulate the specific area of information technologies on a global scale, international cyber law scholars have centered their attention on how general international conventions, particularly the Charter of the United Nations, the Geneva Conventions and additional protocols, and, occasionally, international human rights treaties, apply to the new reality of information technology.

Customary international law arises when a particular way of behaving is *a)* followed as a general practice amongst states, and *b)* accepted by those states as legally binding (commonly referred to as the requirement of *opinio juris*).[13] These two criteria are frequently referred to as the objective and the subjective element of custom, respectively. Traditionally, the doctrine of customary international law has primarily centered on the objective element. The observation of consistent, long-standing state practice in the form of concrete, material action of states has thus been the central criterion for customary law. Meanwhile, the subjective element – *opinion juris* - has been a secondary consideration that served the purpose of distinguishing (legal) obligations from (non-legal) habits.[14] However, a 'modern doctrine' of customary international law has arisen in recent years. The modern doctrine prescribes that the subjective element is the starting point of analysis; states' general statements on rules have become more central, while the 'real' practice of states has been put in the background.[15] The field of international cyber law is an archetypical example of the modern doctrine of customary international law. The scholarship of the field is thus centered on analyzing

[12] Schmitt, 'The Law of Cyber Warfare', 272–73.

[13] Anders Henriksen, *International Law* (Oxford: Oxford University Press, 2021), 23.

[14] Roberts, 'Traditional and Modern Approaches to Customary International Law', 758.

[15] Roberts, 758.

unilateral position papers in which states declare their general views on the cyber-specific content of rules. These papers have been taken as indicative of practice and *opinion juris* merged in one document, making the assessment of the 'real' practice of states largely superfluous. The distinction between the objective and subjective element of customary international law has thus arguably lost much of its meaning in the context of international cyber law.

However attractive it may seem from a scientific perspective with such a definite and authoritative list of empirical material, the positivist reliance on sources suffers from a problem: International legal norms, as expressed in sources, are ambiguous and often conflicting. The problem is particularly evident in the context of international cyber law, in which rules are frequently admitted being 'poorly demarcated' or uncertain.[16] It is thus easy for states to assert that they did not consent to this or that understanding of this or that rule of international law. As an illustration of this problem, let us consider the Russian influence operations against the United States in the context of the presidential election in 2016. According to an American intelligence report:

> Russian President Putin authorized, and a range of Russian government organizations conducted, influence operations aimed at denigrating President Biden's candidacy and the Democratic Party, supporting former President Trump, undermining public confidence in the electoral process, and exacerbating sociopolitical divisions in the US.[17]

The events have spurred a wealth of academic debate on the legality of influence operations. The international legal concept that has drawn the most attention is the prohibition of intervention into the internal or external affairs of other States.[18] It has also been frequently discussed whether the

---

[16] Schmitt, 'Grey Zones in the International Law of Cyberspace', 1.

[17] National Intelligence Council, 'Foreign Threats to the 2020 US Federal Elections', Intelligence Community Assessment, 10 March 2021.

[18] Duncan Hollis, 'The Influence of War; the War for Influence', *Temple Journal of International & Comparative Law* 32 (2018); Barrie Sander, 'Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections', *Chinese Journal of International Law* 18, no. 1 (2019): 1–56; Dale Stephens, 'Influence Operations & International Law', *Journal of Information Warfare* 19, no. 4 (2020): 1–16; Henning Lahmann, 'Information Operations and the Question of Illegitimate Interference under International Law', *Israel Law Review* 53, no. 2 (2020): 189–224;

doctrine of sovereignty, which we will discuss in detail in chapter six, might be violated by influence operations.[19] However, these concepts remain ambiguous in cyberspace, leading Schmitt to the assertion:

> Russia cleverly operated in the grey zone of international law with respect to the two rules their operations implicated, the obligation to respect the sovereignty of other states and the prohibition on intervention into their internal affairs. This hobbled the American response.[20]

A doctrinal account of the arguments and concerns put forward in relation to each of these legal standards is beyond the scope of this chapter. Rather, the key point is that the current uncertainty surrounding the cyber-specific application of general international legal concepts illuminates the indeterminacy arising from the latent conflict between legal sources. As long as states disagree on the cyber-specific implications of sovereignty and non-intervention, it is impossible to reconcile the conflicint views, and thus determine the content of international cyber law, without resorting to an element external to the practice of states (the strategies for which we will get back to soon).

While the ambiguity of the sources of international law is remarkably obvious in the context of international cyber law, in which numerous legal questions remain overtly unresolved, it is important to underscore that the problem of the ambiguity of sources is always there. Whenever a conflict arises between two states, which are formally sovereign and equal, state A may invoke a particular treaty obligation against state B. However, on a very basic level, state B can always invoke its own sovereign freedom from which the treaty obligation is derived and hold that it did not intend with the treaty to restrict its sovereignty in this or that particular manner.[21] Because the value of international legal sources is ultimately derived from the consent of sovereign states, it is in principle always possible to produce a

---

Michael Schmitt, 'Foreign Cyber Interference in Elections', *International Law Studies* 97, no. 1 (2021): 744.

[19] Schmitt, 'Foreign Cyber Interference in Elections', 754; Sander, 'Democracy Under The Influence'; Lahmann, 'Information Operations and the Question of Illegitimate Interference under International Law'.

[20] Michael Schmitt, 'The Law of Cyber Conflict: Quo Vadis 2.0?', in *The Future of Armed Conflict*, ed. Matthew Waxman and Thomas Oakley, The Lieber Studies Series (Oxford: Oxford University Press, 2022).

[21] Koskenniemi, *From Apology to Utopia*, 64.

coherent international legal argument in favor of any state position. In cases of conflict, an adjudicator must therefore choose one interpretation over another, and thereby, choose the will of one sovereign over the will of another.

The issue of conflicting legal sources brings me to introduce a *third* basic presupposition underlying positivist scholarship: through an exercise of interpretation, it is possible to ascertain the correct understanding of specific international legal rules. This belief relies on the notion that it is possible to perform two tasks in an objective manner: *1)* identify neutral principles, and *2)* apply them to concrete occurrences. As accurately summarized by Nigel Purvis:

> Because it needs to construct some grander abstraction or higher-level theory before it can resolve a case, liberal legality must allow for determinate theorizing. Because it must apply abstractions to concrete factual materials in such a way as to produce legal outcomes, liberal legality must achieve determinate application.[22]

The positivist methodology presupposes its ability to perform both tasks. Positivist scholars thus believe that it is possible ultimately to discern the correct application of old legal norms to the new reality of cyberspace – that is, they believe in the idea of an 'immanent intelligibility of norms'.[23] Deductive reasoning can 'yield determinate answers to specific legal questions', leading to neutral interpretative results that are free from bias.[24] In their endeavors to explicate their methodology for this act of interpretation, positivists often resort to the general rules of interpretation laid out in the Vienna Convention Article 31, which provides a list relevant considerations to take into account in the interpretation of a treaty to identify the 'ordinary meaning to be given to the terms of the treaty in their context and in the light of the purpose of the treaty'. The considerations established by the Vienna Convention all center on identifying the will of the contracting states from which the obligation is derived.

Based on these inputs, the scholars of the field of international cyber law are committed to coming as close as possible to describing the law as it is,

---

[22] Nigel Purvis, 'Critical Legal Studies in Public International Law', *Harvard International Law Journal* 32, no. 1 (1991): 106.

[23] Jean d'Aspremont, 'International legal positivism' in Jeffrey L. Dunoff and Mark A. Pollack, eds., *International Legal Theory: Foundations and Frontiers*, 1st ed. (Cambridge: Cambridge University Press, 2022).

[24] Fleur Johns, 'Critical International Legal Theory' in Dunoff and Pollack, 135.

debating how particular norms of international law are most accurately identified, interpreted, and applied to the new reality of information technology. The act of interpretation is thus seen as a technical exercise, the success of which depends on the expertise of the interpreter. In that spirit, the Tallinn Manual describes its mission as that of bringing together 'distinguished international law practitioners and scholars, the so-called 'International Group of Experts' … in an effort to examine how extant legal norms apply to this new form of warfare.'[25] This mission reflects a perception of legal norms as an autonomous, natural (understood as *non-social*) reality that can be exposed through a rigorous interpretative endeavor. The distinguished experts of the field are tasked with the scientific task of identifying, interpreting and applying extant legal norms to cyberspace.

The presupposition that rules have an autonomous existence is further reflected in the way that scholars of the field frequently speak of 'long-standing public international law norms' and of 'existing international law'. The cyber-specific content of these existing rules will be unraveled through the exercise of interpretation.[26] Such attitudes reflect a belief amongst scholars of the field in the capacity to produce determinate answers to particular questions of international law's application to the reality of information technology.[27] As such, they believe that it is generally possible to reach a neutral interpretative result.

The presuppositions underlying positivist scholarship – the reliance on the free consent of sovereign equal states, the resort to formal sources, and the deployment of authoritative interpretative techniques – all assume that legal norms can be neutrally determined within a self-contained system of rules. However, as the field of international cyber law strikingly demonstrates, this presupposition falls apart when faced with the reality of the ever-evolving nature of state practice. The positivist approach struggles to explain how legal change occurs and why certain interpretations gain dominance over others. This issue is particularly evident in the doctrine of customary international law, where the source of law cannot be formally distinguished

[25] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 1–2.

[26] Schmitt, 'The Law of Cyber Conflict'; Michael Schmitt and Sean Watts, 'Beyond State-Centrism: International Law and Non-State Actors in Cyberspace', *Journal of Conflict and Security Law* 21, no. 3 (2016): 595–611.

[27] Fleur Johns, 'Critical International Legal Theory' in Dunoff and Pollack, *International Legal Theory*, 135.

from its application or its violation. As I will explore in the following, this methodological limitation results in an inherent circularity, impeding positivist scholars from producing meaningful conclusions on international cyber law.

Circularity of Doctrine

The positivist assumption that legal norms can be neutrally determined within a self-contained system of rules is particularly striking in the context of international cyber law, because it contradicts a simultaneous acknowledgement within this branch of scholarship: central legal questions are currently unsettled; international cyber law contains multiple ambiguities or 'gaps.' In chapter five, we will explore further how the positivist scholars cope with this contradiction. However, let me first elaborate on the positivist methodology for clarifying the content of international cyber law in these cases of ambiguity. In accordance with the presupposition that international law is derivable from the will of sovereign states, the specific meaning to be given to abstract legal terms is generally clarified through the observation of the views of states. The central endeavor of the scholars of the field is thus to search for emerging consensus in states' unilateral positions on international cyber law.[28] Positivist scholars are, however, challenged in this task because of the frequent occurrence of contradictions in the positions of states.[29] The continuous emergence of new position papers may further disturb the picture by modifying or refusing current understandings of law and thus leading to evolutions in *lex lata.*

To illustrate how new state-practice always has to potential to cause ambiguity around rules that were once perceived well-established, let us consider the debates surrounding the cyber-specific application of the right to self-defense, provided by article 51 of the Charter of the United Nations and widely regarded as reflective of customary international law. The central discussion surrounding the right to self-defense against cyberattacks has been whether cyberattacks causing solely economic damage might

[28] Amongst many others, Biller, 'The Strategic Use of Ransomware Operations as a Method of Warfare', 486; Watts and Richard, 'Baseline Territorial Sovereignty and Cyberspace', 809; Heller, 'In Defense of Pure Sovereignty in Cyberspace'; Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace'; Schmitt, 'Grey Zones in the International Law of Cyberspace'.

[29] François Delerue, 'Reinterpretation or Contestation of International Law in Cyberspace?', *Israel Law Review* 52, no. 3 (2019): 295–326.

constitute an 'armed attack' in the sense of article 51. Until recently, an interpretation of the threshold in article 51 in the context of economic damage would appear as an easy task for the competent adjudicator: Throughout the negotiation of the Charter of the United Nations, Western states insisted on upholding a distinction between economic damage and physical damage.

However, some states have now begun to reconsider the threshold. France has thus opened the door for the opportunity that economic damage suffices to categorize a cyberattack as an armed attack, and Finland has held that the question of whether a cyberattack producing 'significant economic effects such as the collapse of a State's financial system or parts of its economy should be equated to an armed attack' merits further consideration.[30] Relatedly, Norway has asserted that 'the use of crypto viruses or other forms of digital sabotage against a State's financial and banking system, or other operations that cause widespread economic effects and destabilisation, may amount to the use of force in violation of Article 2(4).'[31] Notably, other states take the opposite view, and the question thus remains ambiguous.

Within a positivist legal framework, we can merely scrutinize and compare the prevalent state positions on the question and note how the right to self-defense might eventually undergo an expansion as states continue to publish and further detail their positions. The underlying material developments that may or may not lead to a legal change have no place within this framework. We can thus only speculate silently about how the distinction between economic and physical damage has historically been key to the legitimation of the imposition of destructive economic sanctions against newly independent states without any legal repercussions – and how an increasing exposition to the risk of economic damage in advanced capitalist states due to growing digital vulnerabilities of the financial sector might cause some of these states to reconsider this distinction. The possible legal evolution in the

[30] Ministry of Defense of France, 'International Law Applied to Operations in Cyberspace', 9 September 2019; Finland, 'International Law and Cyberspace - Finland's National Positions', 15 October 2020.

[31] GGE compendium of voluntary contributions, 'Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution' (United Nations, 13 July 2021), 70.

thresholds of the *jus ad bellum* regime in the context of international cyber law illustrates how the positivist methodology is incapable of producing determinate answers to specific legal questions. States' practice is continuously evolving according to considerations that are external to any legal logic. Because state practice is always (potentially) evolving, and because this evolution follows no particular legal logic, the interpretative endeavors of positivists will always be confined to an empty description of symptoms – without any sense of their underlying causes.

As I hinted at in the beginning of the preceding section, the problem facing international cyber law scholars in their efforts to identify how international law applies in cyberspace is a consequence of their methodological starting point: the presupposition of sovereign, equal states. Due to this presupposition, the center of analysis becomes the will of states. However sophisticated lists of sources they study and interpretative principles they deploy, they are unable to explain why the will of some states ultimately win over others. While this problem is just as prevalent in the interpretation of conventions as in the identification of customary international law, the latter is more illustrative of the problem. Let us therefore take a closer look into the circularity inherent in the doctrine of customary international law.

As explained above, customary international law arises when a particular way of behaving is followed as a general practice amongst states and is accepted by those states as legally binding (commonly referred to as the requirement of *opinio juris*).[32] However, any state conduct – even conduct that violates a rule – is state practice, and thus, borrowing a metaphor from Anthea Elizabeth Roberts, the seed for (new) custom with a potential to sprout.[33] Eventually, an apparent violation may effectively repeal or modify an existing customary rule. To avoid tautology, it is necessary that not all practice of all states be law. We need a way of clearly distinguishing practice constituting a rule from other practice. Here is the difficult question: How do we determine if a particular conduct aligns with an existing customary rule, and if it does not, if it constitutes a new rule, a modification of the original rule, or a violation of it? In other words: How do we determine if, and when, a seed for new custom will sprout? When a particular practice comes to constitute a new rule or a modification of the original rule, the conduct has turned from being a *violation of law* into being a *source of law*.

---

[32] Henriksen, *International Law*, 23.

[33] Roberts, 'Traditional and Modern Approaches to Customary International Law', 784.

Positivist legal theorists have come up with various suggestions as to how we can define the point at which the process of a practice turning into law *has happened*. However, they overlook the very mystery, which is *how it happens*. The International Law Commission (ILC) recently undertook the endeavor to 'articulate the methodology for identifying customary international law', a process which resulted in a document of draft conclusions published in 2018.[34] Conveniently, the ILC left the most complex questions out of its analysis:

> Dealing as they do with the identification of rules of customary international law, the draft conclusions do not address, directly, the processes by which customary international law develops over time. Yet in practice identification cannot always be considered in isolation from formation; the identification of the existence and content of a rule of customary international law may well involve consideration of the processes by which it has developed. The draft conclusions thus inevitably refer in places to the formation of rules of customary international law. They do not, however, deal systematically with how such rules emerge, change, or terminate.[35]

The process through which customary international law emerges, changes, or terminates, is where the shortcoming of positivism becomes most clear. The process is, to quote D'Amato, 'wrapped in mystery and illogic.'[36] Even Joseph Kunz has acknowledged that the very coming into existence of a rule of customary international law would presuppose that the states acted in legal error, and he admits that the problem 'has not yet found a satisfactory solution.'[37] At its core, the doctrine entails that the practice of states regulates the practice of states. Since the practice of states constantly evolves, so does customary law. The formally identical nature of the means and the end of regulation means that the identification and application of customary international law cannot be separated from its creation. The forces that determine what comes to be thought of as law are necessarily external to doctrine:

---

[34] International Law Commission, 'Draft Conclusions on Identification of Customary International Law with Commentaries' (United Nations, 2018), 2.

[35] International Law Commission, 4.

[36] Anthony D'Amato, *The Concept of Custom in International Law* (Cornell University Press, 1971), 4.

[37] Josef L. Kunz, 'The Nature of Customary International Law', *American Journal of International Law* 47, no. 4 (1953): 667.

Doctrinal sources' ultimate reliance on the will of formally equal, sovereign states makes the positivist methodology incapable of explaining which state's will wins in cases of conflict. It is impossible to theorize legal change without an element external to doctrine.

Ways of Coping

The problem of positivist legal scholarship's inability to explain which practice becomes law and which practice becomes a violation thereof cannot be reduced to some marginal problem of international law. Rather, it reflects a paradox inherent in the liberal idea of sovereign equality on which the positivist approach relies. To illuminate this paradox, this section scrutinizes two solutions to which positivist scholars have frequently resorted in response to the problem of substantial indeterminacy.

Scholars broadly resort to two argumentative techniques, often in combination: *First,* they consider the power dynamic and strategic interests of states, and *second,* they emphasize normative considerations about which interpretation better suits a set of values deemed universally important. Let us first consider the arguments of scholars who have resorted to the strategic interests of states as an indication of the direction that international legal norms will take. One scholar taking this approach is Matthew Waxman. Acknowledging that 'strategy is a major driver of legal evolution', he asserts that 'major actors … have divergent strategic interests that will pull their preferred doctrinal interpretations and aspirations in different directions, impeding formation of a stable international consensus'.[38] He therefore focuses his analysis on the 'dynamic interplay of law and strategy', in which 'strategy generates reappraisal and revision of law, while law itself shapes strategy – and the moves and countermoves among actors with varying interests, capabilities, and vulnerabilities.'[39] Because states' strategic interests may be conflicting, legal line drawing is 'likely to be shaped by power relations.'[40] As such, '[t]hose with more power have greater ability to promote through State practice their preferred interpretation.'[41] In a similar vein, Schmitt argues that '[t]he more states rely upon cyberspace for essential

[38] Matthew C. Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)', *Yale Journal of International Law* 36, no. 2 (2011): 425.

[39] Waxman, 425.

[40] Matthew Waxman, 'Cyber Attacks as "Force" Under UN Charter Article 2(4)', *International Law Studies* 87 (2011): 44.

[41] Waxman, 51.

functions, day-to-day activities, and well-being, the starker their strategic choice becomes regarding international law'[42], thus presupposing that states choose their legal position on the basis of strategic interests. He further asserts that a 'state's national interests undergird its consent or conduct, and, thus, the development of international law', thus predicting a 'turbulent period' for the law of cyber warfare, since the current international legal norms are being adjusted to the 'changing national interests of states in cyberspace'.[43] In his analysis of cyber sovereignty, Kevin Jon Heller supplements his analysis of which position is the stronger position 'legally' with an analysis of which position is more attractive for states from a policy-perspective.[44] Acknowledging that the current state of law is uncertain and will ultimately be clarified through states' positions, he describes the current moment as a 'process of custom-formation'. In that process, taking strategic interests of states into account appear as a way of 'predicting' the course of legal development.[45] As an analytical maneuver, the emphasis on the strategic interests of powerful states works to resolve the problem of apparent indeterminacy of international cyber law: It adds an element external to law itself that can determine which interpretation will win when two interpretations collide.

However, the maneuver gives the scholars two problems. The *first problem* relates to their conceptualization of international law: By conceptualizing law as a reflection of the strategic interests of powerful states, the scholars fail to explain why this exercise of power takes the form of *law*. Essentially, law's contingency on the strategic interests of powerful states deprives rules of their normative status, and thus, their character as something distinguishable from pure force. The *second problem* relates to their understanding of the central concepts with which they operate - strategy, power, and interests. If these concepts determine legal developments, then an adequate analysis of legal developments requires an adequate theory of these concepts. However, the scholars tend to operate with reductionist and undertheorized concepts that neglect how different social spheres exist within states and how the interests of various social groups within and across societies are inherently conflictual. The identification of a national interest to base a policy on

[42] Schmitt, 'The Law of Cyber Conflict', 5.

[43] Schmitt, 'The Law of Cyber Warfare', 273.

[44] Heller, 'In Defense of Pure Sovereignty in Cyberspace'.

[45] Heller, 1496.

inevitably implies the favoring of one interest over another.[46] Their one-dimensional notion of strategic 'national interests' thus usually ends up universalizing the interests of the elite classes of elite states as the unitary will of the international community of states.[47] These scholars thus come to neglect the real, underlying struggles taking place in societies with a plurality of interests, contestations and conflicts, thereby losing sense of the underlying selective dynamics leading to the promotion of particular interests over others.

The second way of escaping the circularity of doctrine is to resort to normative ideas, raised above the practice of individual states. This technique is reflected in a common assumption that international law works to promote and protect international stability and predictability and ensure peace and order in the international community.[48] If international law has a normative purpose above the will of sovereign states, some views can be promoted as more legitimate than others by being more in line with international law's transcendent purpose. This approach translates into assumptions that certain types of state behavior are conceived as bad, and others are conceived as good. These normative ideas are particularly visible when scholars turn to assess the 'adequacy' of international existing international law for the regulation of cyberspace. For example, Duncan B Hollis argues that areas exist where existing rules of international law are simply insufficient to address the new reality of information technologies. Specifically, he points to states' response options against information operations conducted by non-state actors being inadequate.[49] Such an argument relies on the assumption that international law should work to prevent a certain type of

---

[46] For an elaboration of this problem, see B.S. Chimni's critique of the tradition of legal realism in international law. Chimni, *International Law and World Order*, 54.

[47] B. S. Chimni, 'Customary International Law: A Third World Perspective', *American Journal of International Law* 112, no. 1 (2018): 33.

[48] Delerue, 'Reinterpretation or Contestation of International Law in Cyberspace?', 311; Anthony D'Amato, 'International Law, Cybernetics, and Cyberspace', ed. Michael N. Schmitt and Brian T. O'Donnell, *International Law Studies*, no. 76 (1999): 68; Harriet Moynihan, 'The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace', *Journal of Cyber Policy* 6, no. 3 (2021): 406.

[49] Duncan B. Hollis, 'Why States Need an International Law for Information Operations Symposium: Crimes, War Crimes, and the War on Terror', *Lewis & Clark Law Review* 11, no. 4 (2007): 1023–62.

behavior that is deemed in violation of some grand norm of international peace beyond what follows immediately from applicable international law.

Similarly, Schmitt expresses concern about the 'short-sighted nationalistic geopolitics' of some states, which is 'impeding an interpretive journey that will benefit all members of the international community.'[50] As such, despite his general acknowledgement that states act in accordance with their strategic interests, which will ultimately shape legal outcomes, he also assumes the existence of such thing as an interest of the 'international community', the promotion of which some states are counteracting by prioritizing their strategic interests. This normative assumption also reveals itself in his observation of a tendency to consider international law an 'effective tool in deterring harmful cyber activities', reflecting an underlying normative assessment that some activities are inherently harmful and others are inherently worthy of protection.[51] Similarly, in a critique of the emergence of a position that sovereignty is only a principle, and not a rule, Schmitt contends that 'such a position would dismantle a key normative firewall safeguarding U.S. cyber infrastructure and activities', expressing hope that the ambiguity introduced by this interpretation will remain only temporary.[52] While legal scholars tend to have a stronger weight on either states' strategic interests or normative ends, they often combine the two, thus remaining in an oscillation between emphasizing state behavior and emphasizing normativity. As I will show in the following, the two ways of coping, and the oscillation between the two, are reflective of a paradox inherent in the liberal idea of sovereign equality on which the positivist approach relies.

From Apology to Utopia

The two ways of coping with the circularity of doctrine described above reflect what Koskenniemi has theorized as the ascending and descending strand of argument in international law, or apology and utopia, respectively. The former strand of argument attempts to ensure the law's *concreteness* by rooting it in the actual behavior and interest of states. The latter attempts to ensure the law's *normativity* by creating distance between law and the behavior, will, and interests of states. Ascending arguments guarantee that the law is objective in the sense of being concrete, that is, unrelated to a material

[50] Schmitt, 'The Law of Cyber Conflict'.

[51] Schmitt.

[52] Schmitt, 'Grey Zones in the International Law of Cyberspace', 5.

theory of justice.[53] It thereby gives expression to the central principle of sovereign equality by emphasizing the will of states.[54] However, it also results in the loss of the law's normativity; it becomes indistinguishable from a simple description of state behavior. In other words, it becomes apologetic. A descending argument, on the other hand, manages to uphold a distinction between law and behavior. However, this argument is vulnerable to the objection of naturalism; if law bears no relation to what states have accepted, law is assumed to exist as a natural morality, meaning that the argument becomes utopian. To avoid such utopianism, we must 'establish the law's content so that it corresponds to concrete State practice, will and interest.'[55] As such, the argument needs an ascending justification, 'a link to the subjective acceptance of the State against which we apply the law.'[56] As such, legal reasoning cannot rely entirely on either of the two without being vulnerable to an accusation of being either utopian or apologetic.

The contradiction between the ascending and descending patterns, and the inability of legal doctrine to prefer either, provides the dynamics of the international legal argument.[1] Doctrine is therefore forced to maintain itself in constant movement from emphasizing concreteness to emphasizing normativity and vice-versa without being able to establish itself permanently in either position.[57] When legal scholars debate the content of international cyber law, they are thus subject to a twofold constraint: *On the one hand*, their legal interpretations must be anchored in the real will and practice of states to avoid utopianism. *On the other hand*, their legal interpretations must point to a certain normative commitment to avoid apology. By remaining in oscillation between the two strands of argument, the legal scholars seek to avoid exposing the circularity of their methodology, which in itself contains no criteria for determining which practice of which states turn into law.

While Koskenniemi's thorough and rigorous critique of the liberal paradox inherent in the legal language is compelling, his general, structurally founded critique gives us little sense of the real, systemic subordinations that are enabled by the structural indeterminacy.[58] Ntina Tzouvala captures well this inadequacy:

---

[53] Koskenniemi, *From Apology to Utopia*, 64.

[54] Koskenniemi, 64.

[55] Koskenniemi, 66.

[56] Koskenniemi, 64.

[57] Koskenniemi, *From Apology to Utopia*.

[58] Miéville, *Between Equal Rights: A Marxist Theory of International Law*, 53–54.

> The shortcoming of this explanatory scheme is that it displaces the problem from one set of texts (international law) to another (the works of liberalism). It does so without reflecting on why liberalism carries these impossible contradictions in the first place and, more importantly, why and how these contradictions become invisible and, at the end of the day, inconsequential in so far as liberalism remains hegemonic.[59]

The limitations to Koskenniemi's structuralist framework are important, and the need to move beyond empty deconstruction and root the operations empowered by liberal legality in the underlying material conditions is central to this study. But despite this limitation to Koskenniemi's work, I think that his structuralist exposition of international legal discourse remains the most compelling demonstration of international law's indeterminacy. Above all, his analysis distinguishes itself from other scholarly work on the indeterminacy of international law by operating with two notions of indeterminacy: The substantial determinacy and the structural indeterminacy. The substantial indeterminacy arises from the *ambiguity of language*. Most legal scholars recognize a certain penumbra of uncertainty to any linguistic expressions; words such as 'aggression', 'self-defense', 'war', and 'intervention', are notoriously ambiguous and require an exercise of interpretation before they are applicable in practice.[60] The existence of instances of substantial indeterminacy in international law is broadly recognized, also within mainstream international legal scholarship.[61] However, the substantial indeterminacy is often neglected as a peripheral phenomenon that resonates poorly with the practical life of international law, in which 'almost all nations observe almost all principles of international law and almost all of their obligations almost all the time', as famously put by Louis Henkin.[62] Here,

---

[59] Tzouvala, *Capitalism As Civilisation*, 35.

[60] Koskenniemi, *From Apology to Utopia*, 38.

[61] See for example Myres S. McDougal, 'Law and Power', *The American Journal of International Law* 46, no. 1 (1952): 102–14; Myres S. McDougal, 'Perspectives for an International Law of Human Dignity', *Proceedings of the American Society of International Law at Its Annual Meeting* 53 (1959): 107–36; Myres McDougal, Harold Lasswell, and W. Michael Reisman, 'Theories About International Law: Prologue to a Configurative Jurisprudence', *Faculty Scholarship Series*, 1968.

[62] Louis Henkin, *How Nations Behave: Law and Foreign Policy* (Council on Foreign Relations, 1979).

Koskenniemi's concept of structural indeterminacy is a radical strengthening of the critique of indeterminacy: The structural indeterminacy of international law does not merely refer to a general ambiguity of language, which can be eventually resolved through clarifying practices. Rather, the structural indeterminacy is a property *internal to international legal discourse*. The constant oscillation between concreteness and normativity allows a competent legal interpreter to construct a valid argument for any given result in any given situation. This means that we cannot accept the legal reasons provided for a given result as the real reasons for the result; this result is merely symptomatic of forces that are external to doctrine. The liberal conception of the 'rule of law' thus serves to mystify and legitimate the legal system and thereby obscure the underlying dynamics.[63] Quoting Miéville, the distinction between substantial and structural indeterminacy allows us to see that 'legal relations cannot be separated off either from moral or from "political" relations with any systematicity. *This does not represent the failure of the theory but the peculiar nature of modernity*.'[64] While the content of legal norms is thus ever-changing, positivists insist on fitting the changing content into its interpretive doctrine by classifying it in accordance with a fixed list of inputs. The doctrine – the form – remains static, while the content is ever changing according to dynamics entirely external to doctrine.

Indeterminacy of International Cyber Law

This chapter began with the observation that the nascent academic field of international cyber law has been dominated by positivist, or doctrinal, approaches to international law. Throughout the chapter, I detailed this observation by outlining a set of common presuppositions central to what I understand by positivist international legal scholarship and demonstrating the prevalence of these presuppositions in the growing body of scholarship concerned with international cyber law. Through an elucidation of the shortcomings of each of these presuppositions, I demonstrated the positivist scholars' inability to justify their ways of generating knowledge: their methodology is inherently circular. This reality is reflected in Shirley V. Scott's assertion that 'the questions as to whether and why states 'obey' international law are no longer meaningful. It can now be seen that states neither

[63] Solum, 'On the Indeterminacy Crisis', 462.

[64] Miéville, *Between Equal Rights: A Marxist Theory of International Law*, 150.

obey nor disobey international law.'[65] But even though questions of obeyance are entirely meaningless, the distinction between lawful and unlawful remains crucial. Indeed, there is no inherently 'legal' logic determining the distinction. But the determination of legality *does* take place, and it surely matters. Framing particular decisions and practices in the language of international law is a powerful way of giving them legitimacy and making them seem natural and unquestionable. The illusion of a distinction between the making of law and its interpretation thus has a specific function in international law. Quoting Boer, 'it means that whoever makes a legal argument will have to base their claims on the primary sources of law – or at least make it seem as if they do.'[66] By basing an argument on an interpretation of legal sources, the claim that it supports appears raised above political contestation.

Existing scholarship on international cyber law has failed to offer a systematic, theoretically coherent framework for explaining the emergence of consensus on international rules governing cyberspace. Because of the inability to explain what is accepted as law within a positivist framework, we are compelled to search *beyond* this methodological framework if we want to make sense of the field of international cyber law – that is, if we want to understand why the field has emerged and taken shape in a certain way. To study the field of international cyber law in a scientific way, we must in other words begin by stepping outside of it. Acknowledging that substantial determinacy occurs despite the underlying structural indeterminacy, the task ahead of us is to outline a way of approaching the field of international cyber law that explains why certain ideas come to dominate and why these ideas take the form of law. This will be the endeavor in the following chapter.

[65] Scott, 'International Law as Ideology', 325.

[66] Lianne J.M. Boer, *International Law As We Know It: Cyberwar Discourse and the Construction of Knowledge in International Legal Scholarship* (Cambridge: Cambridge University Press, 2021), 6.

CHAPTER II
A MARXIST LENS

In the preceding chapter, I argued against the idea of an inherent legal logic that can explain the crystallization of rules of international cyber law. This rejection, however, does not amount to a denial of the existence of rules. It merely suggests that these rules do not emanate from a self-contained legal logic. Rules exist *despite* the structural indeterminacy of international law. When positivist scholars focus on how international law applies in cyberspace, they thus fundamentally overlook the social nature of their object of interrogation. The more fundamental question we should ask is: *Why* do certain ideas get accepted as international rules governing in cyberspace?

In this chapter, I argue that it is possible to interrogate this question through a Marxist lens. The chapter has two primary aims. The *first* aim is to expand on my previous critique of positivist scholarship of the field of international cyber law. While chapter one offered an elucidation of the field's methodological limitations, this chapter argues that the field, by approaching international cyber law without considering how the emerging rules reflect and reinforce particular social relations, may inadvertently give legitimacy to ideas that work to sustain relations of domination. The *second* aim of the chapter is to outline the foundations of a Marxist approach to international cyber law. The chapter ultimately summarizes its key conclusions into a set of propositions to guide the study of international cyber law to follow.

Marxism and Law

Marxist legal theory is by no means reducible to one uniform, coherent approach. It rather serves as an umbrella-term for a range of different traditions and perspectives. Despite this diversity, a few general characteristics remain central. A fundamental principle of Marxist social theory in general is that every social form is regarded as historical, and that history is to be understood in material terms.[1] The same is true for Marxist approaches to law specifically. The abstract legal categories through which social orders are reflected – concepts such as law, legal subject, rule, and right – are approached as historically specific categories. However natural and obvious they may seem to us; they are not found in all societies at all times. Rather, they are specific to societies based on the capitalist mode of production.[2] The task for Marxist studies of law is therefore to elucidate 'those historically given material conditions which brought this or that category into being.'[3] The insistence on the historicity of all social forms implies a rejection of the current social order as transhistorical, natural, or determinate. A materialist lens therefore suggests to not just take these forms as given, but to approach them as a reflection of historically specific social relations.

This also means that the ideas and assumptions of positivist legal theory must not be disregarded in an endeavor to interrogate law through a Marxist lens. Just like Marx adopted the categories of bourgeois political economy because they expressed a historical reality in capitalist society, a Marxist analysis of law must operate with the categories of the positivist legal tradition.[4] The critical task, then, is to elaborate on their meaning and significance in a way that exposes their historical and material foundations.

A Marxist lens gives analytical priority to the social relations through which the reproduction of the life of society is organized rather than to legal ideas, seeing the latter as an expression of the former rather than *vice versa*. As a Marxist approach thus rejects the determinacy of *law* central to positivism, it may seem paradoxical that 'determination' is an equally central

---

[1] Marks, 'Introduction', 2.

[2] Simon Clarke, 'Introduction', in *The State Debate*, ed. Simon Clarke (London: Palgrave Macmillan, 1991), 10.

[3] Pashukanis, *Law and Marxism*, 111.

[4] Ellen Meiksins Wood, *Democracy Against Capitalism: Renewing Historical Materialism* (Cambridge: Cambridge University Press, 1995), 23.

concept in Marxist approaches to law.[5] Susan Marks clarifies this apparent contradiction by distinguishing the Marxist understanding of determination from the positivist understanding of determinacy. As she explains:

> [W]hat crucially distinguishes [the Marxist] understanding [of determination] from an understanding of determination as the operation of predictable laws is that [in historical materialism], the limits and pressures - the conditions set by the material base - are not seen as "external" to human will and action, such that our only option is to accommodate to them and "guide [our] actions accordingly". Rather, they are seen as historical inheritances that are the "result of human action in the material world" and hence "accessible" and revisable.[6]

The rejection of the determinacy of *law* does not equate to a rejection of the existence of predictable cases. The rejection rather reflects an understanding that predictability arises not from legal doctrine but from historically specific social relations. Through a Marxist lens, the power of law is not a regulatory power. Instead, its power lies in law's *appearance* as a regulatory power external to the social relations to which it applies and their specific disputes.

Besides from these general characteristics, multiple different streams of legal scholarship exist within the persistently plural category of historical materialism.[7] The remainder of this chapter draws on what I find to be the most influential and compelling contributions in an effort to build a Marxist framework through which we can study the emerging field of international cyber law. This framework, I will argue, allows us to move beyond the circularity of legal doctrine and explain the (re)production of ideas as international law regulating information technologies.

Between Equal Rights

One of the most influential Marxist legal theorists to date is Soviet legal scholar Evgeniĭ Pashukanis, who has been subject to renewed interest in recent years. In *A General Theory of Law and Marxism*, Pashukanis aims to build a general theory of the legal form. By the legal form, he means 'the most fundamental and abstract juridical concepts, such as "legal norm", "legal relation", "legal subject" and so on' – that is, abstract concepts that are

[5] Marks, 'Introduction', 3.

[6] Marks, 3.

[7] Marks, 1.

applicable to each and every branch of law, and whose logical and systematic meaning remains constant regardless of the concrete context to which they are applied.[8] This endeavor was an objection to namely two traditions of legal theory: Formalism and instrumentalism.[9] The formalist theory of law supposedly 'explains nothing, and turns its back from the outset on the facts of reality, that is of social life, busying itself with norms without being in the least interested in their origin (a meta-juridical question!), or in their relationship to any material matters.'[10] The formalist theory thus avoids altogether to analyze law as a historical form, instead pretending that the legal form is transhistorical and natural. Pashukanis sees in the instrumentalist approaches (the 'psychological and sociological theories of law') only little more hope; while he commends them for undertaking to interpret law as a real phenomenon in its origin and development, they 'operate from the outset with concepts of a non-juridical nature' and thus 'overlook the problem involved in it'.[11] The instrumentalist approaches are thus equally guilty of overlooking the legal form as such. Carl Wilén aptly summarizes the Pashukanian critique of the two approaches to law:

> [F]ormalism and instrumentalism are equally incapable of addressing the legal form due to their conceptual presuppositions. Either the legal form is avoided from the very beginning when only content is directly addressed (instrumentalism), or it is erased when rights and law are theorized without considering their historically specific content (formalism).[12]

It is in an effort to supersede both the formalist and the instrumentalist theories of law that Pashukanis undertakes to build a *general theory of the legal form*. Despite his interest in form, we should not mistake his work for that of the formalists to whom it is a reaction. Pashukanis's engagement with law is rooted in a conviction that legal form is not universal but emerged under certain historically specific material conditions. A theory of law should therefore investigate these conditions to comprehend the specific nature of

---

[8] Pashukanis, *Law and Marxism*, 47.

[9] Carl Wilén, 'Why Pashukanis Was Right: Abstraction and Form in The General Theory of Law and Marxism', *Capital & Class*, 2023, 3.

[10] Pashukanis, *Law and Marxism*, 52–53.

[11] Pashukanis, 53.

[12] Carl Wilén, 'Formalism and Instrumentalism in the Marxist Critique of Right: With What Must Pashukanian Theory Begin?', *Rethinking Marxism*, Forthcoming.

this form.[13] The legal form is 'derived from *actually-existing law*, rather than from some abstract notion of law'.[14] In contrast to what the formalists often claim, the legal form cannot be understood as some natural form existing in any society at any time.

In his inquiry into the historically specific material conditions out of which the legal form has emerged, Pashukanis simulates the approach of Marx's critique of the political economy in *Capital* by taking his starting point in the commodity. As we saw in the introduction, a commodity is a thing being produced or acquired with a view to being exchanged. The act of exchange requires the existence of individuals with products at their disposal, who can bring the products to the market to exchange them. Following Marx:

> [The] guardians [of the commodities] must … recognize each other as owners of private property. This juridical relation, whose form is the contract, whether as part of a developed legal system or not, is a relation between two wills which mirrors the economic relation.[15]

Each individual commodity-owner must, in an abstract, formal sense, recognize the other commodity-owner as an equal owner of private property.[16] Without this mutual recognition, what occurred would not be commodity exchange. The legal form is the *necessary form* taken by the relation between these formally equal commodity-owners.[17] The legal form thus presupposes the mutual respect for property rights and the formal equality of the individuals (who, in the legal form, emerge as 'legal subjects').[18] Once the product of labor becomes a commodity and a bearer of value, the individual 'acquires the capacity to be a legal subject and a bearer of rights'.[19] The

---

[13] Robert Knox, 'A Critical Examination of the Concept of Imperialism in Marxist and Third World Approaches to International Law' (phd, London School of Economics and Political Science, 2014), 179.

[14] Miéville, *Between Equal Rights: A Marxist Theory of International Law*, 79.

[15] Marx, *Capital: A Critique of Political Economy. Volume One*, 178.

[16] Marx, 178; Knox, 'A Critical Examination of the Concept of Imperialism in Marxist and Third World Approaches to International Law', 180.

[17] Miéville, *Between Equal Rights: A Marxist Theory of International Law*, 78.

[18] Pashukanis, *Law and Marxism*, 112; Marx, *Capital: A Critique of Political Economy. Volume One*, 178.

[19] Pashukanis, *Law and Marxism*, 112.

legal form thus has a categorical symmetry with the form of the social relation between commodity-owners under capitalism.

The abstract impersonal legal subject presupposes generalized commodity exchange.[20] In turn, generalized commodity exchange presupposes capitalist class relations.[21] Quoting Marx, '[o]nly when and where wage labour is its basis does commodity production impose itself upon society as a whole'.[22] While class subjugation is thus the presupposition of generalized commodity exchange, the abstract impersonal legal subject emerging with generalized commodity exchange shields the class relations on which it relies. As Marx puts it:

> Two people who face each other on the marketplace, in the sphere of circulation, are not just a *buyer* and a *seller,* but *capitalist* and *worker* who confront each other as *buyer* and *seller.* Their relationship as *capitalist* and *worker* is the presupposition of their relationship as *buyer and seller.*[23]

Under these conditions of generalized commodity exchange, all individuals become commodity owners, because even workers own their labor power.[24] The commodity owners engaged in exchange are *free* and *equal* – the commodity-form makes no distinction between the capitalist and the worker. Following Wilén:

> [S]ale and purchase of labor power goes on without damaging the standards of freedom (the exchange and contract are determined by free will), equality (one is exchanged for one), property (each disposes of what is her own), and mutual benefit (self-interest benefits all).[25]

---

[20] Pashukanis, 115.

[21] Søren Mau, 'The Transition to Capital in Marx's Critique of Political Economy', *Historical Materialism* 26, no. 1 (2018): 68–102.

[22] Marx, *Capital: A Critique of Political Economy. Volume One*, 733.

[23] Karl Marx, 'Results of the Immediate Process of Production', in *Capital. Volume One: A Critique of Political Economy*, by Karl Marx, Penguin Classics (London: Penguin in association with New Left Review, 1990), 1015.

[24] Knox, 'A Critical Examination of the Concept of Imperialism in Marxist and Third World Approaches to International Law', 180.

[25] Wilén, 'Formalism and Instrumentalism in the Marxist Critique of Right: With What Must Pashukanian Theory Begin?'

The commodity-form thus denotes an abstract equality of legal subjects with commodities in their possession. The form of the relationship between equal commodity-owners – the contract – is the archetype of the legal form.

It follows from this that a fundamental component to the legal form is the conflict between private interests.[26] At its core, the legal form is structured around owners of private property, and any other area of law is derived from this form. As Miéville explains, a 'complex legal system regulating all levels of social life can be thrown up which appears to differentiate itself from private law, but it ultimately derives from *the clash of private interests'*.[27] Private law is therefore the fundamental, primary level of law from which other fields of law are deduced. This means that the central starting point for any legal relation is the opposition of formally equal subjects.

Contestation is implied in every legal relation, even if exchange is peaceful.[28] Because of the latent conflict prevalent in every legal relation, coercion is at the heart of the legal form. As Miéville puts it: if 'there were nothing to defend its "mine-ness", there would be nothing to stop it becoming "yours" and then it would no longer be a commodity, as I would not be exchanging it.'[29] Coercion is often invisible, because it is implicit, and because the actualization of the latent threat of violence is rarely necessary. However, the implicit nature of the coercion implied in the commodity form does not make it any less violent. With its abstract equality, the legal form formalizes the method of dispute settlement between sovereign, formally equal individuals implied by commodity exchange.[30] In domestic legal systems, the state plays an important role in exercising the coercion implied in the legal form, and thus in upholding the social relations of capitalism. As a superordinate authority, the state ultimately guarantees the enforcement of property relations necessary for commodity-exchange – and by extension, capitalism – to sustain and thrive.

Since the legal form is the form of a particular kind of relationship, rules are contingent on, and thus secondary to, this relationship. The *relationship*, rather than the rule, is therefore the cell-form of the legal fabric; 'only there does law accomplish its real movement'.[31] It follows from this that a study

---

[26] Pashukanis, *Law and Marxism*, 81.

[27] Miéville, *Between Equal Rights: A Marxist Theory of International Law*, 86.

[28] Miéville, 79.

[29] Miéville, 126.

[30] Miéville, 79.

[31] Pashukanis, *Law and Marxism*, 85.

of the legal form must investigate the form of this relationship. Likewise, a study of the *content* of law – of the specific rules emerging within this relationship – must investigate the specific dynamics of the relationship on which the rule is contingent. Even if rules are made to appear as if they have a regulatory force that can be analyzed as an autonomous phenomenon, they remain contingent on the specific relationship that they concern, rather than *vice versa*. Essentially, rules do therefore not primarily *regulate* material relations; they rather *express* them. As this expression of material relations *appears* as a regulatory force, law serves to not only mirror but also support the reproduction of the social relations of capitalism – a point that I will get back to shortly. Pashukanis's insistence to study the legal form in isolation from its content does not make his theory in any way detrimental to examinations of the *content* of law.[32] But this content should be understood as specific expressions of the relationship that it concerns.

The concept of equality between abstract legal subjects stands in sharp contrast to the experienced material reality of humans in concrete relations. Here, different forms of factual subordination (capitalist/proletariat, man/woman, white/black appear highly real, although perhaps mostly so to those persons finding themselves at the unprivileged side of the dichotomies. The assumption of an abstract individuality makes the relations between persons with such very different experiences 'miraculously to appear like equality (citizen/citizen)'.[33] To make sense of the exploitative vertical relations between capitalist and workers that the free exchange of commodities within the sphere of circulation presupposes, we must move beyond the abstract equality and analyze the real dynamics arising from peoples' different access to the means of production. Meanwhile, the legal relationship, characterized by the free and equal exchange borne by abstract, isolated social agents, shields over these underlying inequalities.[34]

The formal, abstract equality of individuals resembles one of the key structuring elements of international law: That of *sovereignty*.[35] For Pashukanis, a parallel can – at least to some extent – be drawn between the

[32] Miéville, *Between Equal Rights: A Marxist Theory of International Law*, 118.

[33] Martti Koskenniemi, 'What Should Lawyers Learn from Marx?', in *International Law on the Left: Re-Examining Marxist Legacies*, ed. Susan Marks (Cambridge: Cambridge University Press, 2008), 37.

[34] Miéville, *Between Equal Rights: A Marxist Theory of International Law*, 92.

[35] Knox, 'A Critical Examination of the Concept of Imperialism in Marxist and Third World Approaches to International Law', 181.

relationship between individual commodity owners and the relationship between sovereign, formally equal states. As we saw above, the liberal assumption of an abstract individuality – the absence of a pre-existing hierarchy – is fundamental to the commodity form, and thus to the legal form. Just like domestic private law suggests that individuals are formally equal while allowing real inequality when it comes to property ownership, international law claims that states have equal rights, while in practice they vary greatly in power and influence.[36] States' abstract subjectivity thus give them a formal equality in their interactions.

The most comprehensive attempt at elaborating on the commodity form theory in the context of international law is China Miéville's *Between Equal Rights.* Combining Koskenniemi's structuralist account of the indeterminacy of international law with Pashukanis's insight that coercion is implied in the legal form, Miéville contends that the means of violence of the stronger coercive force remains in the hands of the very parties disagreeing over the interpretation of international law: states. Because of their stronger coercive force, strong states are able to enforce their own interpretations of law.[37]

In contrast to domestic legal systems, in which states play an important role as an authority that can ultimately exercise the coercion needed to enforce extant property relations, international law contains no enforcement mechanism from without the legal relationship. This feature makes international law all the more illustrative of the implicit coercion in this relationship. In the words of Miéville, the 'very existence of international law as law is evidence that it is in the relationship between legal subjects rather than in any "posited norm" that the essence of the legal form lies.'[38] As there is no force external to the legal subjects to enforce the rights of one when it conflicts with the rights of another, conflict must find its resolution in the relationship itself. Here, states' formal equality signified by the legal form shields over their material inequality.[39] For example, every state is technically free to respond to violations of its rights as it sees fit. But a powerful state is able to respond with threats or force, while a less powerful state can merely offer 'passive resistance or is compelled to concede'.[40] Thereby, 'the *particular*

---

[36] Evgeniĭ Bronislavovich Pashukanis, *Pashukanis, Selected Writings on Marxism and Law*, ed. Piers Beirne and Robert S. Sharlet (Academic Press, 1980), 193.

[37] Miéville, *Between Equal Rights: A Marxist Theory of International Law*, 292.

[38] Miéville, 85.

[39] Pashukanis, *Pashukanis, Selected Writings on Marxism and Law*, 193.

[40] Pashukanis, 193.

contents and norms that actualize the *general* content of competitive social relations are invested into the legal form.'[41]

In the absence of a superordinate force mandated to authoritatively interpret legal material and enforce its resolution in the dispute between two states, the parties themselves – formally equal and sovereign – must perform the act of interpretation and enforcement. For a particular interpretation to be authoritative – for it to defeat its rivals – it must be supported by the stronger coercive power within a given relationship. The direction of international law is therefore ultimately determined by the actors with a power to back their interpretation by force. Borrowing from Miéville, international law is 'simultaneously a *genuine relation between equals*, and a form that the weaker states *cannot hope to win.* That, rather than any simple collapse into power politics, is the meaning of Marx's words that "[b]etween equal rights, force decides."'[42] As we dive deeper into the Pashukanian account of the inter-state rivalries to which international law gives expression, some of the limitations to the commodity form framework begin to appear. But before we get to that, I will show in the following section how the Pashukanian framework allows us to expand on the critique of positivist scholarship on international cyber law.

International Law as Ideology

Pashukanis's loyalty to Marx's approach in chapter one of *Capital* makes his framework powerful in particularly one important respect: It demonstrates how the (re)production of international law is an ideological process, similar to the fetishism of commodities underlying the capitalist economic system. Herein lies two claims that I will substantiate shortly. But first, let me dive briefly into Marx's argument about the fetishism of commodities. To appreciate Marx's argument, we must be attentive to the meaning of the term fetishism in Marx's time of writing, which is quite different from the meaning the term has today. In 18th and 19th century anthropological research, fetishism referred to the attribution of supernatural characteristics to objects and was especially used to describe cultural practices of 'primitive and irrational' non-Western people, which bourgeois society imagined itself as superior to.[43] A German lexicon from 1840 states:

---

[41] Miéville, *Between Equal Rights: A Marxist Theory of International Law*, 141.

[42] Miéville, 142.

[43] Michael Heinrich, *How to Read Marx's Capital: Commentary and Explanations on the Beginning Chapters* (New York City: NYU Press, 2021), 143.

> Fetishism is the divine worship of (usually lifeless) objects, powers, or natural phenomena. In fetishism, which is the lowest level of religious thought, the cult object is the sensuous object itself (not its hidden source), insofar as it expresses its power to people's best disadvantage or advantage. The characteristic of this form of religion is arbitrary choice and arbitrary rejection or variation.[44]

Typical examples of practices that were described as fetishism at the time include totem poles and voodoo practices through which lifeless objects were given a supernatural meaning. By employing the concept of fetishism to describe the way human beings relate to commodities in capitalism, Marx undermines the euro-centric and racist ideology inherent in the concept by demonstrating how it actually describes very well what takes place in the supposedly enlightened Western civilization:

> [The commodity] is nothing but the definite social relation between men themselves which assumes here, for them, the fantastic form of a relation between things. In order, therefore, to find an analogy we must take flight into the misty realm of religion. There the products of the human brain appear as autonomous figures endowed with a life of their own, which enter into relations both with each other and with the human race. So it is in the world of commodities with the products of men's hands. I call this the fetishism which attaches itself to the products of labour as soon as they are produced as commodities, and is therefore inseparable from the production of commodities.[45]

The commodity form entails that the social characteristics of labor are concealed as natural characteristics of things: The money form 'conceals the social character of private labour and the social relations between workers, by making those relations appear as relations between material objects, instead of revealing them plainly.'[46] The fetishism of commodities therefore lies in the appearance of their (exchange) value as natural – that is, non-social – qualities, even though this feature is in fact an expression of historically specific social relations among human beings.

---

[44] *Allgemeines deutsches Conversations-Lexicon für die Gebildeten eines jeden Standes in 10 Bänden,* vol. 4:F-G, Leipzig 1840, 79, quoted in Heinrich, 143.

[45] Marx, *Capital: A Critique of Political Economy. Volume One*, 165.

[46] Marx, 168–69.

Returning to international law, it is now possible to substantiate the first claim made above, *i.e.* that the (re)production of international law is analogous to the fetishism of commodities described by Marx. I showed in chapter one that existing scholarship on international cyber law assume the autonomous existence of rules of international law, and thus, that rules have a regulatory effect. Such a view is premised on the ability to distinguish between is and ought – between legislator, rule, and legal subject. However, within a positivist framework, it is conceptually impossible to distinguish between these formal categories. The legislator is also the legal subject, and the rule cannot be distinguished from its creation or its violation in a systematic manner within a positivist legal framework, which contains no relevant criteria for understanding the selective mechanism that turns some practice into law and some practice into violations thereof. In other words, positivist scholarship is incapable of explaining why certain ideas and practices, rather than alternative ones, come to be accepted as *rules*. In this chapter, we have seen how rules are entirely contingent on the social relationship that they concern. We can therefore paraphrase Marx's description of the commodity and say about rules of international law that while the rule *appears* at first sight as an extremely obvious, trivial thing, our analysis brings out that it is *a very strange thing.*[47] Rules of international law have no existence that can be understood autonomously from the social relations between states. The latter *appear* as natural (*i.e.* non-social) rules of international law, while in fact, rules are the sum of these relations. In other words, rules of international law are reifications of the social relations between states.

The abstractions of law are no less artificial than the abstractions of the political economy. Just like no chemist has ever discovered the exchange-value in an object, none of law's abstractions – legal subject, rule, right, property – are identifiable by the research methods of natural science.[48] Yet, behind these abstractions lie perfectly real social forces.[49] Rather than reflecting an internal, self-contained legal logic, legal norms reflect social forces. When international legal scholars nevertheless treat rules as if they had an autonomous existence, they inevitably come to fetishize international law, *i.e.* treat rules as if they had a natural existence with a regulatory power. This maneuver simulates the fetishism of commodities described by Marx.

---

[47] Marx, 163.

[48] Marx, 177.

[49] Pashukanis, *Law and Marxism*, 59.

Let me now turn to substantiate the second claim made above: that the fetishism of international law is an *ideological process*.[50] As mentioned in the introduction, I use the term *ideology* to refer to the ways in which ideas sustain relations of domination.[51] There is some disagreement in the literature whether the fetishism of commodities describes an *ideological naturalization* or a *real phenomenon*. While the former reading has traditionally been dominant, scholars have in recent years increasingly argued for the latter reading. Proponents of this position analyze the concept of fetishism as a reference to the real inversion that happens when relations between humans are mediated through relations between things.[52] For example, Werner Bonefeld writes:

> The fetishism of commodities does not disguise the "real" social relations of capitalism. Rather, the fetishism of commodities expresses the "real" social relations in the form of capital as the automatic subject of bourgeois society.[53]

While it is certainly true that capitalism relies on a practical inversion in which human beings relate to each other by means of things (i.e. an inversion that takes place on the level of social practice, and not ideology), I also think that such an interpretation fails to see how the fetishization lies exactly in the ideological expression of real social relations in a reified form, which makes these social relations *appear* as something else than what they really are – that is, as natural characteristics of things. As Søren Mau explains:

> For the religious mind, what is *in reality* a product of the human brain *appears* as autonomous figures with a life of their own – which they are *not.* Similarly with commodities: what is *in reality* a set of social relations among human beings *appear* to be relations exclusively among commodities.'[54]

---

[50] Thompson, *Ideology and Modern Culture*, 56; Marks, *The Riddle of All Constitutions*, 10–11.

[51] Eagleton, *Ideology*; Rehmann, *Theories of Ideology*; Althusser, *On The Reproduction Of Capitalism*.

[52] Heinrich, *How to Read Marx's Capital*, 143f.; Werner Bonefeld, *Critical Theory and the Critique of Political Economy: On Subversion and Negative Reason* (London & New York: Bloomsbury, 2014), 54.

[53] Bonefeld, *Critical Theory and the Critique of Political Economy*, 54.

[54] Mau, *Mute Compulsion*, 190–91.

The point of Marx's turn to the 'misty realm of religion' is exactly to underscore how the social relations of capitalism *appear* as something distinct from these relations. The fetishism of commodities thus lies in the *appearance* of value as a natural quality of the commodity. The social relations of capitalism thereby become reified – the social relations between humans appears as relations between things. If we understand ideology as the ways in which ideas serve to sustain relations of domination, then the social relations of capital's *appearance* as natural qualities of things is an ideological operation: It makes these relations seem natural and uncontestable. I therefore adhere to the former reading of fetishism, according to which the concept refers to an *ideological naturalization* of social forms.[55] At the same time, however, it is important to see how this *ideological* inversion is intimately connected the *practical* inversions between humans and commodities which lies at the heart of capitalist society.

I will argue that the fetishism of international law is ideological in the same way: International law *appears* as if it had an autonomous existence distinct from the social relations that it concerns. The ideological character lies exactly in international law's ability to mask relations between states as rules, which come to appear natural and uncontestable.

The ideological nature of the fetishism of international law becomes evident when compared to law in medieval Europe, where there was an overt absence of distinction between law and legislator. The rule was inseparable from its application. As a result, the spheres of activity of judge and legislator were unapologetically indistinguishable.[56] With legal positivism, in contrast, there *appears* to be a distinction between the creation of law, on the one hand, and its concrete application, on the other hand. This distinction – often praised as the 'rule of law' – serves a specific function in legal argumentation: It signifies that 'whoever makes a legal argument will have to base their claims on the primary sources of law – or at least make it seem as if they do'.[57] This change makes law appear as a category distinct from partial interests and social forces. Positivist international legal scholars contribute to the reproduction of this fantasy: By erroneously assuming that it is capable of deductive reasoning, they reproduce and give legitimacy to particular ideas as natural and autonomous forces, reifying the dynamics of social relations as 'rules'. The theoretical foundations underlying this maneuver

[55] Mau, 188.

[56] Pashukanis, *Law and Marxism*, 58–59.

[57] Boer, *International Law As We Know It*, 6.

remain mostly unexamined by the positivists, leaving much to wish for in terms of a coherent self-scrutiny of legal doctrine as a valid form of knowledge construction. Quoting Miéville, their work is 'the more ideological for that'.[58]

We can thus expand on the critique of positivist scholarship on international cyber law. I argued in chapter one that this body of scholarship was methodologically inadequate because it contained no coherent way of distinguishing between the creation and violation of international law. Our Marxist lens now allows us to see that the positivist scholars' reproduction of certain ideas as the content of international cyber law amounts to a reification of the dynamics of extant social relations. This scholarship is therefore not only methodologically insufficient; is also an ideological operation.

The Content of International Law

In the preceding chapter, we were left with the question: when several possible interpretations of a legal norm exist, how can we understand why one of them ultimately defeats its rivals? The contours of a Pashukanian answer to this question has now emerged: The interpretation of the more powerful coercive force in the underlying social relationship will ultimately defeat its rivals and come to stand as authoritative. The 'content' of law, which appears to us as an interpretation that ultimately gets accepted as a rule, is therefore an expression of the dynamics of this social relationship. As we dive into the Pashukanian account of these dynamics, some of the limitations to the commodity-form theory emerge.

To Pashukanis, the social relationship that international law expresses is the social relation between capitalist states, understood as a relationship of economic and geopolitical competition in line with orthodox Marxist theories of imperialism. Bukharin and Lenin both understood the concept of imperialism as the rivalry between major capitalist states expressed in conflict over territory, leading ultimately to inter-imperialist war.[59] To them, the focus was on the struggle for dominance playing out between capitalist states. Meanwhile, the colonies figured primarily as passive battlegrounds, not as

---

[58] China Miéville, 'The Commodity-Form Theory of International Law', in *International Law on the Left: Re-Examining Marxist Legacies*, ed. Susan Marks (Cambridge: Cambridge University Press, 2008), 92.

[59] Anthony Brewer, *Marxist Theories of Imperialism: A Critical Survey* (London: Routledge, 1990), 88.

active participants.[60] This understanding is based on an immediate identification of the state with the interests of capital, that is, a general assumption that capitalist states represent the interests of their elites.[61]

Relying on this understanding, Pashukanis sees international law as an expression of the social relation between capitalist imperial rivalries, while the remainder of the world is simply the objects of their transactions.[62] He quotes Lenin to assert that capitalists divide the world 'because the degree of concentration which has been reached forces them to adopt this method in order to receive profit.'[63] The world is thus divided between capitalist states in proportion to strength – be economic or military.[64] Agreements between states are a 'means for jealously protecting their particular interests, preventing the expansion of their rivals' influence, thwarting unilateral conquest, i.e. in another form continuing the same struggle which will exist for as long as capitalist competition exists.'[65] To Pashukanis, international law 'owes its existence to the fact that the bourgeoisie exercises its domination over the proletariat and over the colonial countries.'[66] Imperialist states act through international law, using it to articulate their own interests, and international law thus serves to 'concretize' economic and political relationships.[67]

Viewing imperialism and the state-system through this lens entails that the 'content' of international law is a reflection of the dynamics of the relationship between capitalist states. Following the analogy between individual commodity owners and sovereign states, the relationship between capitalist states simulates the relationship between individuals engaged in commodity exchange in domestic law with only a 'degree in difference' between

---

[60] Brewer, 88–89.

[61] Pashukanis, *Pashukanis, Selected Writings on Marxism and Law*, 174; Clarke, 'Introduction', 3; Miéville, *Between Equal Rights: A Marxist Theory of International Law*, 138.

[62] Pashukanis, *Pashukanis, Selected Writings on Marxism and Law*, 169; Miéville, *Between Equal Rights: A Marxist Theory of International Law*, 138.

[63] Pashukanis, *Pashukanis, Selected Writings on Marxism and Law*, 170., in which Pashukanis quotes Vladimir Lenin's *Imperialism, the Highest Stage of Capitalism* (1917)

[64] Pashukanis, 170.

[65] Pashukanis, 170.

[66] Pashukanis, 173.

[67] Knox, 'A Critical Examination of the Concept of Imperialism in Marxist and Third World Approaches to International Law', 182.

domestic law and international law.[68] International law is understood as a function of the interests of the 'commanding and ruling classes of different states which have identical class structures' – in plain words, the capitalist classes of capitalist states.[69] The central struggle is based on the economic division of the world. This division will be brought about politically by the capitalist state, which relies in turn on the capitalist economic system.[70]

The Pashukanian framework contains an important limitation that impedes us from moving much beyond these crude contours of a theory of the content of international law: It is incapable of explaining the role of the state-system in contemporary capitalism. This limitation is a result of two distinct problems: *First*, the historical specificity of the Leninist theory of imperialism on which Pashukanis relies, and *second,* the reliance on an analogy between states and individual commodity-owners. In the following two sections, I unfold these two problems with a view to offering a corrective that makes us better suited for a study of the content of the nascent field of international cyber law.

Leninist Imperialism in the Current Millennium

At Lenin's and Pashukanis's time of writing in the first quarter of the 20th century, the world was not fully, or even predominantly, capitalist.[71] Colonies were not treated as equal subjects in international law, but rather as objects.[72] The relationship between capitalist states and the Third World was still marked by the formal control over colonized states. Curiously, this historical specificity has not stopped Miéville from relying quite loyally on a Leninist view on imperialism in his construction of a contemporary commodity form theory of international law.[73] To Miéville, the subsequent changes brought about by the widespread formal decolonization processes of the 20th century entail, above all, a completion of the analogy between the abstract equality of commodity-owners and the abstract equality of states. With formal decolonization, material inequalities between states in the Global North and the Global South are now shielded almost completely

---

[68] Chimni, *International Law and World Order*, 470; Pashukanis, *Pashukanis, Selected Writings on Marxism and Law*, 180.

[69] Pashukanis, *Pashukanis, Selected Writings on Marxism and Law*, 171.

[70] Miéville, *Between Equal Rights: A Marxist Theory of International Law*, 139.

[71] Wood, *Empire of Capital*.

[72] Chimni, *International Law and World Order*, 472.

[73] Miéville, *Between Equal Rights: A Marxist Theory of International Law*, 292–93.

by the juridical principle of abstract equality between sovereign states.[74] Just like bourgeois economy transforms everyone into formally equal commodity-owners regardless of their access to property, the universalization of the doctrine of sovereignty transforms states into formally equal subjects regardless of the continuation of the same material inequalities that characterized the colonial era.

Miéville has sometimes been criticized for thereby failing to appreciate that in historical terms, the universalization of the principle of sovereign equality represents important progress, neocolonial international law being less oppressive than colonial international law in crucial ways.[75] While it is doubtlessly correct that formal decolonization represented progress in significant ways, this point does not harm the merits of Miéville's important point that the international legal form shields and legitimizes the material differences still prevailing between the Global South and the Global North. Following Miriam Bak McKenna, '[f]ormal post-colonial sovereignty did not necessarily translate to freedom and independence in an international system that was still broadly structured around imperial hierarchies.'[76]

It is thus entirely coherent to hold, at the same time, that the forms of exploitation characterizing formal colonialism were in crucial respects more devastating than current forms, *and* that formal sovereign equality, nonetheless, gives way for new and more subtle forms of exploitation.[77] To understand the difference, we might compare traditional imperialism with certain pre-capitalist domestic class relations: just like in the relationship between feudal lords and peasants, the relationship between colonial masters and their colonial subjects was reasonably clear. In contrast, the class relation between capital and labor is much more difficult to decipher because of the mystifications of the wage form, and because the compulsion by which workers are forced to sell their labor power is not primarily the threat of violence, but the economic power of capital. If we take seriously the analogy between states and individuals – which Miéville does arguably even more than Pashukanis – the subtle nature of the compulsion that drives workers to sell their labor power parallels international relations in the aftermath of

[74] Miéville, 268.

[75] Chimni, *International Law and World Order*, 476.

[76] Miriam Bak McKenna, *Reckoning with Empire: Self-Determination in International Law* (Leiden: Brill, 2023), 109.

[77] Susan Marks, 'Empire's Law', *Indiana Journal of Global Legal Studies* 10, no. 1 (2003): 451; McKenna, *Reckoning with Empire*, 109.

formal decolonization. An empirical objection that the colonial violence may have been more brutal than contemporary forms of imperialism does not hamper the validity of this argument. The problem with Miéville's reliance on a Leninist theory of imperialism therefore does not follow from its neglect of the progressive nature of decolonization.

The problem follows instead from the failure to consider how the global expansion of capitalism might have altered the nature of inter-state rivalries and conflicts. The Leninist theory of imperialism relies on an orthodox theory of state-monopoly capitalism, which identifies the state *a priori* with 'its' capitalist class. However, in the 21st century, the whole world has been fused into one big economic system, and capitalists operate across geographical borders. Miéville fails to consider how the increasingly transnational existence of classes may change the role of states *vis a vis* capitalists. This is curious, because Miéville wrote *Between Equal Rights* in the beginning of the current millennium, in which a heated debate unfolded on the nature of imperialism in an era of global capitalism. In the much-debated *Empire,* Michael Hardt and Antonio Negri argued that as the economy is developing towards an ever-increasing level of globalization, the sovereignty of states is progressively declining. As the ease of movement across national borders for primary factors of production and distribution, such as money, technology, people, and goods, had been increasing, the power of states to regulate these flows and impose their authority over the economy was argued to be diminishing:

> The primary factors of production and exchange - money, technology, people, and goods - move with increasing ease across national boundaries; hence the nation-state has less and less power to regulate these flows and impose its authority over the economy.[78]

Since the capitalist world had effectively fused into a single socio-economic unit ruled by a self-conscious global bourgeoisie, they argued that individual states have lost their importance.[79] They pointed to a process of 'deterritorialization' with respect to earlier systems of domination and exploitation,

---

[78] Michael Hardt and Antonio Negri, *Empire* (Cambridge, MA: Harvard University Press, 2001), xi.

[79] Hardt and Negri, *Empire*; Bob Sutcliffe, 'Imperialism Old and New: A Comment on David Harvey's The New Imperialism and Ellen Meiksins Wood's Empire of Capital', *Historical Materialism* 14, no. 4 (2006): 61.

entailing that hierarchies are now constituted and sustained by much more complex patterns and logics.

These radical claims gave rise to a wealth of scholarly disputes on the nature of imperialism in the 21st century. Building on Hardt and Negri's ideas, scholars like William I Robinson, Jerry Harris, Nick Dyer-Witheford and, within the context of international law, B.S. Chimni (even if only to a certain extent), have pointed to an entirely globalized economy in which the divide between first-world and third-world economic interests are vanishing to be replaced by a global class dichotomy: The transnational capitalist class and the transnational proletariat class.[80] Globalization has led to the merger of capital to the point where national ownership is of little relevance. Once nation-centric economies have given way to the transnationalization of production and cross-border flows of money.[81] In a similar vein, Douglas Kellner has described a development towards a new postindustrial form of 'technocapitalism', which implies the growing power of globalized transnational corporations and global governmental and corporate bodies and the declining significance of states and their institutions.[82]

The implications for international law of an acceptance of Hardt and Negri's diagnosis of the current world order would be profound.[83] Not only are global economic structures organized less along territorial lines, visibly challenging the idea underlying a Leninist conceptualization of imperialism in which states represent 'their' capitalist classes. States are allegedly also losing importance in facilitating, restricting, or regulating these structures. By claiming that sovereignty has ceased to be an attribute purely of state-based polities and has become also an attribute of global order, Hardt and Negri break with the primary organizing principle underlying international law. As such, a tempting conclusion to draw from Hardt and Negri's diagnosis would be that international law has become entirely redundant.

---

[80] Dyer-Witheford, *Cyber-Proletariat*; William I. Robinson, *Can Global Capitalism Endure?* (Los Angeles: SCB Distributors, 2022).

[81] Jerry Harris, 'Globalization, Technology and the Transnational Capitalist Class', *Foresight* 17, no. 2 (2015): 194–207.

[82] Douglas Kellner, *Technology and Democracy: Toward A Critical Theory of Digital Technologies, Technopolitics, and Technocapitalism*, Medienkulturen Im Digitalen Zeitalter (Wiesbaden: Springer Fachmedien Wiesbaden, 2021), 25.

[83] Marks, 'Empire's Law'.

The central theses of *Empire* have been compellingly disproven by a wealth of imperialism scholars in the beginning of the current century.[84] We will soon in this chapter return to some of the insights from this stream of scholarship to define the role of the state-system in contemporary global capitalism. But for now, I merely want to point out the inadequacy of the commodity form framework following from its reliance on a Leninist view of imperialism, which – even without accepting the radical post-imperialist claims of Hardt and Negi – has irrefutably evolved within the last century. By overlooking how the global dynamics of capitalism are profoundly different in the 21st century than they were in the beginning of the 20th century, Miéville misses an opportunity to explicate compellingly the dynamics of the state-system that are reflected in international law.

The State-Form

The second and more serious problem with the commodity-form framework follows from its reliance on an analogy between states and commodity-owners. By understanding states in an analogy to individuals that confront each other as formally free, competitive individual entities, the commodity-form theory not only neglects how the increasingly transnational existence of the capitalist class may impact the role of the state. It also inadvertently leads to a replication of the bourgeois imaginary of the state as a natural entity. The theory thus presupposes that the state-form has a clear unitary meaning that can be understood in abstraction from underlying historically specific social relations.[85] Let me unpack this argument by starting with a short detour, beginning with another, also valid critique that has sometimes been advanced of Pashukanis: His narrow focus on the commodity form leads to a near-complete neglect of production, which is the site of both exploitation and class formation.[86] As Tzouvala explains:

---

[84] Wood, *Empire of Capital*. See also David Harvey, *The New Imperialism* (Oxford: Oxford University Press, 2003); Robert Brenner, 'What Is, and What Is Not, Imperialism?', *Historical Materialism* 14, no. 4 (2006): 79–105; Sutcliffe, 'Imperialism Old and New'; Alex Callinicos, *Imperialism and the Global Political Economy* (Cambridge: Polity Press, 2009); Christian Fuchs, 'Critical Globalization Studies and the New Imperialism', *Critical Sociology* 36, no. 6 (2010): 839–67.

[85] Tzouvala, *Capitalism As Civilisation*, 15.

[86] Tzouvala, 25; Li, 'How to Read a Case', 561.

> [T]he attempt to derive the 'nature' of (international) law exclusively from the commodity-form attaches Marxian theories of law to the common-sense realities of the circulation sphere that involve commodity owners trading freely in the market. This, however, ignores the conceptually unbreakable ties between the sphere of circulation and the sphere of production in Marx and the fact that law plays a crucial role in organising the subjugation of this very special commodity, labour-power.[87]

As we saw in the introduction, capitalism is defined by two sets of historically specific social relations: the *vertical* class relations between workers and capitalists, and the *horizontal* market relations among workers themselves and capitalists themselves. If we ignore either of these, we end up with an incomplete and distorted view of capitalism. By constructing the theory of the legal form on the basis of an analysis of the horizontal relationship between commodity owners without sufficiently taking into account how this relationship is premised on the vertical class antagonism, Pashukanian approaches risk underestimating the deep inequality at the heart of capitalist property relations. While this critique is valid, I also think that it underestimates the Pashukanian contribution in elucidating how the legal form, exactly by denoting an abstract equality of subjects, shields over the unequal relations of production. However, if we want to understand the *content* of international law, we need an elaboration of the ways in which the law works to organize and uphold this class subjugation (a subjugation that is not only shielded by the legal form but that is also its presupposition). This brings me to my critique: To understand the role of law in the organization of this subjugation, we need a theory of the role of *the state*. Pashukanis does in fact provide the contours of such a theory role in relation to domestic relations, arguing that class rule takes the form of official state rule only under capitalism:[88]

> In so far as the exploitative relation exists formally as a relationship between two 'autonomous' and 'equal' owners of commodities, contract through which the worker subjugate themselves to the capitalist, 'of whom one, the proletarian, sells his labour power, and the other,

[87] Tzouvala, *Capitalism As Civilisation*, 25.

[88] Pashukanis, *Law and Marxism*, 139–41.

> the capitalist, buys it, political class power can take on the form of public authority. [89]

However, this particular role of the state as an apparatus external to the capitalist class and the individual capitalist somehow vanishes in the Pashukanian account of the relations between states. For all its rigor in demonstrating the legal form as a product of capitalism, the commodity-form theory's explication of international law inadvertently ends up presupposing the form of the state *a priori*. States merely appear as natural entities whose dynamics come to be reflected in juridical battles.[90] But the very concept of the state-system and its relation to the capitalist mode of production goes unaddressed. A Marxist theory of international law requires an adequate theory of the state. Such a theory must distance itself from the liberal imaginary of states as natural or pre-political entities, showing instead how the state plays a distinct role in reproduction of the social relations of capitalism.[91]

By asserting that a Marxist theory of international law requires a Marxist theory of the state, I open up to complex discussions about the historical emergence of capitalism, the state-form, and international law. These discussions, which have in recent decades been dominated by debates between the world-system theory of Immanuel Wallerstein and Giovanni Arrighi[92] and the political Marxism of Robert Brenner and Ellen Meiksins Wood[93], lies beyond the scope of this dissertation. Instead of a detailed reconstruction of these debates, I will confine myself to drawing the crude contours of my own position within them. I follow the political Marxist tradition in seeing

---

[89] Pashukanis, 141.

[90] Tzouvala, *Capitalism As Civilisation*, 15.

[91] Tzouvala, 25.

[92] Immanuel Maurice Wallerstein, *World-Systems Analysis: An Introduction* (Durham: Duke University Press, 2004); Giovanni Arrighi, 'Capitalism and the Modern World-System: Rethinking the Nondebates of the 1970's', *Review (Fernand Braudel Center)* 21, no. 1 (1998): 113–29; Kerem Nişancıoğlu and Alexander Anievas, *How the West Came to Rule: The Geopolitical Origins of Capitalism* (London: Pluto Press, 2015).

[93] Robert Brenner, 'The Origins of Capitalist Development: A Critique of Neo-Smithian Marxism', *New Left Review*, no. 104 (1977): 25-; Wood, *Empire of Capital*; Maïa Pal, '"My Capitalism Is Bigger than Yours!": Against Combining "How the West Came to Rule" with "The Origins of Capitalism"', *Historical Materialism* 26, no. 3 (2018): 99–124; Benno Teschke, *The Myth of 1648: Class, Geopolitics, and the Making of Modern International Relations* (London & New York: Verso, 2003).

capitalism as a system in which all economic actors depend on the market for their most basic needs.[94] Historically, the creation of this generalized market dependency presupposed widespread proletarianization, that is, the establishment of a system of class domination in which a small elite controls the resources everyone else is dependent upon. In other words, the subjugation of part of the population by another part of the population is a constitutive feature of capitalism. This subjugation emerged in late medieval and early modern England, with the crucial help of the state, which was necessary for its creation and remains necessary for its reproduction.[95] As Wood explains:

> [T]he disposition of power between the individual capitalist and worker has as its condition the political configuration of society as a whole - the balance of class forces and the powers of the state which permit the expropriation of the direct producer, the maintenance of absolute private property for the capitalist, and his control over production and appropriation.[96]

Benno Teschke has even argued that the very consolidation of the modern state can be traced back to the need for an authority to facilitate this subjugation. Since the 'constitution, operation, and transformation of geopolitical orders are predicated on the changing identities of their constitutive units', a theory of the state must be attentive to the particular property regimes at particular times.[97] The political institutions under capitalism 'fix social property regimes, providing rules and norms, as well as force and sanctions, for the reproduction of historically specific class relations.'[98] Whether or not we go as far as Teschke and trace the very formation of the state-form back to the rise of agrarian capitalism in 16th century England, the state remains intrinsically connected to capitalism. The state has historically been key to the enforcement of the subjugation necessary for the establishment of capitalism – the process of so-called primitive accumulation. Since then, the state has worked to sustain capitalism by upholding the social relations of production, but also by the expansion of the capitalist mode of production into new territories, thus satisfying capitalism's inherent drive for expansion. This

[94] Wood, *Empire of Capital*, 10.

[95] Wood, 17.

[96] Wood, *Democracy Against Capitalism*, 20.

[97] Teschke, *The Myth of 1648*, 7.

[98] Teschke, 7.

function shines through in international legal discourse. The endeavor to expand the capitalist mode of production into non-capitalist societies has been essential to the evolution of legal concepts of statehood, sovereignty, and civilization. Throughout the 19th century, sovereignty was reserved for 'civilized' states, which was defined as a modern capitalist state as it had developed in Europe and the United States. Ntina Tzouvala shows how the argumentative pattern underlying the notion of civilization continued well into the 20th century, in which the granting of sovereignty was conditioned on an assimilation of capitalist regulatory models.[99] We will delve more into the doctrine of sovereignty in chapter six, which explores how these historical dynamics of the doctrine echo in contemporary discussions of digital sovereignty.

But for now, a crucial question remains: What is the role of the state-system in the current era, in which the global expansion of capitalism is near-complete? The task ahead of us lies in elucidating the evolving yet persistent functions of the state-system – and, by extension, international law – in the 21st century. These reflections will serve as a framework for the interrogation to follow of how international cyber law operates as a mechanism for sustaining and reproducing capitalist social relations in the global economy of our time. In the following, I argue that the state-system of the 21st century plays a distinct role in the sustenance of capitalism, which is both *necessary for* and *external to* the process of capital accumulation.

The State-System in Global Capitalism

We have seen now that the commodity-form theory is valuable in theorizing the legal form and the ideological role of international law, but that it assumes what needs to be explained when it comes to the social relations between states giving *content* to this form. The state-system has historically played a distinct role in capitalism which is external to capital but necessary for its reproduction and expansion. We have now come to consider the role of the state-system – and, by extension, international law – in the current era in which the global expansion of capitalism is near-complete.

It is in our effort interrogate that question that the scholarly contestations of Hardt and Negri's radical claim of the declining significance of states come in helpful. Before diving into these insights, a caveat is in place that the role of the state-system remains complex and manifold. I am well aware

[99] Tzouvala, *Capitalism As Civilisation*.

that addressing the question at this general level necessarily risks results in some degree of reductionism. Rather than claiming to offer final answers, I will emphasize two overarching functions that states fulfil in contemporary global capitalism: The need for *stability* and the need for *expansion*. With the increasingly global life of capital, I will further argue that these functions increasingly rely not on individual states but on the *state-system.*

First, capitalism needs a certain level of stability and predictability in its social arrangements. One of the most vital ways in which states provide this stability is by possessing the 'ultimate coercive force that capital needs but lacks.'[100] By supplying an elaborate legal and institutional framework, backed up by coercive force, states sustain not only the social relations of capitalism but also its complex contractual apparatus and its intricate financial transactions.[101] The detachment of economic from extra-economic power is unique to capitalism. It allows the economic power of capital to reach far beyond the grasp of existing political and military power. However, importantly, capital's economic power cannot exist without the support of extra-economic force, and the extra-economic force necessary to reproduce capitalism is today, as before, primarily supplied by the state.[102] The formal separation of the state from the capitalist class allows extra-economic force to operate not by intervening directly in the relation between capital and labor, but more *indirectly*, by sustaining the system of economic compulsions, the system of property (and propertylessness) and the operation of markets.[103] Even in an economy that relies on capitalist imperatives, the ultimate sanction that sustains the system as a whole therefore belongs to the state, which commands the legal authority, the police and the military power necessary to exert direct coercive force.[104] While the capitalist class exploits propertyless workers forced to sell their labor power to survive, the state plays a key role in maintaining these property relations at arm's-length from capital.[105] Even if Pashukanis – and Miéville – captured the important role of the state in upholding stability in property relations on a domestic level, the two problems raised above impeded them from considering the

[100] Wood, *Empire of Capital*, 24.
[101] Wood, 17.
[102] Wood, 5.
[103] Wood, 4.
[104] Wood, 16.
[105] Wood, 16.

implications of this role for the state-system, states' international relations, and international law.

I follow Ellen Meiksins Wood in arguing that the more universal capitalism has become, the more it needs an equally universal system of reliable local states to uphold these social relations across geographical borders.[106] In *Empire of Capital*, Wood shows how states, by securing property relations through the exercise of direct extra-economic coercion, provide the stability and predictability needed for capital accumulation.[107] As flows of commodities and money are becoming global, the establishment of stable and reliable conditions on the entire routes of exchange across the globe are vital for the reproduction of capitalist social relations. A global system of capitalist states is thus necessary to provide the stability and predictability needed for global capitalism.

Second, capital is, by definition, expansive – it contains an inherent strive to seek 'beyond every spatial barrier'.[108] To appreciate the role of the state-system in the facilitation of this expansion, let us first reiterate how the capitalist economy compels everyone to follow particular logics. Individual capitalists must follow the laws of the market to survive.[109] Capitalism's inherent tendency towards crises and stagnation arises, at least in part, from the fact that the individual capitalist is compelled to seek out profits even at times where the market is satisfied. This frequently leads to overaccumulation, which we may follow Harvey in defining as a 'surplus of capital lacking profitable means of employment'.[110] In contrast to individual capitalists, which make decisions based on the imperatives of capital, states operate *in abstraction* from the interests of individual capitalists and work to sustain *capitalism as such*. Avoiding stagnation requires that capital is reinvested and thus kept in circulation. States play a central role in keeping up economic activity, including by seeking out new terrains for capital, making investments, and manipulating the forces of the market including through the weapon of debt.[111]

---

[106] Harvey, *The New Imperialism*, 2003; Wood, *Empire of Capital*; Callinicos, *Imperialism and the Global Political Economy*.

[107] Wood, *Empire of Capital*, 17.

[108] Karl Marx, *Grundrisse: Foundations of the Critique of Political Economy* (London: Penguin Publishing Group, 1993), 524.

[109] Wood, *Empire of Capital*, 10–11.

[110] Harvey, *The New Imperialism*, 2003, 42, 87f.

[111] Wood, *Empire of Capital*, 12.

A way for states to avoid stagnation has historically been to maintain capitalism's constant geographical expansion, thus opening up demand for both investment goods and consumer goods in non-capitalist territories.[112] Following David Harvey, the 'implication is that non-capitalist territories should be forced open not only to trade (which could be helpful) but also to permit capital to invest in profitable ventures using cheaper labour power, raw materials, low-cost land, and the like.'[113] The collapse of the Soviet Union and China's economic liberalization led to the large-scale integration of previously inaccessible assets into global capital accumulation.[114] As new territories were opened up to capitalism, wide-ranging structural, institutional, and legal changes were accomplished in those states in their efforts to become active players in global capitalism.[115] Particularly since the establishment of the World Trade Organization in the mid-1990s, the European Union and the United States have been pressing free trade on other states to allow for the global flows of capital and commodities and enable continuous accumulation.[116] These efforts have been accompanied by promotion of debt levels, embodied in the domination of the IMF, the World Bank and financial institutions in the Global North which would impose loan conditions that opened up Global South states to the exploitation of their assets.[117] The neoliberal era provides the most striking illustration of these tendencies. In the aftermath of the crisis of overaccumulation in the 1970s, the United Kingdom and the United States 'transformed the whole orientation of state activity away from the welfare state and towards active support for the 'supply side' conditions of capital accumulation.'[118] Privatization of public domains, release of raw materials such as oils, and public investments in labor-saving technologies (which we will explore in chapter three) constitute examples of capitalist states' attempts to keep up the economic activity on which capitalism is dependent, preventing crises and stagnation.[119]

---

[112] Harvey, *The New Imperialism*, 2003, 139.

[113] Harvey, 139.

[114] Harvey, 149.

[115] Harvey, 153, 156.

[116] Callinicos, *Imperialism and the Global Political Economy*, 9.

[117] David McNally, 'From Financial Crisis to World-Slump: Accumulation, Financialisation, and the Global Slowdown', *Historical Materialism* 17, no. 2 (2009): 39; Harvey, *The New Imperialism*, 2003.

[118] Harvey, *The New Imperialism*, 2003, 157.

[119] Harvey, 150.

Scholars like Harvey, David McNalley, and Neocleous assert that the continuous state subsidy of the capitalist economy to avoid stagnation amounts to a continuous form of so-called primitive accumulation.[120] To Neocleous, new enclosures are permanently enacted as a process essential to the accumulation of capital, from the privatization of 'anything that looks remotely like "the commons"' to the ending of 'anything that looks like communal control of the means of subsistence'.[121] Harvey, rephrasing this process as 'accumulation by dispossession', similarly points to the privatization of global environmental commons such as water, air, and land, corporatization of hitherto public assets, such as universities, and privatization of nationalized industries as examples of states expanding the terrains open for capital accumulation.[122] Here is not the place to discuss whether these forms of accumulation can be properly conceptualized as so-called primitive accumulation, accumulation by dispossession, or something else. Rather, the crucial point for our purposes is that capitalist states play a central role in facilitating capitalism's seamless flows through their territories and continuing to seek out new terrains for capital.[123] While some of the methods through which states fulfil this function are mainly domestic, the global life of capital entails that the task increasingly lies on a *system of capitalist states*.

We can therefore conclude that states and the state-system continue to play crucial roles in contemporary capitalism, perhaps even more so in a time when the whole world is fused into one big economic system. The formal separation of states from the capitalist class allows states to ensure stable and reliable property relations, ultimately with extra-economic force, at arm's-length from capital. Furthermore, the formal separation of states from the capitalist class allows states to facilitate capital's continuous expansion, thus solving the recurring problem of overaccumulation. Capitalism therefore continues to be dependent on the state-system, and the state-system plays a continuously central role in capital accumulation which is external

---

[120] Harvey, *The New Imperialism*, 2003; David Harvey, 'The "New" Imperialism: Accumulation by Dispossession', *Socialist Register* 40, no. 40 (2009); McNally, 'From Financial Crisis to World-Slump'; Mark Neocleous, 'International Law as Primitive Accumulation; Or, the Secret of Systematic Colonization', *European Journal of International Law* 23, no. 4 (2012): 941–62.

[121] Neocleous, 'International Law as Primitive Accumulation; Or, the Secret of Systematic Colonization', 960.

[122] Harvey, *The New Imperialism*, 2003, 145–49.

[123] Callinicos, *Imperialism and the Global Political Economy*, 84.

to, yet vital for the reproduction of the social relations of capitalism.[124] This means that global capitalism is deeply reliant on a system of capitalist states.

In turn, states have a strong incentive to pursue such policies that sustain and support the capitalist economy, because they have become dependent upon economic growth for their own existence and functioning.[125] William Clare Roberts explains how this dependency of the state upon capital makes the state inherently hostile to any attempts of refusing, evading, or escaping capitalism: 'All such attempts will, just to the extent that they are or promise to be successful, encounter the armed agents of the state. *This is where the state fits into capitalism*.'[126] Capitalism, then, is a global system that eventually compels everyone, including statßes, to follow.

A Marxist Lens

In this chapter, we have seen legal form carries a categorical symmetry with the form of the relationship between commodity owners. The formal equality between legal subjects shields over the material inequality in the social relations of capitalism, which are defined by the different access that individuals have to productive resources. As such, while the social relationship expressed in the legal form is the relationship between formally equal, sovereign individuals, the 'content' of law is an expression of the real dynamics of the underlying social relations. In international law, states relate to each other as formally sovereign and equal entities. What comes to constitute the 'content' of law within this form expresses the dynamics of the underlying social relations between states. Understanding the dynamics of these relations, however, requires us to move beyond the Pashukanian framework; these dynamics cannot be understood in a simple analogy between states and capitalist social relations, because the role of states in the reproduction of capitalism is external to capital. An analysis of international law should thus center on the state-system and its specific role in the reproduction of global capitalism. States should not be analyzed as autonomous *sources* of power, but rather as entities playing a vital role in the reproduction of capitalism. But where does this leave us in a study of why international cyber law takes a particular content?

---

[124] Wood, *Empire of Capital*, 15.

[125] Roberts, 'What Was Primitive Accumulation?', 533.

[126] Roberts, 533. (my emphasis). See also Fred Block, 'The Ruling Class Does Not Rule', *Socialist Revolution* 6–28 (1977): 58–59; Callinicos, *Imperialism and the Global Political Economy*, 86.

It is now possible to translate this general framework into two specific propositions that can guide and structure the study of international cyber law to follow. *First,* the 'content' of international cyber law requires an interrogation of the specific dynamics of the state-system in relation to the social relations of capitalism out of which the contemporary information technology landscape has emerged. Positivist scholarship misses entirely how the social relations of capitalism are the crucial connection between the state-system and the information technologies to which they seek to apply international law. They thus focus their analyses on states' immediate attention to the information technology landscape as if it had an autonomous, natural existence. A Marxist study of international cyber law should interrogate the information technology landscape as the result of the social relations of capitalism out of which it has emerged. The first step thus lies in scrutinizing the social relations underlying the information technology development of the past half century and examining the role of the state-system in the reproduction of these relations. This task will be the endeavor of chapter three.

Second, the crystallization of consensus on certain 'rules' of international cyber law reflects the common ideas of capitalist states with the coercive power to ultimately back their interpretation by force. When certain ideas are accepted as legal, they are given a natural, independent existence, which makes them seem raised above political contestation. Here, the task for a Marxist study of international cyber law is to elucidate these operations. The second step thus lies interrogating the emergence of the field of international cyber law and root it in the role of states and the state-system in the reproduction of the social relations of capitalism (chapters four to six).

CHAPTER III
THE DIGITAL LANDSCAPE

This dissertation is fundamentally about international law, not information technology. However, international law cannot be understood in a vacuum from material reality. As we saw in the preceding chapter, the 'content' of international law expresses the role of the state-system in the reproduction of the social relations of capitalism. To understand why particular ideas become accepted as international cyber law, it is necessary to commit to a certain level of engagement with the information technology landscape as it has emerged out of these social relations. I thus find myself, to quote Marx, 'in the embarrassing position of having to discuss what is known as material interests.'[1] In this chapter, I therefore tell the story of how the contemporary information technology landscape has emerged out of the social relations of capitalism. Moreover, I illuminate the crucial role played by states in the technological development process – and, by extension, their role in the reproduction of capitalism.

The chapter begins by situating the analysis to follow in the economic context out of which the information technology landscape has emerged. Against this backdrop, I begin the analysis with the invention of the digital code in the 1950s, soon followed by a growing interest in connecting digital computers to each other. I then turn to examine how the opportunities now unlocked by these groundbreaking, and publicly funded, technological inventions, were appropriated and further developed to increase profits. I

[1] Marx, 'Preface'.

finally examine some of the more recent technological developments and economic restructurings, including changing labor relations and the emergence of new types of commodities in the contemporary data economy. In conclusion, I offer some reflections on how the insights of the chapter challenges an otherwise dominant technology view, setting the scene for the chapters to follow.

CONTEXTUALIZATION

In popular accounts of the emergence of information technology, a 'Darwinian' discourse prevails that successful technology – that is, the technology that has come to dominate as the only viable and available solution to a given task, must have evolved in some 'necessary' way, analogous to that of natural selection.[2] Any successful technology must, by definition, be the best, simply because it was the one to survive the rigorous trials of the competitive marketplace.[3] This tendency not only has the effect of removing any sense of agency from the individual. It also has the effect of removing any sense of agency from *humankind,* and thus, of naturalizing technological developments and raising them above the sphere of political contestation. Technological developments appear as an 'autonomous process, having a life of its own which proceeds automatically, and almost naturally, along a singular path.'[4] In this view, the technological landscape is not the result of the will and action of persons with the capacity to act, but rather as the only possible outcome of an unavoidable, natural selection. As we will see in chapter four, the field of international cyber law is no exception to this discursive tendency.

Against the backdrop of this longtime popular Darwinian narrative, I will argue for what I find to be a more accurate conceptualization of technologies: Technologies reflect the mode of production prevalent in a given society at a given time. Humans cannot survive without technology. At any given historical period, humans have developed technologies for their own reproduction. The use and construction of technology is inherent to the human labor process; humans are 'a tool-making animal'.[5] The techno-determinists are therefore correct insofar as technology is a natural feature of the human species. Besides from this transhistorical fact however, the *particular*

[2] Noble, *Forces of Production*, 144–45.

[3] Noble, 144–45.

[4] Noble, xi.

[5] Marx, *Capital: A Critique of Political Economy. Volume One*, 286.

technologies developed and deployed for the survival and reproduction of humans depend entirely on the given economic formations of society. Technologies of a given society reflect their modes of production; quoting Marx, '[r]elics of bygone instruments of labour possess the same importance for the investigation of extinct economic formations of society as do fossil bones for the determination of extinct species of animals.'[6] Different economic epochs are characterized by different instruments of labor, and all tools are thus historically specific and reversible. This means that there is nothing natural or inevitable about specific technologies at use at a given time. The path of technological development is not prescribed in evolutionary terms; it merely mirrors the historical epochs through which it has moved.

As capitalism is now the dominant economic system on a global scale, it is useful to reiterate the basic features of this system before we can appreciate how the contemporary information technology landscape has emerged and taken shape within it. As we saw in the introduction to this dissertation, capitalism describes a society in which the dominant mode of production is the production and exchange of commodities with a view to generate profit. The term *capital* describes this process, which we can summarize in the formula M-C-M'. The key to the creation of surplus value lies in the production process in which the means of production is brought together with labor power, resulting in a commodity that the capitalist can bring to the market and exchange for more money than he put into the process, resulting in a profit. We also saw in the introduction how a precondition for the generation of profit is the establishment and reproduction of a particular set of social relations, which are characterized by specific logics that everyone must follow: In the vertical relations between workers and capitalist, the worker must sell their labor power to survive. In the horizontal relations between capitalists, companies must follow the laws of the market, which entails putting profit above all other considerations. This inherent strive for profit entails that capitalism is driven toward endless expansion.[7]

Under capitalism, the development of technologies is taking place within these social relations and is bound to follow the logics of capital. By means of their ownership over the means of production, the capitalist class has the power to direct the production process and the resources to develop new technologies. The individual capitalist is not, however, free to choose

[6] Marx, 286.

[7] Harvey, 'The Enigma of Capital and the Crisis This Time'.

whatever technology they find useful on the basis of whatever interests and concerns they might have. The technological design choices must follow the laws of the market, which entails that profit must be put above all other considerations.[8] The competition between capitalists entails a constant drive to produce technologies that reduce production costs. In the vertical relationship between the capitalist and the workers, the capitalist must maintain their position of control, thereby remaining in power of the means of production and keeping down wages.

As we saw in chapter two, states play an indispensable role in the reproduction of capitalism. The capitalist state is dependent on a 'healthy' capitalism that generates a certain level of growth. Historically, technologies that improve capital accumulation have been instrumental in ensuring such growth and thus preventing stagnation. While capitalists have an incentive to develop such technology, technological inventions are sometimes too costly to be deemed profitable or 'worth the risk' for the individual capitalist. The capitalist state may therefore intervene and provide the capitalist class with research in technological inventions ready for appropriation by the capitalist class.[9]

Now that we have situated the analysis within the broader context of capitalism, it is useful to zoom in on the particular historical period in which the technologies at issue – information technologies – have emerged and developed, that is, from the mid 20th century and beyond. In the years following World War II, the global economy was characterized by strong postwar growth, often referred to as the golden age of capitalism. Global manufacturing production expanded at an average annual rate of 7.1 per cent per year, in real terms.[10] The increasing productivity and intensified global competition enabled by new technological inventions resulted in persistent overcapacity in manufacturing. As a consequence, profit rates systematically declined from the mid-1960s.[11] From the start of the so-called 'long downturn' around 1973, capitalist states managed to prevent the kind of crises that had historically troubled the capitalist system by increasingly relying on

[8] Wood, *Empire of Capital*, 10–11.

[9] Harvey, *The New Imperialism*, 2003, 145–50.

[10] Robert Brenner, *The Economics of Global Turbulence: The Advanced Capitalist Economies from Long Boom to Long Downturn, 1945-2005* (London & New York: Verso, 2006); Aaron Benanav, 'Automation and the Future of Work—1', *New Left Review*, no. 119 (2019): 24.

[11] McNally, 'From Financial Crisis to World-Slump', 49.

borrowing, both public and private, to boost demand. However, this strategy achieved only limited stability, which came at the expense of worsening stagnation. With the growing debt burden and the persistent issue of overcapacity, the economy was increasingly immune to such stimulus efforts.[12]

In response, a profound economic restructuring took place following the recessions of 1974-75 and 1980-82. In the United States, a neoliberal economic policy was carried out to reassert American competitiveness, which sought to weaken union power, strengthen financial capital and reassert the centrality of the dollar as the international means of payment. The United States implemented the largest tax reduction history together with a series of stimulus packages, indicating a willingness to do whatever was necessary to prevent economic depression and create the conditions needed to stimulate private borrowing and demand.[13] As we will see, this endeavor further involved the undertaking of a massive expansion in spending on the defense-backed information technology industries, positioning the United States as a global pioneer in emerging high-tech industries. Profound changes in production methods were the combined effects of neoliberal economic policies and technological investments.

The 1990s and start 2000s marked a period of exceptional economic optimism, not least in light of the end of the Cold War and capitalism's definitive expansion into a global market. However, this period proved to be more of a parenthesis in the global economic history than a profound turn, as the capitalist economy has continued its tendency towards crises and stagnation since then. In an effort to overcome this tendency, capitalists continue to seek out new terrains for growth. Capitalist states have supported these efforts through the facilitation of new terrains for expansion enabled by borrowing, technological investments, and attempts at effectively expanding liberal rule to the Global South (a process to which we will return in chapter four).

The invention of the digital code and the technological breakthroughs enabled since then must be understood as concrete responses to the

---

[12] Robert Brenner, 'What Is Good for Goldman Sachs Is Good for America: The Origins of the Present Crisis', *UCLA: Center for Social Theory and Comparative History*, 2009, 2.

[13] Brenner, *The Economics of Global Turbulence*, 165–67; Charmaine Chua and Spencer Cox, 'Battling the Behemoth: Amazon and the Rise of America's New Working Class', *Socialist Register* 59 (2022): 3–4.

economic imperatives existing throughout this period. As I will show, the research underlying the most economically risky, and most groundbreaking, technological inventions, were carried out by states, particularly the United States. However, these technologies were soon adopted and further developed by corporations to whom the digital code unlocked a series of opportunities to maximize and seek out new venues for profit. These opportunities included labor-saving through automation, opportunities to seek out the cheapest markets for labor power and pit workers from different regions against each other, a minimization of freight costs, and an increasing control over the labor process through centralization, deskilling, and surveillance of workers.

In the following, I begin the story of the construction of the contemporary information technology landscape with an analysis of the emergence of its basic components, which were both inventions of the United States Military: The digital code and the internet. I then turn towards what I will argue to be the most profound changes to follow from these inventions, rooting these inventions in the social relations of capitalism.

The Digital Code

The most fundamental technological breakthroughs underlying the contemporary landscape of advanced information technologies were results of public-private research partnerships established for military purposes in the United States during World War II. American elite research institutions such as the Massachusetts Institute of Research (MIT), California Institute of Technology, Columbia University, and Harvard University carried out wartime military research under contracts with the Office of Scientific Research Development.[14] Tremendous amounts of public money were put into the research activities carried out at these private research institutions.

While analog computers had become increasingly prominent in the first half of the 20th century, the earliest digital computers began to be built in the end 1930s. The military context for the creation of the digital computer is reflected in its basic architecture. The system of numerical control, perfected at the Massachusetts Institute of Technology, was initially competing with alternative, equally promising methods of automation, most notably the record-playback method. Numerical control was a more complicated system than record-playback, but the required skills was those of managers

[14] Noble, *Forces of Production*, 10–11; Mueller, *Breaking Things at Work*, 96.

and programmers. In turn, record-playback depended on the skills of a machinist to record the moves to be replicated by the machine. Ultimately, the system of numerical control was chosen, but for reasons other than the technical superiority typically advanced by its promoters. It was chosen because it suited the specific needs of those in control of the technological systems: Its design would make its operators almost independent of skilled machine workers. Alternative systems such as record-playback left control in the hands of skilled workers.[15] The system of numerical control underlying any piece of information technology as of today was therefore not chosen because it was a more productive piece of technology than its contemporary alternatives, but because of its architecture of centralized command and control.

As we saw above, the global economy in the years following World War II was characterized by strong post-war growth and a rapid expansion of global manufacturing production.[16] In this era, the United States not only had the most dynamic economy in the world – it also had the most advanced technologies.[17] The technologies established in private-military partnerships turned out to have a broader scope of application than the military context for which they were initially developed. The military demand for efficiency, centralized control and effective monitoring mirrored an industrial interest in upholding control over workers. The capitalist imperative to maximize profit in every endeavor necessitates a relentless pursuit of technological innovations to reduce costs. By not only automating work processes, but also disempowering workers, the system of numerical control was attractive for industry for exactly the same purposes that had made it the preferred technology in the military context in which it had been born. The extensive public investment in military technology empowered the machine tool industry to develop and produce commercially available models of numerical control machine tools.[18] By the mid-1950s, numerical control had emerged from the military research collaborations to become a sophisticated, albeit complex and costly solution for automating machine tools. With continued state

---

[15] Noble, *Forces of Production*.

[16] Brenner, *The Economics of Global Turbulence*; Benanav, 'Automation and the Future of Work—1', 24.

[17] Benanav, 'Automation and the Future of Work—1'.

[18] William Makely, '50 Years of Technological Development', Cutting Tool Ingeneering, 2005, 6.

subsidies, it soon evolved into the defining and widely adopted approach to programmable automation, shaping manufacturing not only in the United States but across the industrialized world.[19]

The electrical power and petroleum refinery industries were amongst the first to deploy the new technologies. Throughout the 1950s, digital computers were increasingly used to monitor performance, log data, and instruct operators. The development quickly escalated, and by 1964 there were some one hundred digital computers in the United States petroleum-refining industry.[20] The tendency soon spread to every industrial sector.[21] Steel rolling mills, blast furnaces, and various chemical processing plants around the United States came under full computer control during the 1960s.[22] The introduction of new computer-control technology was accompanied by a significant loss of worker demand and worker control.[23] Their ultimate weapon, the strike, had lost much of its power, since the accelerating automation undermined its effect. Rather than illuminating the necessity of competent workers, strikes just gave supervisors and technicians an opportunity to automate even more.[24] Several strikes were lost in the petroleum refinery industry during the late 1950s and early 1960s, as the refineries were able to continue production at nearly full capacity. As a result, union density declined dramatically and persistently in the United States, Canada, United Kingdom, France, Spain and elsewhere.[25] Waves of automation sped up and intensified work processes, pushed down real wages, shed labor, and broke down shop-floor organization of workers.[26]

Faced with the threat of communist expansion in Europe, East Asia, and Southeast Asia, the United States was willing to share its technological advancements with former imperial rivals like Germany and Japan, as well as other key nations, to bring them under its security umbrella.[27] Over time, more states began to develop manufacturing capacity, embraced export-driven growth, and entered global markets. This resulted in a slowdown in

---

[19] Noble, *Forces of Production*, 144.

[20] Noble, 61.

[21] Doctorow, *The Internet Con*, 20.

[22] Noble, *Forces of Production*, 60.

[23] Noble, 64.

[24] Noble, 65–66.

[25] McNally, 'From Financial Crisis to World-Slump', 47.

[26] McNally, 47.

[27] Benanav, 'Automation and the Future of Work—1'.

manufacturing output growth, and labor deindustrialization spread not only to Latin America, the Middle East, Asia, and Africa, but to the global economy as a whole.[28]

THE INTERNET

In extension to the interest in automation, a strong miliary interest persisted in connecting digital computers to each other. The United States Department of Defense eventually funded the creation of ARPANET, designed as a decentralized communication system allowing data to travel between computers through multiple paths. ARPANET came to be the center of an interconnected group of networks that we know today as the internet.[29] Like the system of numerical control, most of the research underlying the realization of ARPANET was carried out by private research institutions and paid for by the United States.[30] In 1973, SATNET (or the Atlantic Packet Satellite Network), linked computers from ARPANET to Europe for the first time.[31] With this possibility of interconnection between computers came also major commercial potentials. In 1985, the first .com-domains were registered, and by the early 1990s came the World Wide Web and the introduction of commercial browsers (Mosaic and then Netscape). A separation was completed ten years later between the military aspect the civil aspect of ARPANET, leading to the birth of a global system of interconnected computer networks, which we know today as the internet.[32] Throughout the 1990s, the United States Government gradually transferred the ownership

---

[28] Benanav.

[29] The story of ARPANET is often taken to be the starting point of any history of the internet on a global scale. However, parallel efforts were in fact taking place around the globe: the economic management project Cybersyn in Chile, the National Physical Laboratory Network in the United Kingdom and Akademset in the USSR are just a few examples. I focus this chapter on ARPANET because it was ARPANET that eventually became the dominant technology – not because of its technical superiority but because of its position in the geopolitical landscape of the time. See Liam Mullally, 'The Actually Existing Internet: Opening the Internet (1969-1991)', *The Autonomy Institute* (blog), 2024; Evgeny Morozov, 'The Santiago Boys - the Tech World That May Have Been', Chora Media, n.d.

[30] Liam Mullally, 'The Actually Existing Internet'.

[31] Liam Mullally.

[32] Liam Mullally.

of the internet's infrastructure from the state to commercial hands.[33] As corporations had now taken over the infrastructure – created at enormous public expense – they began to make profit from selling access to it.[34] The privatization of internet governance culminated with the formation of the Internet Corporation for Assigned Names and Numbers (ICANN) in 1998, which took over from the United States the technical maintenance of the internet.[35]

When studying the transmission of technological solutions from the military to the market taking place during the Cold War, one feature is remarkable: As predicted by Murray Geisler in 1960, 'management problems of large military organizations share much in common, both on the general and specific level, with those of private industrial and commercial organizations'.[36] Military and large corporate organizations both need effective systems of communication between units and a centralization of control that effectively concentrates the power at the top organizational layer. The outputs of military logistics research, such as the digital code and the internet, therefore had immense relevance to private industries – and by extension, to contemporary capitalism.[37] The technological inventions resulting from the scientific efforts carried out in public-private partnerships for military purposes thus resulted in technologies that became an essential precondition for massive automation in industries, as well as for the corporate adventures later to take place in Silicon Valley and beyond.[38]

As Mariana Mazzucato has shown, contemporary advanced information technology products would not exist without the massive amount of public investment behind the computer and internet revolutions.[39] The costs of the necessary initial research clearly exceeded what would have been achievable

---

[33] Couldry and Mejias, *The Costs of Connection*, 20; Ben Tarnoff, *Internet for the People: The Fight for Our Digital Future* (London & New York: Verso, 2022), xiii.

[34] Tarnoff, *Internet for the People*, xiv.

[35] See Mueller, *Ruling the Root*.

[36] Murray A. Geisler, 'Logistics Research and Management Science', *Management Science* 6, no. 4 (1960): 444; Cowen, *The Deadly Life of Logistics*, 6. Cowen, 6.

[37] Cowen, *The Deadly Life of Logistics*, 6.

[38] At the discretion of the Office of Scientific Research Development leadership, over 90 percent of the research contracts awarded during the war granted ownership of patents on inventions – resulting from this publicly supported research – to private contractors. See Noble, *Forces of Production*, 16.

[39] Mazzucato, *The Entrepreneurial State*.

within the commercial sector alone. While the pressure of competition generally incentivizes the individual capitalist to develop new technologies that allows them to decrease their costs of production, the individual capitalist is constrained by the available finances, and research into new technology entails a financial risk. In contrast, we saw in chapter two how capitalist states act in abstraction from the interests of the individual capitalist to sustain the general economic activity of society. It was therefore precisely the separation of the state from market forces that enabled it to fund the extensive research that would later make up the foundation for many of the most profitable inventions.[40] The substantial role of states in the development of the contemporary information technology landscape not only disproves a common tendency to attribute the technological progress of the past half century to the tech industry. It also illustrates how states continue to play a role in countering capitalism's tendency towards crises and stagnation by facilitating the continuous expansion of capitalism with extensive subsidies.

However, with capital's inherent strive for expansion, every technological improvement can only satisfy the economy for so long. As the intensification of global competition and increasing productivity enabled by these new technologies increasingly led to overcapacity in manufacturing, resulting in the systematic decline of profit-rates from the mid-1960s, solutions were needed to avoid stagnation. As we saw above, the reliance on borrowing and demand was insufficient – the growing debt burden and the persistent issue of overcapacity left the economy progressively less responsive to such stimulus efforts.[41] A profound economic restructuring soon followed – and information technologies played a key role. One of the most important aspects of the response to the crisis tendencies was the so-called logistics revolution, which enabled a spatial reorganization of manufacturing industries, an attack on working-class organizations, an emasculation of states in the Global South, and a generation of huge new reserves of global labor via what David McNally has described as accelerated primitive accumulation.[42] The emergence of 'lean production', *i.e.* the production of goods in direct response to market demands, came in as another response to the stagnation. The developments resulted in new forms of precarity in the working class, further

[40] Tarnoff, *Internet for the People*, 6–7.

[41] Brenner, 'What Is Good for Goldman Sachs Is Good for America: The Origins of the Present Crisis', 2.

[42] McNally, 'From Financial Crisis to World-Slump'.

hampering workers' collective bargaining power, and continuing to make more people permanently or temporarily superfluous to capital. In addition to the developments in logistics and in production, the acceleration of the global finance industry concentrated unimaginable amounts of wealth in increasingly fewer hands almost without wage-labor. By all these means, rates of exploitation were increased, South-to-North value-flows were accelerated, and the rate of profit was significantly boosted from its lows of the early 1980s.[43] As I show in the following sections, information technology was a vital component in this profound restructuring, which has continued until present.

The So-Called Logistics Revolution

Some of the most profound technological processes of standardization, concentration, and effectivization took place within the sphere of distribution, which emerged as a key response to the economic stagnation. Improvements in efficiencies along transportation routes held the potential to reduce freight costs and significantly speed up the turnover of capital.[44] Firms thus began to compete on the basis of the *distribution* of goods and services rather than merely the products themselves.[45] These major changes were, as I will show soon, enabled by information technologies.

Improved efficiency in transportation was not the end of it. Rather, the emerging sector of logistics quickly evolved from an initial, narrow focus on transportation and storage into a wide-ranging 'science of circulation' responsible for the integrated management of the supply chain as a total system, from purchasing and production to packaging and final delivery.[46] In a time of economic recession, marked by an intensified concern for cost control and competition, the logistics sector thus emerged as a way of reducing costs and increasing profits. Over last 50 years, the logistics sector has evolved into a multitrillion-dollar industry with a central role in the functioning of the global economy.[47] Numerous important technological interventions were underlying this development, many of which are beyond the

[43] McNally.

[44] Deborah Cowen, 'A Geography of Logistics: Market Authority and the Security of Supply Chains', *Annals of the Association of American Geographers* 100, no. 3 (2010): 600–620.

[45] Chua et al., 'Introduction', 619; Danyluk, 'Capital's Logistical Fix'.

[46] Danyluk, 'Capital's Logistical Fix', 2.

[47] Danyluk, 1.

scope of this dissertation's focus on information technologies. However, one inescapably foundational technology needs mentioning: the standard shipping container. By enabling a highly automated system for moving goods from anywhere to anywhere with a minimum of cost and complication on the way, the container made shipping cheap.[48] By making shipping so cheap that industry could locate factories far from its customers, the container paved the way for Asia to become the world's workshop, bringing consumers a previously unimaginable variety of low-cost products from around the globe.[49] Notably, the opportunities unlocked by the imposition of the standard container were reliant on information technologies. Digital computers enabled the immensely complex calculations of quantitative spatial modeling within the shipping industry.[50] And as soon as computers started to be connected to each other, they further enabled the tracking of goods under transportation. On mainland, automated systems empowered by information technology smoothened warehouse management and order fulfillment, reducing errors and lead times and streamlined communication between suppliers, manufacturers, and distributors.[51]

The increasing reliance on advanced, world-spanning logistics systems for the everyday production and distribution of goods entails new vulnerabilities for capitalism. As Martin Danyluk asserts:

> With the global diffusion of manufacturing and the lengthening of supply chains, the reproduction of capitalism depends more than ever on carefully orchestrated movements of goods, components, and raw materials across long distances.[52]

The reshaping of production into what Anna Tsing has called 'supply chain capitalism'[53] has made scholars argue for a conceptualization of logistics not simply as an emergent industry or business science but as a *distinctive mode of*

---

[48] Marc Levinson, *The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger* (Princeton: Princeton University Press, 2016), 2.

[49] Levinson, *The Box*.

[50] Cowen, 'A Geography of Logistics', 615.

[51] Makely, '50 Years of Technological Development', 5.

[52] Martin Danyluk, 'Seizing the Means of Circulation: Choke Points and Logistical Resistance in Coco Solo, Panama', *Antipode* 55, no. 5 (2023): 1371.

[53] Anna Tsing, 'Supply Chains and the Human Condition', *Rethinking Marxism* 21, no. 2 (2009): 148.

power.[54] This mode of power is characterized by an alternative geography, which is not structured around fixed territories, but around a mutating web of lines, junctions, frictions and flows.[55] Logistics systems are increasingly transforming everyday life under the justification that 'rapid, efficient circulation is necessary to the welfare of the economy, the state, and its people'.[56] But while advances in logistics have enhanced companies' abilities to channel flows of commodities and money, they have also brought about deteriorating consequences for much of the world.[57] Capital is increasingly accumulated in ways that exacerbate existing inequalities and produce new forms of danger and precarity.[58] Logistics systems have intensified long-standing processes of exploitation in at least two ways that we may call class-based exploitation and imperialist exploitation, respectively.[59]

First, with the ability to source labor from anywhere in the world, capital can seek out the cheapest sites of production.[60] The improved opportunities to relocate jobs have increased competition between workers in different locations, thereby weakening their collective power.[61] Quoting Jasper Bernes, logistics has been 'one of the key weapons in a decades-long global offensive against labour.'[62] *Second,* the development in logistics centralized and maintained the control of global supply chains in the hands of imperial powers throughout the widespread formal decolonization taking place during the 1950s and 1960s. As Charmaine Chua shows in her forthcoming book, *The Logistics Counterrevolution: Fast Circulation, Slow Violence, and the Transpacific Empire of Capital,* the rise of logistics went hand in hand with the fall of formal empire. Efforts in the Global South to acquire economic independence by nationalizing transport infrastructure were countered by British and American investments in shipping containerization, reshaping global supply

[54] Chua et al., 'Introduction'; Cowen, *The Deadly Life of Logistics*; Danyluk, 'Seizing the Means of Circulation'.
[55] Danyluk, 'Seizing the Means of Circulation', 1371.
[56] Chua et al., 'Introduction', 624.
[57] Chua et al., 624.
[58] Chua et al., 619.
[59] Chua et al., 619.
[60] Mau, *Mute Compulsion*, 273.
[61] Jasper Bernes, 'Logistics, Counterlogistics and the Communist Prospect', *Endnotes*, 2013.
[62] Bernes.

chains through the construction of an expensive, standardized, global system, economically out of reach for the newly independent states.[63]

The so-called logistics revolution has been a vital component in the unfolding of globalization.[64] Sites of extraction, production, and consumption have been linked together into profitable networks across the globe. Global economic space has been remade in a way that promotes the ongoing accumulation of capital.[65] The circulation of goods and the spatial organization of economic activity have undergone profound transformations, intensifying global economic interdependencies and contributing to the creation of uneven geographies of wealth and poverty.[66] The technological opportunities unlocked with the invention of the digital code and the internet were thus operationalized in the development of a complex global economic restructuring, making 'the world smaller and the world economy bigger'.[67]

In close connection to the developments in logistics, profound changes took place within the sphere of production. Information technologies enabled an unprecedented flexibility, precision, and effectiveness in the planning process, reducing waste by downsizing and re-organizing work. In turn, the life of the working class was made ever more precarious. These changes are the subject of the following section.

Production: Lean and Just in Time

An intrinsically connected response to the problem of overcapacity was the development of methods of 'lean production', or just-in-time production, which arose as a more efficient, flexible, and cost-effective alternative to traditional mass production.[68] The concept of just-in-time production can best

---

[63] Charmaine Chua, *The Logistics Counterrevolution: Fast Circulation, Slow Violence, and the Transpacific Empire of Capital*, Forthcoming.

[64] Cowen, *The Deadly Life of Logistics*, 8.

[65] Danyluk, 'Capital's Logistical Fix', 19.

[66] Danyluk, 19.

[67] Levinson, *The Box*.

[68] In critical logistics literature, the development of lean- or just-in-time production is often treated as part of the so-called logistics revolution, reflecting how the sphere of logistics has grown beyond the narrow question of transportation and into a comprehensive discipline that partly removes the boundaries between production and circulation. See Chua et al., 'Introduction'. Alberto Toscano similarly critiques the tendency to class logistics and transport on the side of circulation, asserting that

be understood by contrasting it to the prevalent norm at the time, which we might call just-in-*case* production: Essentially, raw materials were turned into commodities through wage-demanding work with a view to being brought to the market and hopefully sold for a profit. Such procedure involved a risk of producing more commodities than it was possible to sell – a risk that became progressively more real during the era of persistent overcapacity in manufacturing arising from increasing productivity. Just-in-time production came in as a response to that problem.[69] Just-in-time production models entail that suppliers maintain the capacity to expand, contract, modify production in response to changing demands. The tendency became possible through a restructuring of the vertical relations of capital – that is, the relation between the immediate producers (workers) and the owners of the means of production (the capitalists). The traditional model of organizing capitalist production with a permanent staff with fixed hours, sick days, and occasional leaves is expensive and unflexible in times of varying demand. In response, businesses started to increasingly rely on a network of subcontractors, temporary workers, and mutable organizational structures, allowing for the replacement of a full-time workforce with an army of temporary workers whose schedules are irregular and unpredictable.

The reliance on, and tendency to produce, a 'reserve army of labor' is not a new phenomenon. Marx describes in *Capital* how spheres of change in the composition of capital is always connected with violent fluctuations and the temporary production of a surplus population, the existence of which is not only a consequence of capitalism, but also its precondition:[70]

> [I]f a surplus population of workers is a necessary product of accumulation or of the development of wealth on a capitalist basis, this surplus population also becomes, conversely, a lever of capitalist accumulation, indeed it becomes a condition for the existence of the capitalist mode of production. It forms a disposable industrial reserve army, which belongs to capital just as absolutely as if the latter had bred it at its own cost.[71]

---

locational change could be a commodity on its own right, see Alberto Toscano, 'Lineaments of the Logistical State', *Viewpoint Magazine* (blog), 2014.

[69] Jason E. Smith, *Smart Machines and Service Work: Automation in an Age of Stagnation* (London: Reaktion Books, 2020).

[70] Marx, *Capital: A Critique of Political Economy. Volume One*, 782.

[71] Marx, 784.

The emergence of just-in-time-production has kept a progressively larger part of the population out of stable labor relations, thus marking a continuation and exaggeration of capitalism's inherent tendency to produce and rely on a reserve army of labor. This tendency has continued until present, as technological developments have given rise to new techniques for keeping workers in precarity.[72] Some of the most profound restructurings have taken place during the last 10-15 years. Technological tools have been developed to facilitate the complex coordination necessary for the establishment of a standby workforce ready to step in according to changing productive needs. Couldry and Mejias describe a tendency toward an essentially technologized form of a subsistence economy in which a growing part of the population is being kept in unemployment so that they can be easily hired in times when overproduction is necessary.[73] The realization of the economic advantages of a temporary workforce requires precise control over the flow of goods and information. The development of information technology control systems that facilitate accurate and quick communication and coordination between units has been key to the emergence of just-in-time production.

Within workplaces, datafication is changing how workers are managed, intensifying the level of control into what Gavin Mueller calls a 'digital panoptic workplace'.[74] Remote desktop surveillance (such as the measurement of keyboard strokes and surveillance of screens), monitoring of work interactions, and bodily surveillance through the use of wearable devices and self-tracking technologies, are all common ways in which capitalists develop and deploy technology to squeeze more profit out of the labor force.[75] In the warehouses of tech giants like Amazon and Walmart, workers are exposed to unprecedented regimes of measurement, surveillance, discipline, and data collection, with even their bodily functions closely monitored.[76] In a recent study, more than half of these workers reported that their required production rate sometimes made it hard for them to use the bathroom, and 91% of Walmart workers had experienced dehydration. Numerous reports have also detailed how Amazon's surveillance of union organizing and

---

[72] Guy Standing, *The Precariat: The New Dangerous Class* (London: A&C Black, 2011).

[73] Couldry and Mejias, *The Costs of Connection*, 61.

[74] Couldry and Mejias, 63; Mueller, *Breaking Things at Work*, 101.

[75] Couldry and Mejias, *The Costs of Connection*, 64–65.

[76] Oxfam America, 'At Work and Under Watch: Surveillance and Suffering at Amazon and Walmart Warehouses', 10 April 2024.

activism amongst their workers. Employee message boards are carefully monitored, software is deployed to track potential union activity, and job postings for intelligence analysts tasked with identifying and addressing 'labor organizing threats'.[77] Accelerating monopolization of these digitalized retail industries further exacerbates workers' precarious position. In many American towns, Amazon is the only major employer, leaving workers with little choice to go elsewhere to sell their labor power.[78]

Through continuous surveillance and monitoring, labor relations are becoming more directly extractive.[79] With the deployment of these high-tech surveillance solutions, industry after industry are pushing employees to their limits.[80] Through lean, continuous monitoring and surveillance, these new rates of exploitation are made to seem like the 'natural' outcome of algorithmic processes, rather than deliberate acts.[81] Infinite amounts of technological inventions are being developed to increase profits by lowering the costs of production through the minimization of labor expenses. These technologies are all designed to ensure a centralization of control over every expenditure and every aspect of the production process in the hands of corporations.

Financialization

Another profound technologically empowered change that arose in response to the global recessions took place in the financial sector. In an era when traditional industrial production was not as profitable as it used to be, the financial sector emerged as a new avenue for capital accumulation. While the financial sector had already become progressively larger in the 1950s and 1960s, it was still operating within the regulatory framework characteristic of the post-war boom.[82] However, across the global recessions of 1974-1975 and 1980-1982, an intense restructuring of the financial sector emerged. The process was enabled by the collapse of the Bretton Woods Agreement in the beginning of the 1970s, which had so far fixed currency

---

[77] Michael Sainato, '"You Feel like You'Re in Prison": Workers Claim Amazon's Surveillance Violates Labor Law', *The Guardian*, 21 May 2024, sec. US news.

[78] Doctorow, *The Internet Con*, 18.

[79] Couldry and Mejias, *The Costs of Connection*, 13.

[80] Esther Kaplan, 'The Spy Who Fired Me: The Human Costs of Workplace Monitoring', *Harper's Magazine*, March 2015.

[81] Couldry and Mejias, *The Costs of Connection*, 62.

[82] Lapavitsas, *Profiting Without Producing*, 3.

exchange rates to gold as the universal standard.[83] In the years to follow, financial assets would expand its share of the total economy. Financialization thus emerged out of the major economic disturbances of the 1970s as a solution to the structural stagnation.[84] Following Costas Lapavitsas, financialization can be understood as 'a systemic transformation of advanced capitalist economies pivoting on changes in the underlying conduct of non-financial enterprises, banks, and households.'[85] Financial markets, financial motives, financial institutions, and financial elites gained increasing importance in the operations of the economy and its governing institutions, both at the national and international levels.[86] The shift towards reliance on speculative activities over production implies an ever-greater reliance on credit and debt.[87] As part of this restructuring, corporate investments became more international in orientation.[88] Between 1980 and 2007, global financial assets grew from $2 trillion to $196 trillion, a substantial part of which was made up of cross-border investments.[89]

Continuous economic expansion characterized the global capitalist economy of the 1990s. An immense hype surrounding 'new technology' and the 'new millennium' fueled the rise of innumerable Internet-based firms, which attracted an extensive amount of attention from venture capitalists, leading to the dot-com bubble, occurring mostly in the stock market of the United States.[90] By late 2000, the flow of easy money came to an end, leading to a burst of the bubble, impacting the entire stock market.

The global recession of 2008-2009 not only elucidated how finance has an inherently destructive influence on the rest of the economy – it also

---

[83] Bretton Woods had enforced the convertibility of the American dollar into gold at a permanent rate, thus fixing exchange rates during the long boom, see Lapavitsas, 3; Harvey, 'The Enigma of Capital and the Crisis This Time'; Brenner, 'What Is Good for Goldman Sachs Is Good for America: The Origins of the Present Crisis'; McNally, 'From Financial Crisis to World-Slump'.

[84] McNally, 'From Financial Crisis to World-Slump', 56; Lapavitsas, *Profiting Without Producing*, 260.

[85] Lapavitsas, *Profiting Without Producing*, 15.

[86] Gerald Epstein, *The Political Economy of Central Banking: Contested Control and the Power of Finance, Selected Essays of Gerald Epstein* (Edward Elgar Publishing, 2019), 380–406.

[87] Harris, 'Globalization, Technology and the Transnational Capitalist Class'.

[88] McNally, 'From Financial Crisis to World-Slump', 49.

[89] Harris, 'Globalization, Technology and the Transnational Capitalist Class', 4.

[90] Lapavitsas, *Profiting Without Producing*, 271.

manifested the pivotal role of states in supporting and promoting financialization.[91] As Lapavitsas shows, collapse of the United States financial system and, by extension, much of global finance was only avoided through state intervention supplying banks with liquidity and capital, all drawn from public resources.[92] Central bank intervention has repeatedly rescued banks while ameliorating the impact of crisis on real accumulation.[93] This integration of financial institutions with the state, which Harvey describes as a 'state-finance nexus', underscores the state's profound dependence on capital and its consequent willingness to do whatever it takes to sustain economic growth.[94]

The emergence of financialization might feel a bit off the topic in a chapter about information technologies. However, the emergence and growth of financialization is a crucial part of the story. The reason why financialization is of interest for our purposes is the pivotal role played by information technologies in the construction of the financial sector.[95] Since the 1990s, algorithmic trading has mechanized and accelerated the speed of speculation in financial markets.[96] Daily trades have become heavily reliant on information technologies and runs without daily human input. Success on the speculative financial market is, above all, dependent on speed in these algorithmic operations.[97] Trade-data is transmitted via fiber-optic cables at about a billion feet every second.[98] The result is a technological competition of having the fastest servers with the nearest proximity to SWIFT, the company who runs the super-computer through which global trades are processed.[99] Physical proximity gives a millisecond advantage in the speed of information – and thereby, in the ability to make profit.[100] Information technology is the

[91] Lapavitsas, 260.
[92] Lapavitsas, 1.
[93] Lapavitsas, 260.
[94] Harvey, 'The Enigma of Capital and the Crisis This Time'.
[95] Jerry Harris, 'Transnational Capital and the Technology of Domination and Desire', *Race & Class* 57, no. 1 (2015): 5.
[96] Laura Bear, 'Speculation: A Political Economy of Technologies of Imagination', *Economy and Society* 49, no. 1 (2020): 7.
[97] Harris, 'Globalization, Technology and the Transnational Capitalist Class', 8–9.
[98] Harris, 9.
[99] Harris, 'Globalization, Technology and the Transnational Capitalist Class'.
[100] Harris, 9.

nervous system of the global financial economy.[101] In moving from analog to digital financialization, the state assumes a new role, which is to support the creation of national digital infrastructures to promote data driven finance.[102] These technological and economic developments have enabled capitalists to become immensely rich with a minimum use of labor.[103] The capitalist class has come closer than ever to realizing the fantasy of jumping directly from money to money magnified (M- M') without the labor-demanding commodity-production as an intermediary step (M–C–M').[104] Information technologies have thus been vital in the centering of financialization in the global economy.

The development towards increasing financialization of the economy has continued ever since its beginning in response to the economic stagnation of the 1970s. Hundreds of new financial products have been created in the current century, which all depend entirely on the functionality of information technology. As of today, financial institutions and assets are the dominant element in the world economy. The top 60 global corporations by assets are all financial institutions.[105] An ongoing circulation of capital flows through international financial institutions, with investments coming from capitalists the world over. Through this activity, a transnational economy is being constructed, giving formation to what some scholars have named the *transnational capitalist class* (TCC).[106] None of these developments would have

---

[101] Harris, 'Transnational Capital and the Technology of Domination and Desire', 7.
[102] Ghazal Mir Zulfiqar, 'Digital Financialization and Surveillance Capitalism in the Global South: The New Technologies of Empire', *Sage Journals*, 2023.
[103] Harris, 'Globalization, Technology and the Transnational Capitalist Class', 8.
[104] Dyer-Witheford, *Cyber-Proletariat*, 23. For a contrary view, see Bear, 'Speculation'.
[105] Marketcap, 'Top Public Companies by Total Assets (February 2025)', Balance sheet, February 2025; Harris, 'Globalization, Technology and the Transnational Capitalist Class', 4.
[106] Harris, 'Transnational Capital and the Technology of Domination and Desire', 5; William I. Robinson and Jerry Harris, 'Towards a Global Ruling Class? Globalization and the Transnational Capitalist Class', *Science and Society* 64, no. 1 (2000): 11–54; Chimni, *International Law and World Order*. For discussions of the TCC in the context of international law, see BS Chimni, 'International Institutions Today: An Imperial Global State in the Making' (2004) 15 European Journal of International Law 1; Akbar Rasulov, '"The Nameless Rapture of the Struggle": Towards a Marxist Class-Theoretic Approach to International Law' (2010); Mai Taha, 'Reading "Class" in

been even near possible without advanced information technology. In turn, a progressively growing share of the world economy is now entirely reliant on stable information technology infrastructures.

We have so far seen how information technologies unlocked a wealth of opportunities to continue capital accumulation despite the consistent tendencies towards crises and stagnation since the 1970s. The emergence of the logistics sector, just-in-time production, and financialization, have been entirely reliant on the technological opportunities denoted by the digital code and the internet. In the remainder of this chapter, the task ahead of us is to trace capitalism's creativity towards new roads to accumulation in the current millennium. Not only have the above phenomena continued steadily until today. The progressively more advanced digital landscape has also given rise to new methods of accumulation.

Platform Capitalism

I will end this chapter by providing some reflections on some of the more recent developments within the digital landscape. In addition to the changing methods of production and circulation, information technologies increasingly became the foundation of new markets for consumption from around the end 1980s and onwards. In the current millennium, personal computers, smartphones, and tablets have come to make up profound needs of everyday life, marking a seamless continuation of capitalism's 'astonishing history of the production of new needs, wants and desires, in part through the production of new lifestyles'.[107] The new digital products for consumption not only allowed the tech corporations to make profit from the sale of a personal computer or a smartphone. It also opened the doors to new methods of accumulation. By the late 1990s, low interest rates and rising venture capital investment fueled the rapid growth of tech startups, contributing to what became known as the dot-com bubble. During this brief but significant period, internet-based companies attracted vast investments, often with speculative business models. Following the burst of the dotcom bubble in 2000, websites changed their business strategies towards more interactivity – a shit sometimes termed the 'web 2.0'. Manifested by the emergence of companies such as Amazon, Facebook, Twitter, and Google, this shift gave

International Law: The Labor Question in Interwar Egypt' (2016) 25 Social & Legal Studies 567.

[107] Harvey, 'The Enigma of Capital and the Crisis This Time'.

rise to the emergent data economy, in which new digital methods of value extraction accelerated.[108] Individual desires, reading habits, consumer preferences and behavior, political beliefs, cultural habits, food preferences, and networks of friends and family, have all become increasingly transparent to the corporate forces in Silicon Valley that own and control the technology on which everyday life is increasingly dependent.[109] Social platform corporations make hundreds of billions of dollars on attracting the attention of social platform users and selling that attention as a commodity to whoever is interested. The selection of content to which platform users are exposed is composed on the basis of complicated algorithms that determine whose attention should be sold to whom.[110] As such, while social media have become central to communication of all kinds, the routes taken by the digital content on these platforms are algorithmically controlled to maximize the generation of profit.

Couldry and Mejias show how human life is increasingly being structured so that it generates data from which profit can be extracted. They employ the term 'data relations' to describe this new type of human relations that allows human life to become an input or resource for capitalism, enabling the commodification of almost every aspect of life.[111] Not only social interactions, but ever more of aspects of life are being continuously monitored and surveilled; as the Internet of Things expands, data relations are established from our use of everyday tools.[112] Kitchen appliances, cars, security systems, lighting fixtures, and thermostats can all be controlled via connected devices such as smartphones, which increasingly have the capacity to monitor its users, collecting data of value to the tool's makers.[113] The availability of personal digital devices has thus opened up new opportunities to exercise surveillance over human life and control it in ways that maximize the generation of profit.

---

[108] Mueller, *Breaking Things at Work*, 108.

[109] Harris, 'Transnational Capital and the Technology of Domination and Desire', 13.

[110] Matthew B. Crawford, *The World Beyond Your Head: On Becoming an Individual in an Age of Distraction* (Farrar, Straus and Giroux, 2015).

[111] Couldry and Mejias, *The Costs of Connection*, 85.

[112] Couldry and Mejias, 7. See also Elsa Kugelberg, 'Dating Apps and the Digital Sexual Sphere', *American Political Science Review*, 2025, 1–16., elucidating corporate intervention into the 'digital sexual sphere'.

[113] Couldry and Mejias, *The Costs of Connection*, 23.

Couldry and Mejias analyze data relations through a colonial lens – an analytical maneuver that I will argue to be highly questionable. They assert that what happens to human life when it becomes an input for capitalism amounts to a new form of colonialism that they term *data colonialism.* As they explain:

> [I]f colonialism can be understood, among other things, as a process that allows one party to occupy the living space of another and appropriate his resources, overpowering him through a combination of ideological rationalizations and technological means (which include the use of surveillance and dominance), then we propose that we have entered a new phase of colonialism.[114]

The colonial terminology suggests that data is a resource, which can be extracted, commodified, and capitalized like a so-called natural resource such as oil, coal, and gold.[115] Although data is clearly not a material extracted from the earth in a 'raw' state, several authors have adopted an expansive definition of extraction that can encompass this apparent anomaly. Couldry and Mejias's overly broad definition of colonialism leads them to overlook central features of historical colonialism. In colonial history, the violent enclosure and dispossession of non-capitalist societies entailed the deprivation of resources from non-capitalist societies, making them dependent on capitalism for their survival (part of the process of so-called primitive accumulation). The problem with this understanding of data in an analogy to raw natural resources lies in its immaterial nature: The 'extraction' of data can hardly be said to entail to the *expropriation* of this resource from others. Unlike territory and natural resources, data is not a 'zero-sum game'; Google's surveillance of my movement does not deprive me of the same knowledge, nor does it deprive others from extracting the same data.

There are arguably more merits to an analysis that analyzes the *control of attention to digital content* through a colonial lens; unlike data, attention demands time, which is a finite resource. We may argue that social platform corporations capture the time of their users and sell it based on complex algorithms to make profit in a maneuver akin to the extraction of natural

---

[114] Couldry and Mejias, 45.

[115] Cornelius Puschmann and Jean Burgess, 'Metaphors of Big Data', *International Journal of Communication* 8 (2014): 1690–1709; Catriona Gray, 'More than Extraction: Rethinking Data's Colonial Political Economy', *International Political Sociology* 17, no. 2 (2023).

resources. However, even here, it is important to keep in mind the *function* of historical colonialism. As part of the process of so-called primitive accumulation, the central aim of colonialism was not so much to build up wealth as it was to expropriate from the majority of the population the *means of their subsistence*. By removing the necessary reproductive resources from people, they were forced to enter into labor relations to survive. However much the commodification of our attention intervenes into our personal spheres and profits from ever more intimate aspects of life, it does not deprive us from the means of our subsistence in a way that in my view merits a colonial lens. Rather than theorizing the contemporary data economy as a new phenomenon, I thus hold it is more accurate to understand it as an expression of the inherent drive for capitalists to seek out new venues for capital accumulation – and thus a continuation of business as usual by new technological means.

Information technologies have also given rise to new forms of labor relations that maximize corporate flexibility through what is sometimes referred to as the 'gig economy'; an economy that relies increasingly on the existence of a precarious workforce that can be readily employed in response to the specific needs of the market at a given time. The 'gig economy' relies on digital platforms that facilitate the buying and selling of labor power with various areas of services, ranging from food delivery and taxi services to digital tasks.[116] Workers are sometimes claimed to be empowered through these tendencies because they, as contractors, set their own hours and choose their own tasks. A *Forbes* article uses the romantic metaphor 'polyworking' to describe a 'growing trend of managing multiple concurrent jobs rather than relying on a single source of income', which allegedly 'gives employees a greater sense of control over their career trajectory'.[117] To the morally conscious minds concerned that polyworking would be like 'cheating on their primary employer', the article gives comfort by ensuring that this is not the case: Polyworking allows employers the 'advantages of a diverse skillset' and a 'more adaptable and resilient workforce'. Other advantages, which are left out in the Forbes article, include escaping the burdens of collective bargaining of organized workers, of regulations concerning minimum wage and

[116] Srnicek, *Platform Capitalism*.

[117] William Arruda, 'Why Polyworking Is The Future Of Work And How To Become A Polyworker', Forbes, 5 November 2024.

retirement, and of having to deal with illness leaves and parental leaves.[118] The platform technologies underlying the gig economy grant employers the privilege of a precarious, and therefore flexible, adaptable and available workforce over whom it has almost no responsibility.[119]

More than making workforces flexible to the changing needs of capital, automation efforts continuously seek to make workers superfluous altogether. Uber makes an accurate illustration of this tendency and, Couldry and Mejias suggests, an indication of a projected direction for global capitalism: First, Uber represented the potential to create new forms of exploitative work through digital platforms. Now, it seeks to circumvent human labor altogether through heavy investigations into driverless cars and trucks.[120] According to Uber, 'autonomous vehicles and human drivers together on one platform means the right ride for every customer is always within reach.'[121] Autonomous vehicles and 'human drivers' come to appear as good colleagues, working together towards the shared goal of improved personal transportation for their clients, awkwardly ignoring how the former is being aggressively developed to disempower and ultimately eradicate the latter. Couldry and Mejias predict that the combined effects of the gig economy and automation will likely be disastrous for most workers in most sectors of the economy: many of them face replacement by machines, while those who remain will more likely accept lower wages and worse working conditions as the specter of a reserve army of gig workers, robots, and artificial intelligence hangs over their heads.[122]

Technology for Whom?

David Noble reminds us that 'when technological development is seen as politics, as it should be, then the very notion of progress becomes

---

[118] A Danish study has shown the effects of collective bargaining on the salary and working conditions in the food delivery sector, a large area for the gig economy. See Magnus Thorn Jensen et al., 'Overenskomst giver take-away-bude bedre vilkår og markant bedre løn' (Copenhagen: Cevea, 16 May 2022). See also Couldry and Mejias, *The Costs of Connection*, 59; Chua and Cox, 'Battling the Behemoth', 12.

[119] Standing, *The Precariat*.

[120] Couldry and Mejias, *The Costs of Connection*, 62.

[121] 'Uber', Uber, accessed 29 November 2024, https://www.uber.com/us/en/autonomous/.

[122] Couldry and Mejias, *The Costs of Connection*, 61.

ambiguous: what kind of progress? Progress for whom? progress for what?'[123] We need, as Cory Doctorow argues, to stop thinking merely about what technology *does* and start thinking about who technology does it *to* and who it does it *for*.[124] In this chapter, we have seen how the emergence and development of information technologies are deeply rooted in the social relations of capitalism. The pressures of competition compel producers to adopt new technologies to reduce labor time, thereby increasing profits. Automation processes, powered by machine learning, have rendered skilled labor increasingly redundant, centralized control over production and weakened workers' collective bargaining power. The rise of an advanced logistics industry has intensified competition among workers across the globe while reinforcing systems of domination and control between the Global North and Global South. Meanwhile, warehouse workers face relentless surveillance and control, exemplified by grueling conditions put in place by companies like Amazon and Walmart. The expansion of the financial sector has been facilitated by sophisticated digital trading technologies, developed and maintained with significant state support. The contemporary data economy continues to commodify more aspects of human life, extending the reach of capitalist exploitation into everyday existence. Simultaneously, the gig economy has exacerbated worker precarity, leaving many without stable employment or protection. Throughout this process, capitalist states, especially the United States, have played an important role in facilitating and financing the research necessary to develop some of the most groundbreaking technological inventions that facilitate ongoing accumulation by exploitation.

That information technologies have changed societies in profound ways has long been a truism. Nevertheless, this rather banal point is often the farthest positivist legal scholars go in engaging with the material reality to which they seek to apply international law. As we embark on the task of exploring how international cyber law has taken form in the following chapters, one key insight from this chapter should remain at the forefront: The profound technological changes are by no means neutral, natural, unavoidable, or predestined. Nor are they irreversible. They are the results and expressions of the social relations out of which they have emerged. These relations are inherently conflictual. Rather than being a domain of universally

---

[123] Noble, *Forces of Production*, xv.

[124] Doctorow, *The Internet Con*, 1. See also Wendy Liu, *Abolish Silicon Valley: How to Liberate Technology from Capitalism* (London: Watkins Media Limited, 2020).

shared values or interests, the information technology landscape is, at its very core, a terrain of conflict and contestation. In this chapter, we have come closer to understanding who and what has driven the technological development. In the chapters to follow, I turn to explore how states and the state-system have responded to this process and how these responses come to be reflected in international cyber law.

CHAPTER IV
CYBER AS *SECURITY*

> If in the past people were connected by sea lanes and trade routes, then today we are often connected by the Internet, along with the threats that loom in cyber-space. … Cyber attacks are a threat not only to sophisticated information technological systems, but also to a community as a whole.
>
> Toomas Henrik Ilves[1]

Security is a peculiar word. It once denotes a universal, shared interest, while also almost certainly presuming a social antagonism; after all, the security risk must come from somewhere. As illustrated by Estonian President Ilves' address to the General Assembly, cyberattacks are widely perceived as a threat to *community as a whole* – an idea that often goes unchallenged.[2] Assessments of cybersecurity appear raised above political contestations and conflicting interests – as technical assessments with which laypeople can hardly disagree.

---

[1] Toomas Hendrik Ilves, 'Address by H.E. Mr. Toomas Hendrik Ilves, President of the Republic of Estonia to the 62nd Session of the United Nations General Assembly' (62nd Session of the United Nations General Assembly, United Nations Headquarters, 25 September 2007).

[2] See for example United Nations Secretary General, 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135)' (United Nations, 14 July 2021).

Ilves did not choose to address the topic of cybersecurity in the United Nations General Assembly in September 2007 out of the blue. A few months earlier, Estonia had become the first state to be subjected to a large-scale Distributed Denial of Service (DDoS) attack.[3] The disruptions, which followed the relocation of a Soviet-era statue in Tallinn in April 2007 and lasted 22 days, were reported to have 'seriously impaired the daily operation of various organisations including banks, government departments, and small businesses,'[4] with online banking being often emphasized as one of its most 'vital targets'.[5] Never before had a cyberattack shut down digital activities of a state so comprehensively. Despite the unprecedented nature of the 2007 cyberattacks, Ilves's language – cyberattacks, threats looming in cyberspace – was familiar in the General Assembly; cybersecurity had become a prominent theme in international fora throughout the past decade.

This chapter turns from the material base to the ideational sphere to explore how the idea of information technology as a security-issue has evolved in the relation between states. As critical cybersecurity scholars have long shown, there is nothing natural or given about the link between information technology and security.[6] The presuppositions on which the dominant notion of cybersecurity relies are by no means natural or uncontestable. Questions about who and what poses a threat, and who and what needs protection, have no natural answers – only social answers. I follow critical security scholars in acknowledging that the word 'security' has a performative character – that is, it does not only describe the world but can also transform social reality.[7] Following Marc Neocleous:

> The starting point of the critique is to see it not as some kind of universal or transcendental value, but rather as a mode of governing, a

[3] Samuli Haataja, 'The 2007 Cyber Attacks against Estonia and International Law on the Use of Force: An Informational Approach', *Law, Innovation and Technology* 9, no. 2 (2017): 160.

[4] Haataja, 161.

[5] Rain Ottis, 'Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective', *Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia*, 2008, 1.

[6] Myriam Dunn Cavelty, 'From Cyber-Bombs to Political-Fallout: Threat Representations with an Impact', *International Studies Review* 15, no. 1 (2013): 105–22; Liebetrau, 'Problematising EU Cybersecurity', 705.

[7] Balzacq, Léonard, and Ruzicka, '"Securitization" Revisited', 495.

> political technology through which individuals, groups, classes, and, ultimately, modern capital is reshaped and reordered.[8]

If we understand cybersecurity not as a fixed, neutral term that can be readily applied to an evolving reality, but as a concept being actively constructed within international discourse, then its power becomes strikingly clear. The notion of cybersecurity has the effect of neutralizing political action and raising whatever purpose it serves above political contestation, cloaking the particular with an emblem of universality. The task ahead of us is therefore to unpack the process through which the now dominant understanding of cybersecurity has been constructed in the social relations between states – in other words, to critically interrogate the emergence of the dominant understanding of cybersecurity.[9]

From the very moment that legal discourse began to migrate into the international discussions of cyberspace a few years after Ilves's speech, the rationalities of the notion of cybersecurity had been well-established and became a *raison d'etre* of the field of international cyber law. The presuppositions as to what needs protection and what makes a threat were thus never part of the legal discussions. If we want to unpack the emergence of these key ideas, we must begin our interrogation well before the point in history when the idea of cyberspace as object of international legal regulation materialized. This chapter therefore examines critically how the contemporary notion of cybersecurity has been constructed in the social relation between states. The analysis begins in the end 1980s when the link between information technologies and security was established in international fora for the first time. It then turns to explore how the discourse on information technologies changed in the neoliberal era of the 1990s, resulting in a revised concept of 'cybersecurity' when security recurred on the agenda around the beginning of the new millennium. Rooting the evolving ideas in the material base, I show how the notion of cybersecurity has emerged and evolved as a reflection of the role of the state-system in global capitalism.

Linking Technology and Security

The link between technology and security emerged within the United Nations for the first time toward the end of the Cold War, in 1988, with the

---

[8] Neocleous, *Critique of Security*, 4.

[9] Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder: Lynne Rienner Publishers, 1998).

General Assembly's adoption of a resolution on Scientific and Technological Developments and Their Impact on International Security.[10] The resolution expressed growing concern over the potential for technological advancements to be applied for military purposes, thereby escalating both the sophistication and destructive capacity of modern armaments. While the resolution contained no reference to *information* technology, it mandated the Secretary-General to prepare and submit a report to the General Assembly on the implementation of the resolution. This subsequent report would later establish the link between information technology and international security concerns, setting the stage for broader discussions on the topic in years to come.

The Secretary-General's report, published in 1990, analyzed technology trends in five key areas: information technology, nuclear technology, space technology, materials technology, and biotechnology.[11] Among these, information technology was highlighted for its crosscutting relevance, as it played a pivotal role in the research, management and control systems of all the other major technologies. The report of the Secretary-General reflects an instrumentalist view of technology that sees information technologies as neutral tools. The report thus described how information technologies made up an 'effective force multiplier', suggesting that information technologies could be instrumentalized to multiply any other force, while itself being omnipotent – and thus, neutral.[12] In this view, information technologies could be *deployed* for a variety of purposes and contexts, which were each laden with particular risks and benefits. The instrumentalist view is further reflected in a notion that information technologies were 'dual-use' technologies, that is, technologies that could be deployed for both military and non-military purposes. Such description detaches technologies from their use, thus depoliticizing technologies by portraying them as merely instrumental to any thinkable purpose of their user.

The security-related aspect of information technology was seen to lie in their potential for a particular type of use, namely, their potential to bring

[10] United Nations General Assembly, 'Scientific and Technological Developments and Their Impact on International Security (Res. 43/77)', 7 December 1988.

[11] United Nations Secretary General, 'Scientific and Technological Developments and Their Impact on International Security - Report of the Secretary General (A/45/560)', 17 October 1990.

[12] United Nations Secretary General, sec. 64.

about dramatic developments in the military sector.[13] The relevance of information technology to security, then, was seen to arise from their military deployment. The very technologies – and the continuous progressive development thereof – were deemed irrelevant to the security assessment. In this view, only a particular type of technology *use* could give rise to security concerns.

While military use of information technology was thus seen to make up a security concern, commercial uses of information technology were promoted as universally beneficial. Drawing on a report compiled two years earlier by a High-Level Experts Group on the Social Aspects of New Technologies for the Organization for Economic Corporation and Development (OECD), the Secretary-General concluded that information technology came to the top in comparison to the other technologies on five counts: *First*, it excelled in generating a wide range of new products and services. *Second*, it significantly improved the cost and technical performance of existing processes, services, and products. *Third*, it enjoyed high levels of social acceptance, positioning it as a transformative force across societies. *Fourth*, it attracted robust private industrial interest, driving rapid innovation and commercialization. *Finally*, its broad applicability across diverse sectors further solidified its status as a leading technology of the time.[14] The commercial use of information technologies was thus being praised for its potential to accelerate growth. By detaching technologies from the concerns that may follow from their specific use, the instrumentalist technology view removes technology out of controversy and contestation.

Conceiving technologies as neutral tools in this manner brings with it an implicit claim that technological inventions occur regardless of social context. Technologies are thus perceived as the necessary outcome of a rational, politically uncontestable development process.[15] In line with this implicit claim, a deterministic understanding of technology is underlying the report of the Secretary-General, revealing itself in a portrayal of information technology developments as inevitable and natural. For example, technologies are described in an active language that attributes agency to technologies. The report notes how information technology 'is moving very fast' and that

---

[13] United Nations Secretary General, sec. 64. (emphasis added)

[14] United Nations Secretary General, 'A/45/560'.

[15] Daniel R. McCarthy, 'Technology and "the International" or: How I Learned to Stop Worrying and Love Determinism', *Millennium* 41, no. 3 (2013): 474.

new materials have 'opened up new possibilities' that will maintain growth rates of computing capability well into the next century.[16] The discursive attribution of agency to technologies has the simultaneous effect of removing any sense of agency from humans – and from states – who must simply adapt to technological change.

In line with this passive understanding of states' position in this rapidly developing technological landscape, the report asserts that all states were dependent on the development of their digital capacities at a rapid pace, as the failure to do so would force the state into the role of 'paying customer for expensive services it cannot do without.'[17] In other words, there was no real choice for a state as to whether to join the digital transition or not; '[i]f a nation falls behind in computing and communication technology, it falls behind everywhere.'[18] States were thus portrayed as having no real influence on the predetermined, automatic course of developments. States were merely compelled to stay at the forefront of the digital transition.

The report further observed that there was a trend in all areas of endeavor to value intellectual property more highly, demonstrated by both the need to encrypt and efforts to decrypt data outside the military arena.[19] The report thus hinted at an emerging role of the state-system in upholding and protecting emerging property relations in the digital space, reflecting how states play an important role the protection of extant property relations. Yet, in these first stirrings of international debate on information technologies and security, the international *security* concerns generally remained related the military use of information technologies, while the commercial use of information technologies was kept out of the security discussions and celebrated as rapid, inevitable developments to which everyone must adapt.

In a follow-up resolution to the report of the Secretary General, the General Assembly reiterated the Secretary General's celebration of information technologies as a potential for new products, investment, and industry, stating that 'progress in science and technology for civilian applications *needs to be maintained and encouraged*.'[20] By seeking to maintain and promote the

---

[16] United Nations Secretary General, 'A/45/560', para. 63.

[17] United Nations Secretary General, para. 70.

[18] United Nations Secretary General, para. 70.

[19] United Nations Secretary General, para. 70.

[20] United Nations General Assembly, 'Scientific and Technological Developments and Their Impact on International Security (Res. 45/60)', 4 December 1990. (emphasis added)

continuous expansion of civilian digital infrastructures, states thus embraced the industrial transformations that had rapidly transformed the global economy.

It is now possible to root this initial link between security and information technologies in the material reality of the end-1980 era. At this time, information technologies that were originally developed and deployed for military purposes in the United States had been significantly advanced and began rapidly to gain momentum. The Reagan Administration's large-scale peacetime military expansion had driven the widespread development of government-owned and government-leased networks. The military sector had so far been the main driver of information technology development, and the commercial adoption of computation had merely followed from the overlapping needs of militaries and corporations, which both benefitted from efficiency, centralized control, and effective monitoring. However, the foundational technology of the digital code had also become broadly available to such an extent that a wider range of commercial actors could now afford to continue the technological development process. Information technologies increasingly began to make up new markets for digital products, as home computers and digital mobile networks were being developed at a high pace. The commercial continuation of the technological opportunities unlocked by the digital code was a source of economic prosperity to be promoted. There was no point in discussing any limitations to the anticipated commercial adventures and resulting growth rates within a framework of security. In this era, the security discussions were thus limited to the military aspects of information technology, while the commercial aspects were deliberately left out of discussions.

In conclusion, the initial link within the United Nations between information technologies and security relies on a view that information technologies are inherently neutral pieces of technology. This means that they can be deployed for a variety of purposes, of which some are military and others civilian – and of which some are deemed a security risk, and others are not. Technological development is seen as an inescapable process, driven at a rapid pace by market forces and beyond governmental control. The security-concerns arise merely from the military deployment of information technologies, while the development and deployment of information technologies for commercial purposes should be encouraged and promoted.

The debate on security in the context of information technologies was on a pause in the international fora of the 1990s. As I will show shortly, the

focus in this era was turned towards the acceleration of the commercial process of global expansion of the 'information society'. In the following section, I interrogate the debates on the information technology landscape of the 1990s. I examine how a decade of market-oriented technophilia came to influence the concept of 'cybersecurity', when security concerns recurred in the discussions of information technology within international fora almost a decade later. As I will show, the concept of 'cybersecurity' had been subtly revised in a way that suited a new reality of digital dependencies arising from the global expansion of the 'information society'.

Information Superhighway

Information technologies remained a hot topic during the 1990s. However, with the end of the Cold War and the temporary cease of global geopolitical tensions, the security-concerns that had before surrounded the discussions of information technology faded from the international agenda. Discussions of the rapid spread of information technologies were instead marked by widespread enthusiasm about the visions for an emerging 'information society'. The era was shaped by a Fukuyaman idea of the 'end of history' – a belief in the universalization of Western liberal democracy as the ultimate form of human governance.[21] Within this narrative, the expansion of capitalism into virtually every geographic and economic corner of the globe was framed as a natural and inevitable consequence of its perceived triumph as the most effective economic system. The development and proliferation of the 'information society' were integral to this broader neoliberal project. Information technologies were thus portrayed as key instruments in promoting free markets, enabling open communication, and fostering global integration, reinforcing the ideological and economic dominance of Western (neo)liberalism.

The United States was a forerunner in the technological development process, propelled not only by substantial investments in technology research as discussed in chapter three, but also by a technophile political climate celebrating and encouraging technological innovation in private industries. A key priority of the Bill Clinton and Al Gore administration was the construction of an *information superhighway*, envisioned as a transformative infrastructure project across the globe. The establishment of a high-

[21] Francis Fukuyama, *End of History and the Last Man* (Simon and Schuster, 2006). See further Marks, *The Riddle of All Constitutions*, 16, 33–37.

capacity, high-speed computer network was seen as having the potential to do for the flow of information what the transcontinental railroad did for the flow of goods a century ago.[22] In 1996, Bill Clinton signed the Telecommunications Bill, the primary goal of which was to liberalize the market of information technology, essentially allowing any communications business to compete in any market against any other.[23] The deregulatory maneuver was seen as a milestone in the 'information revolution', allowing its expansion 'all across our land and across the world'.[24] Technological progress was perceived as an unstoppable development driven by inexorable market forces. In this perspective, the only viable response option was to embrace the transformation, to become 'wired and connected,' and to participate in the supposed joys and benefits of the 'Digital Technology Revolution'.[25] Such framing presents technological changes as natural and self-evident developments in a global trajectory toward a destined digital future for humanity.

Throughout this period, the facilitation of the expansion of the 'information society' became a central agenda in international fora. A series of international meetings took place, all characterized by a strong emphasis on market-driven technological growth. The first of these was the G7 Conference on the Global Information Society, which played out in Brussels in February 1995. Here, ministers from the leading states in the Global North (France, Germany, Italy, Japan, the United Kingdom, the United States, and Canada) gathered alongside representatives from the largest information technology corporations.

The conference explicitly recognized the private sector as a key driver of the emerging Global Information Society, framing the event as an 'opportunity for the private sector to participate in G7 discussions, in full recognition of the important role it must play in the development of a global information society.'[26] Featuring ministerial discussions, technology showcases

---

[22] John Markoff, 'Building the Electronic Superhighway', *The New York Times*, 24 January 1993.

[23] Guy Lamolinara, 'Wired for the Future - President Clinton Signs Telecom Act at LC', Library of Congress, Libarary of Congress, 19 February 1996.

[24] Lamolinara.

[25] Kellner, *Technology and Democracy*, 17–18.

[26] European Commission, DG III, 'G7 Ministerial Conference on the Global Information Society: Round-Table Meeting of Business Leaders': (G7 Ministerial conference on the global information society, Brussels, 25 and 26 February 1995: Publications Office of the European Union, 1995), 5.

promising to 'improve our daily lives,' and a roundtable with business leaders, the event reinforced the prevailing belief that technological progress, steered by market forces, would deliver universal benefits. Beyond promoting a narrative of market-driven technological advancement as inherently positive, the conference also underscored the close alignment between states and the tech industry. By actively engaging with industry leaders to shape regulatory and policy frameworks, states positioned themselves as key facilitators of the market expansion on which capital is dependent. This dynamic reflected a broader trend in which governments sought to create favorable conditions for technological growth, ensuring that private sector innovations could scale globally.

In his opening remarks to the Conference, president of the European Commission Jacques Delors addressed the corporate representatives present at the conference with an attitude of outright admiration. Celebrating their impressive turnover and the significant employment opportunities they generated, he stated:

> We are here to listen to you … You are at the centre of the development of the information society: market evolution, all the initiatives that you and other companies have taken, launching new products for example, creating new forms of agreement, taking adventurous steps for the future with the multimedia in a combination of pictures, sound and written text.[27]

In praising tech corporations as the driving force behind the development of the 'information society' and promising to listen to their needs, Delors manifested the role of states as facilitators of the ideal conditions for capital accumulation in an emerging digital arena. By assuring the corporate representatives that any discussion of the role of states would focus on '*what you want them to do*',[28] he reaffirmed a strong alignment between state policy and the needs and interests of the tech industry. Delors's remarks thus expose intrinsic ties between states and the tech industry in this neoliberal era.[29]

A strong consensus prevailed at the G7 conference around the idea that free markets and rapid technological innovation were the primary engines of progress. Many participants framed the market not only as a driver of

[27] European Commission, DG III, 13.

[28] European Commission, DG III, 13. (my emphasis)

[29] See Clarke, 'Introduction', 3.

economic growth but also as a mechanism for addressing broader societal challenges. Within this perspective, deregulation was widely seen as essential to unlocking the full potential of the 'information society on a global scale. As one participant at the conference asserted:

> We should change all the rules that restrict the market and new demand. That should be done swiftly and worldwide. A fast worldwide deregulation of infrastructure is needed … to create the conditions enabling us to take advantage of the information society.[30]

Deregulation was widely deemed a necessity for achieving the full potential of the 'information society'; by dismantling regulatory barriers, governments could unleash the innovative and transformative power of the private sector, creating conditions for technological progress and, by extension, economic growth.

Even the issue of global inequality was conceived soluble within the broader vision of deregulation as a solution to societal challenges. Global inequality was thus primarily understood in terms of unequal *access* to technological products, reflecting the prevailing assumption that information technologies inherently foster progress. While inequality came to be reframed as unequal access to technology products, access was yet again frequently reframed as *demand* for technology products. This framing conveniently aligned with expectations that demand for technology products would make up the main driver of future European wealth.[31] The strategy for reducing inequality thus appeared closely tied to a strategy of wide geographic expansion of demand for technological goods and services – an approach that, while promoting accessibility, also facilitated the expansion of European tech corporations into new consumer markets. As one statement at the conference summarized, addressing inequality meant ensuring the 'lowest prices and the best services and the biggest choice of content, access to creative, innovative services and avoiding inequality by having prices that is accessible to everyone'.[32]

With representation solely from the tech industry, the 'public' was mainly thought of in terms of two roles: consumers and, to a lesser extent, workers.

---

[30] European Commission, DG III, 'G7 Ministerial Conference on the Global Information Society: Round-Table Meeting of Business Leaders':, 16.

[31] European Commission, DG III, 14.

[32] European Commission, DG III, 19.

Public needs were reduced to availability and affordability of products, centering on the importance of a greater selection of technology products at competitive prices. As Cory Doctorow observes, this perspective reduces people to consumers whose influence is primarily exercised through purchasing decisions rather than through political or collective action.[33] Consumers are 'ambulatory wallets' voting with their dollars to 'acquire life's comforts and necessities, without regard to the impact their production has on your neighborhood, your environment, your politics or your kids' futures.'[34] As a reflection of this Borkist conception of societal needs, *competition* was praised as the key mechanism for social and economic progress.[35] The dominant idea was that a liberalized market environment would foster innovation, flexibility, and responsiveness to consumer demand, ultimately benefiting society.[36] The conference report summary encapsulated this approach succinctly: Companies needed 'a liberalized environment which allows them to be flexible and innovative so that they can respond to competition and consumer demand. Market forces will ensure choice and low prices for customers.'[37] By linking the expansion of competition to addressing global inequality, the discussions effectively aligned social progress with the interests of the technology industry, positioning market forces as the primary solution to economic disparities.

The atmosphere of the G7 Conference reflects the prevailing attitude among the Global North states of the 1990s, which broadly embraced market liberalization as the key to addressing every societal need in the emerging 'information society'. This era of techno-optimism, as Douglas Kellner aptly describes, was characterized by the promise that the proclaimed 'information superhighway' would deliver more jobs, new economic opportunities, enhanced entertainment, and 'expanding prosperity in an info-topia that would make Adam Smith proud.'[38] The G7 conference illustrates how

---

[33] Doctorow, *The Internet Con*, 12.

[34] Doctorow, 12.

[35] For an illumination of how Robert Bork and the Chicago School shaped the discourse of the era, see Doctorow, 11–25. See also R.H. Bork and J.G. Sidak, 'What Does the Chicago School Teach about Internet Search and the Antritrust Treatment of Google?', *Journal of Competition Law and Economics* 8, no. 4 (2012): 663–700.

[36] European Commission, DG III, 'G7 Ministerial Conference on the Global Information Society: Round-Table Meeting of Business Leaders':, 19.

[37] European Commission, DG III, 6.

[38] Kellner, *Technology and Democracy*, 5.

this narrative was hyped and promoted by the powerful economic interests behind the emergent digital technologies while capitalist states were facilitating the best conditions for the tech industry.

The alignment between G7 states and the tech industry reveals how the advanced capitalist states leading the international agenda on the nascent 'information society' were working to ensure the best conditions for capitalism to sustain. As I argued in chapter two, capitalism is dependent on states for making the necessary investments and seeking out new revenues for capital, thus avoiding crises and stagnation.[39] We saw in chapter three how the basic components of the technological developments underlying the 'information society' had been developed by states, especially the United States, and then released to market forces tasked with the transformation of technologies into economic progress. Now, the task for states was to ensure adequate regulatory regimes that would allow tech corporations to expand their markets in an endeavor to sustain economic growth.[40]

The technophile promotion and celebration of the 'information society' throughout this neoliberal era of unambiguous market-optimism became pivotal in shaping the contemporary notion of cybersecurity when security-concerns recurred in international fora around the new millennium. Before delving into the recurrence and evolution of the contemporary notion of cybersecurity, let me first shed light on how the technophile discourses of the 1990s were operationalized in an extensive push for the global expansion of the 'information society.' As we will see, this expansion became synonymous with the expansion of capitalism itself.

DIGITALIZATION AS CIVILIZATION

The geographical epicenter of the process of building the 'information society' was unequivocally in the Global North, a reality reflected in the list of attendees at the G7 conference in Brussels mentioned above. Alongside representatives of the G7 states, the conference almost exclusively consisted of representatives from tech corporations located in the Global North. Within this framework, the expansion of technology markets in the Global South was framed as a key economic opportunity – particularly for the European Union. The conference rhetoric highlighted the importance of systems that would enable European 'brain power and … knowledge to circulate', thus

[39] Harvey, *The New Imperialism*, 2003, 150.

[40] Kellner, *Technology and Democracy*, 5.

directly linking the increase of digital technologies in the Global South to the strengthening of the European economy.[41] As one speaker put it, such developments would doubtlessly 'be the basis of wealth of the future.'[42] Implicit in this vision was an economic model that positioned the Global South primarily as a consumer market for technology products developed in the Global North. While discussions often highlighted the benefits of expanding digital access worldwide, they did so largely from the perspective of ensuring economic growth.

To compensate for the absence of representatives from the Global South in the G7 group, Thabo Mbeki, deputy President of South Africa who was recently elected in the first election after apartheid, had been invited to speak 'on behalf of the developing world.'[43] Mbeki emphasized how it was necessary to address the challenge of 'bringing the developing world on to the information superhighway'.[44] While his message stressed the importance of bridging the global digital divide, he also framed this challenge as an essential step in promoting global economic growth and development. The importance of bridging the digital divide thus appears mainly as a means to promote global economic growth, aligning his remarks with the dominant logic at the conference: the integration of the Global South into the information superhighway was mainly a tool for expanding markets for digital products.

However, recognizing the need for broader participation in shaping a Global Information Society, Mbeki urged the G7 group to convene a follow-up initiative that would include 'a cross-section of the developing world together with the G7 group and the European Union … to exchange views on such questions as strategy, finance and international coordination.'[45] The G7 welcomed this proposal. Consequently, a ministerial conference was held one year later in Midrand, South Africa, on 'the Information Society and Development (ISAD)'. The conference brought together

[41] European Commission, DG III, 'G7 Ministerial Conference on the Global Information Society: Round-Table Meeting of Business Leaders':, 14.
[42] European Commission, DG III, 14.
[43] Derrick L. Cogburn, 'Globalization and Governance in Cyberspace: Mapping the Processes of Emergent Regime Formation in Global Information and Communications Policy' (University of Michigan - School of Information, 2000), 8.
[44] European Commission, DG III, 'G7 Ministerial Conference on the Global Information Society: Round-Table Meeting of Business Leaders':, 90.
[45] European Commission, DG III, 93.

representatives from 40 states and 18 international organizations to focus on the 'specific needs of the developing countries'[46] and to 'consider how developing countries could be integrated into the emerging global information society'.[47] The conference thus marked – at least in principle – an effort to facilitate broader conversations about digital infrastructure.

The Midrand Conference holds particular significance, as its conclusions have been consistently recalled in subsequent United Nations General Assembly resolutions.[48] It has been recognized as a key moment in highlighting

---

[46] Commission of the European Communities, 'The Information Society and Development: The Role of the European Union - Communication from the Commission to the Council to the European Parliament to the Economic and Social Committee and to the Committee of the Regions', 15 July 1997, 3.

[47] Ian Taylor, 'Information Society and Development Conference' (House of Commons - Parliament of the United Kingdom, 12 June 1996).

[48] United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 57/53)', 22 November 2002; United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 59/61)', 3 December 2004; United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 61/54)', 6 December 2006; United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 62/17)', 5 December 2007; United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 63/37)', 2 December 2008; United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 64/25)', 2 December 2009; United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 65/41)', 8 December 2010; United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 66/24)', 2 December 2011; United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 67/27)', 3 December 2012; United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 68/243)', 27 December 2013; United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 69/28)', 2 December 2014; United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the

the need to include the Global South in international discussions on information technology. As we dive into the views and positions being expressed at the conference, they provide valuable insights into the intrinsic ties between the 'information society' and capitalism – and the endeavors to simultaneously expand both into the Global South in the 1990s.

The perhaps most striking aspect of the Midrand Conference is its largely unchanged continuation of the neoliberal approach of the G7 Conference the previous year.[49] Rather than marking any significant substantial departure, the conference thus reinforced the prevailing emphasis on a market-driven expansion of the 'information society', now framed under the goal of promoting development. From the Chair's conclusions of the Midrand conference, it appears:

> [There is] clearly an unsatisfactory level of investment in information infrastructure development in the less industrialised countries. Being able to mobilise the necessary investment, particularly from the private sector, is of paramount importance to the developing countries. Of equal importance is being able to develop networks which enable the whole of their populations to gain access to the global information infrastructure and participate in the [global information society] at affordable prices.[50]

This framing largely focused on investment mobilization, particularly from the private sector, as a means of expanding access to digital infrastructure. The general view seemed to be that the head start of the Global North in producing the technologies of the future presented a window of opportunity for the Global South; as the price of new information technologies continued to fall, the Global South could 'leapfrog' entire stages of traditional

---

Context of International Security (Res. 70/237)', 23 December 2015; United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 71/28)', 5 December 2016; United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 74/29)', 12 December 2019; United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 75/240)', 31 December 2020.

[49] Taylor, 'Information Society and Development Conference'.

[50] 'Information Society and the Developing World (ISAD) - Chair's Conclusions' (Midrand, South Africa: Gallagher Estate, 13 May 1996).

industrial development in setting up their own information infrastructures and applications.[51]

The realization of these advantages, however, was seen as contingent upon certain adjustments from the Global South governments. In particular, the establishment of the necessary digital infrastructures to unlock these opportunities required an 'affordable investment climate'.[52] Achieving such a climate would, for many states in the Global South, 'necessitate changes in the regulatory framework and economic restructuring aimed at a more liberalised telecommunications sector.'[53] As such, to mobilize and attract investment from the Global North, Global South states were encouraged to create a 'climate conductive to investment', including by introducing an 'adaptable regulatory framework based upon competition and aiming at the provision of more choice, higher quality and better access'.[54] This narrative positioned the adoption of a liberal regulatory regime as the essential path towards the benefits of the 'information society'. Such a regime included a focus on deregulation and market competition, alongside adequate protection of intellectual property rights. These conditions point to the expansion of the information society being not merely about technological access but just as much about integrating the Global South into a global capitalist system on terms set by the advanced capitalist states of the Global North.

The atmosphere tended to overlook the broader economic asymmetries arising from Global South economies being primarily positioned as markets for consumption and investment. It also glossed over the structural dependencies often arising from the establishment of dependencies on foreign investment, expertise, and infrastructure. Representatives from the Global South thus expressed concerns and critiques regarding the dominant market-driven approach advocated by the Global North. The diverging interests became evident as debates unfolded, with some Global South delegates pushing back against the emphasis on privatization, deregulation, and free-market competition as the primary solutions for expanding digital infrastructure. One particularly pointed intervention came from a South African delegate who took the podium to declare that 'this conference is not the

[51] 'ISAD (Midrand)'.

[52] 'ISAD (Midrand)', 26.

[53] 'ISAD (Midrand)'.

[54] 'ISAD (Midrand)'.

ISAD follow-up. That conference is yet to take place.'[55] Critiquing the one-sided focus on privatization, deregulation, free markets and competition, he underscored the importance of sovereign national governments to determine their own goals in the telecommunications sector to avoid 'information colonialism'. He called for a transformation of the internet from a *hobby of the rich to a tool for the masses*.[56]

At the initiative of Egypt, a follow-up conference was supposed to take place the following year, but it never materialized.[57] Perhaps tellingly, another actor entered the process to fill the void: The World Bank, which hosted a conference in Toronto, Canada, on Global Knowledge for Development in June 1997. This event marked a significant shift in the leadership of the global information society agenda, in which the finance-centered approach to information technologies became even more explicit. At the World Bank conference, Information technology was presented not only as a means to promote freedom of information but also as a catalyst for broader socio-economic transformation. Conference discussions linked digital expansion to a range of ambitious objectives, including gender equality, international peace, democracy, and poverty elimination. But the prevailing message was clear: A liberal regulatory framework in the image of the Global North was the only viable pathway to achieve these goals.[58]

The global expansion of digital infrastructure was thus intrinsically tied to the project of a broader global economic restructuring. Capitalist states of the Global North urged Global South governments to adapt to a neoliberal regulatory model of market competition and protection of property rights. Within this discourse, regulatory adjustments were framed as a necessary step toward modernization and economic growth. At the same time, Global South states were portrayed as lacking the financial and

---

[55] Cogburn, 'Globalization and Governance in Cyberspace: Mapping the Processes of Emergent Regime Formation in Global Information and Communications Policy', 10.

[56] Cogburn, 10.

[57] Cogburn, 10.

[58] For example, such views are expressed by President of the World Bank James D. Wolfensohn and Senior Vice President and Chief Economist of the world bank Joseph E. Stiglitz in 'Summary Report from Global Knowledge 97: Knowledge for Development in the Information Age' (The International Institute for Sustainable Development (IISD), 22 June 1997), https://wgbis.ces.iisc.ac.in/envis/doc97html/infogkd630.html.

technological capacity to independently shape their own digital futures. An implicit assumption thus persisted that the Global South faced inherent challenges in administrative and economic governance compared to the Global North. This notion was evident in the discourse of the European Union. In a post-conference evaluation report, the European Union emphasized that attracting private investment in the Global South would require the establishment of a 'stable, predictable, and transparent' legislative and regulatory framework, one that would allow for 'rational economic decisions.'[59] This emphasis on rationality implied that existing regulatory structures in the Global South were irrational, and that adaptation to European regulatory models was thus necessary to attract the rational investors of the Global North. The idea of the global 'information society' being inevitable and universally beneficial not only depoliticized debates about digital expansion but established also a singular trajectory of technological progress – one set forth by advanced capitalist states in the Global North. In this framing, the adoption of liberal regulatory frameworks was presented as the only viable path forward for the Global South. The global expansion of the 'information society' was thus closely connected to the expansion of capitalism itself.

Today, the level of information technology development has in itself become a benchmark of evaluation. Various global indexes assess governments' readiness to implement emerging technologies, particularly in the field of artificial intelligence. Among them, the Government AI Readiness Index is the most prominent.[60] This index ranks national governments based on their ability to integrate artificial intelligence into public service delivery, with the explicit goal of helping governments across the globe to benchmark their effective governance of artificial intelligence, providing a means for 'officials [to] keep up with global developments and learn ... what their peers are working on'.[61] As Holden and Harsh observe, the index is framed by celebratory discourses about the socially transformative power of artificial

[59] Commission of the European Communities, 'The Information Society and Development: The Role of the European Union - Communication from the Commission to the Council to the European Parliament to the Economic and Social Committee and to the Committee of the Regions', 7.

[60] Kerry Holden and Matthew Harsh, 'On Pipelines, Readiness and Annotative Labour: Political Geographies of AI and Data Infrastructures in Africa', *Political Geography* 113 (2024): 6.

[61] Holden and Harsh, 6.

intelligence.[62] A determinist language portrays artificial intelligence as an autonomous, self-referential technology that will have ripple effects when it finally impacts society.[63] Meanwhile, Global South Governments everywhere are positioned as 'lagging behind the technology and needing to catch up to optimise the social goods of AI'.[64] A similar discourse is seen in the frequent appraisal of investments of the tech industry for generously attempting to lift Global South regions out of their disconnected desolation. Google's privately owned Equiano fiber-optic pipeline, which reached the coast of Nigeria in April 2022, connecting to the Lagos Open Access Data Centre, is being promoted as a transformative development for data infrastructure, promising to bolster the Economic Community of West African States (ECOWAS) and drive modernization in the region.[65] In that sense, we might say that if capitalism has historically been key to the recognition as a sovereign state (a point to which we will return in chapter six) then digitalization is an increasingly key parameter for the recognition as a capitalist state.[66]

CYBER AS *SECURITY*

As we have now seen, discussions of the security-aspects of information technologies had been on hold from 1991 and until the end of the 1990s, in which the focus was mainly on the expansion of the 'information society' into new territories. In a sense, a twofold process of expansion took place in this early era of the 'information society': A geographical expansion and an expanding commodification. So far, we have seen how a geographical expansion of digital infrastructure was unfolding, with digital infrastructure being increasingly built into every corner of the world – satisfying capital's strive to tear down every spatial barrier.[67] Quoting Renata Ávila Pinto, 'the world's offline populations are the disputed territory of tech empires, because whoever gets them locked into their digital feudalism, holds the key to the future.'[68] Tech corporations continuously engaged in races to 'connect

[62] Holden and Harsh, 5–7.
[63] Holden and Harsh, 5–7.
[64] Holden and Harsh, 6.
[65] Holden and Harsh, 4.
[66] Tzouvala, *Capitalism As Civilisation*.
[67] Marx, *Grundrisse*, 524.
[68] Pinto, 'Digital Sovereignty or Digital Colonialism?', 17. Notably, the notion of techno-feudalism remains disputed. For an elucidation of the position, see Cédric

the disconnected', expanding their digital empires and thus also expanding their terrain for accumulation.[69]

But the geographical expansion was soon accompanied by an increasingly expanding commodification of digital life. Throughout the 1990s, cyberspace was still widely considered a form of 'public space'. Corporations had only recently taken over the (publicly funded) infrastructure of the internet, and now they could make profit from selling access to it. As Gavin Mueller describes, the internet of this period remained largely noncommercial, characterized by user-driven content and open platforms:

> [The internet was] a province of amateurs and hobbyists. Firms generated revenue from providing access to the internet, but once there, user behavior ran free through what were mostly noncommercial spaces: unofficial fan webpages, lightly regulated forums, troves of freely available games and software.[70]

While the establishment and expansion of the basic architecture underlying global connectivity and the markets for technological products had been at the core of the commercial adventures described above, the internet itself was mostly a noncommercial space. However, as has always been the case with public space under capitalism, it thereby also represented a terrain open for appropriation – a terrain which every settler could turn 'into his private property and his individual means of production'.[71] Paraphrasing the discourse of improvement deployed in the early days of capitalism to justify the enclosures of 'wasteland', a process of 'cultivation' of cyberspace took place throughout the 1990s and 2000s.[72] As we saw in chapter three, the late 1990s witnessed a rapid growth internet-based companies. With the the burst of the dotcom bubble in 2000 and the launch of the 'web 2.0', websites changed their business strategies towards more interactivity, giving

---

Durand, *How Silicon Valley Unleashed Techno-Feudalism: The Making of the Digital Economy* (London & New York: Verso, 2024).

[69] Pinto, 'Digital Sovereignty or Digital Colonialism?', 17.

[70] Mueller, *Breaking Things at Work*, 108.

[71] Marx, *Capital: A Critique of Political Economy. Volume One*, 934.

[72] Neocleous, 'International Law as Primitive Accumulation; Or, the Secret of Systematic Colonization', 953; Jessie M. Hohmann and Christine Schwöbel-Patel, 'A Monument to E. G. Wakefield: New and Historical Materialist Dialogues for a Posthuman International Law', in *International Law and Posthuman Theory*, ed. Mathilda Arvidsson and Emily Jones, 2023, 152.

rise to the emergent data economy, in which new digital methods of value extraction accelerated.[73] Ever-more aspects of economic life became dependent on digital technologies. This expanding commodification of cyberspace gradually led to widespread dependencies on stable and reliable digital infrastructure, resulting in an emerging awareness of the economy's vulnerability to their disruption.

As digital networks became increasingly central to global commerce – and, by extension, to national economies, concerns began to emerge over their potential vulnerabilities. From 1998 and onwards, developments in the field of information and telecommunications in the context of international security recurred as a theme within the United Nations and became permanently included on the General Assembly agenda. Following up on the 1990 General Assembly resolution's appraisal of progress in science and technology for civilian applications, the 1998 resolution of the General Assembly states that 'considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication'. This framing thus continued the appraisal of global digital infrastructure as an unequivocal global goal.[74] The General Assembly further recalled the 'approaches and principles' outlined at the Midrand conference, thus reinforcing a policy paradigm of worldwide competition, private investment, and deregulation as central to the global expansion of the 'information society.' By incorporating these conclusions into a resolution on international security, the General Assembly effectively extended the neoliberal discourse of the 1990s into the emerging domain of *cybersecurity*.

In this recurrence of security on the agenda, the appreciation of civilian technology infrastructure came to assume an even more defining role in this recurring notion of cybersecurity. The shift reveals itself as an assumption that the stability and functionality of information technology systems is a universal public interest. The preambular paragraphs of the resolution thus set the stage through a reiteration of the importance of progress in technological developments:

> [The General Assembly] sees in [the process of developing and applying the latest information technologies and means of

[73] Mueller, *Breaking Things at Work*, 108.

[74] United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 53/70)', 4 December 1998.

> telecommunication] the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of humankind and additional improvements in the circulation of information in the global community.[75]

This perspective positions progress in digital technology as an essential pillar of international development, framing their development and application as a means to advance civilization, foster international cooperation, and enhance global information exchange. The General Assembly notes how the 'dissemination and use' of information technologies affect a set of universal interests, which is enhanced by broad international cooperation.[76] The preambular paragraphs of the resolution thus establish how the stability of information technologies is a universal goal, underscoring the role of the state-system in facilitating this stability.

Unlike the 1991 General Assembly resolution, which distinguished between military and civilian technology and limited discussions of security to the military technology use, this later resolution integrated civilian technological infrastructure into security considerations. As a result, cybersecurity came to be understood not only in terms of military technology use but also as the protection of digital systems that underpin economic and social functions. The reframing of stability in information technologies as an object of protection is symptomatic of the new concept of cybersecurity, as the concept took shape in the operative paragraphs of the resolution.

Security concerns were now seen to arise from the use of these technologies for purposes that were 'inconsistent with the objectives of maintaining international stability and security', and which may 'adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields'.[77] In this framing, the main security concern arose from use of technology that caused the disruption and destabilization of digital systems of any kind. In other words, the stability and reliability of information technologies had become the *object of protection*. The concept of cybersecurity had thus been altered, aligning with the economic and

---

[75] United Nations General Assembly.

[76] United Nations General Assembly.

[77] United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 58/32)' (United Nations, 8 December 2003).

technological developments of the preceding decade – a shift that coincided with the growing reliance on digital infrastructure for economic growth.

It is well-known that security became a buzzword in the 2000s following September 11, 2001, which led the United States to declare a 'new national emergency' three days later.[78] These events further prompted discussions of the security aspects of computers and information technology, particularly with regard to questions of digital infrastructure protection, electronic surveillance, the terrorist use of hacking, and the internet as a networked platform for communication across and against states.[79] The primary threats were perceived to arise from individuals and non-state groups, rather than states. Within the still dominant Fukuyaman narrative of an inevitable global expansion of liberal democracy, the key challenge was seen to arise from individual actors who resisted or sought to undermine this vision through disruptive digital activities. As a result, the discourse on cybersecurity was largely framed around preventing these threats from hackers, extremist groups, and cybercriminals.

In an effort to elaborate on the 'existing and potential threats in the sphere of information security', a Group of Governmental Experts (GGE) in the Field of Information and Telecommunications in the Context of International Security was appointed in a resolution of the General Assembly in 2004. However, it took some years before substantive conclusions were reached by the GGE. In its first substantial report, published in 2010, the GGE noted:

> [T]hreats may cause substantial damage to economies and national and international security. Threats emanate from a wide variety of sources, and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike. Their effects carry significant risk for public safety, the security of nations and the stability of the globally linked international community as a whole.[80]

---

[78] Neocleous, *Critique of Security*, 76.

[79] Hansen and Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', 1155–56.

[80] Group of Governmental Experts, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (United Nations, 30 July 2010), 6.

The GGE report thus reinforced the idea that the disruption of information technology systems makes a security risk. The assumption is further reflected in the notion that 'the same ICTs that support robust e-commerce can also be used to threaten international peace and national security.'[81] In this framing, global trade becomes symptomatic of the status quo worthy of protection. In turn, the GGE expresses an increasing concern for individuals, groups or organizations, including criminal organizations' engaging in 'disruptive online activities'.[82] The bad actors - those who pose a security threat – are per definition individuals and groups external to information technology systems, threatening their stability.

To summarize, the expansion of the 'information society' into new industries and geographical corners entailed profound dependencies on stable and reliable digital infrastructures. With these dependencies came new vulnerabilities – including risks of financial theft by hackers, the anxieties of intellectual property owners over file sharing diminishing their rights and profits, and the risks posed by software vulnerabilities and computer viruses, posing a latent threat of digital disruption.[83] In response to these vulnerabilities, cybersecurity evolved as a concept centered on maintaining the stability and reliability of digital infrastructures. As the economy of capitalist states depend on sustained growth, the private-economic risks of those in control of information technology systems have been translated into universal security concerns, which capitalist states sought to address in their international relations.[84] The concept of cybersecurity took form around the necessity of the capitalist state to protect the reliability of digital infrastructures. Threats were framed as, by definition, *external* to the technological systems which, in this era, was perceived to arise from cyber criminals and groups hostile to Western liberalism.

SECURITY FOR WHOM?

Capitalist states have generally played a key role in facilitating the technological developments on which contemporary global capitalism relies through both financial and technological support. But more than that, the

[81] Group of Governmental Experts, 6.

[82] Group of Governmental Experts, 7.

[83] Hansen and Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', 1161.

[84] Hansen and Nissenbaum, 1161.

neoliberal era of the 1990s witnessed Global North states pushing extensively for the global expansion of the 'information superhighway' through the establishment of the ideal legal and economic conditions in the Global South. The horizontal relation between capitalists marked by competitive struggle entails a constant drive for developing and deploying new technological tools to lower production costs and seek out new spaces for capitalist accumulation. The corporate interest in expanding the 'information society' into new geographical terrains illustrates this mechanism. However, these spaces were never just readily available. Regulatory and economic frameworks of Global South states had to be harmonized with the frameworks of advanced capitalist states. This process of harmonization involved the imposition of a neoliberal paradigm that emphasized privatization, deregulation, and the protection of intellectual property rights, reshaping the Global South in the image of the Global North. This process elucidates how the expansion of the 'information society' went hand in hand with the expansion of capitalism itself. This process was key to avoiding economic stagnation, as it opened up new territories to accumulation, satisfying capitalism's need of economic growth.

As security in relation to information technologies recurred as a theme in the beginning of the current millennium and materialized in the notion of 'cybersecurity', the concept took shape around the neoliberal techno-determinism of the 1990s. The debate was thus centered on ensuring stability and reliability in global information technology infrastructures against disruptions and intrusions from individuals and non-state groups. The dominant concept of cybersecurity reflects how the state-system seeks to establish stable and reliable conditions for capital as flows of commodities and money are becoming increasingly global. The 'information superhighway' is symptomatic of how the state-system not only seeks to establish new terrain for capital accumulation, but also to provide the stability and predictability needed for the social relations of capitalism to function along these newly established global digital routes.

The notion of security signals *exceptionality*.[85] Any social antagonisms and conflicting interests surrounding technological designs appear irrelevant to a security assessment. However, when security is seen as politics, as it should be, then the very notion of security becomes ambiguous: what kind of security? Security for whom? Security for what? As we unpack how the concept

[85] Buzan, Wæver, and Wilde, *Security*, 21.

of cybersecurity has developed, it becomes evident that the notion of (cyber)security does not simply represent a reaction to objective conditions; it is, following Krause and Williams, 'built on a series of political and epistemological choices that define what is considered security.'[86] My aim in this chapter has been to elucidate how the contemporary notion of cybersecurity has been constructed, showing how it mirrors the role of the state-system in the reproduction of the social relations of capitalism. My analysis has shown that the notion of cybersecurity relies on a market-focused celebration of technological expansion, suggesting that the stability and reliability of information technology systems makes the object of protection. Meanwhile, any external intrusion into these systems is framed as a universal cybersecurity threat. My analysis thus challenges the assumption of universality underlying mainstream scholarship and unravels the depoliticizing effect of the exceptionality that accompanies dominant notions of cybersecurity.

A counterargument to my claim might suggest that while information technologies indeed introduce vulnerabilities for capital, they also introduce vulnerabilities for everyone else. As the world has become increasingly digitalized, the stability and reliability of digital infrastructure is a shared concern across society. From this perspective, protecting information technologies is not just about maintaining stability for capital – it is about ensuring the functionality of essential systems on which everyone depends. However, such an argument presupposes that the interests of capital and the interests of the working class are indistinguishable – that the protection of capital is synonymous with the protection of society. This presupposition is deeply flawed. As we saw in chapter three, the digital landscape has emerged as a result and expression of inherently conflictual social relations. Certainly, disruptions in information technologies can be immediately frustrating not only for those who own and control these systems but also for individuals who have come to rely on them in their daily lives. Yet, for the latter group, this frustration does not amount to a shared interest in the system's continued stability. Rather, it should be interpreted as an expression of the powerlessness following from their complete dependence on vast corporate entities that control and profit from ever more aspects of life through digital technologies.

To take a concrete example, let us return to the infamous 2007 cyberattacks on Estonia, mentioned in the introduction to this chapter. Among the

[86] Krause and Williams, 'Broadening the Agenda of Security Studies', 234.

most frequently emphasized consequences was the temporary shutdown of online banking services – a disruption that was widely portrayed as an elucidation of the importance of cybersecurity. There is no doubt that such an outage was frustrating for customers who depend on their banks for daily transactions. However, this frustration should be understood in the broader context of how digital technology has facilitated an unprecedented acceleration in the wealth accumulation of the financial sector. As we saw in chapter three, algorithmic and high-speed trading have mechanized and accelerated the speed of speculation in financial markets, exponentially increasing the scale of financial transactions. These developments, enabled by the digital transformation of the financial sector, have made financial elites immensely rich, in turn intensifying economic inequality. To financial institutions, the threat of disruptions in their digital infrastructure threatens the very foundation of their wealth. For most customers, however, the bank is symptomatic of a system that has exacerbated economic disparities. Suggesting that bank and customers alike have a shared, universal interest in protecting these digital systems is only a coherent argument if we ignore the material realities of the economy underlying the information technology landscape. Once we root the digital landscape in the social relations out of which it has emerged, its inherently political nature becomes clear.

In this chapter, I have shown how the notion of cybersecurity has been shaped around the evolving needs of capital throughout the development of digital technologies. In the initial years, digital technologies were key to an economic expansion that should prevent capitalist economies of the Global North from crises and stagnation. With the success of the global expansion of the 'information society', the capitalist economy became increasingly dependent on the stability of digital infrastructures. Risks of destruction, disruptions, and theft of digital content materialized as vulnerabilities to capital as such. In response to these vulnerabilities, a revised notion of cybersecurity was centered on the protection of digital infrastructures against external intrusions which, at this time, was mainly seen to stem from cyber criminals and non-state groups hostile to Western liberalism. In the following chapter, I turn to examine the emergence of international legal discourse in the context of information technologies. As we will see, the legal discussions inherited the rationalities of cybersecurity, which became defining for the contours of the field of international cyber law.

CHAPTER V
THE BIRTH OF INTERNATIONAL LAW

Framing particular concerns in the language of international law is a powerful way of making them appear both natural and unquestionable. As we saw in chapter two, international law masks relations between states as rules, which come to appear natural and uncontestable. In that light, it is perhaps surprising that international legal discourse did not migrate decisively into the international discussions of information technology sooner than it did. It remained contested whether cyberspace was a lawless domain until around the early 2010s, when consensus gradually began to crystallize that international law applies to cyberspace. This shift redirected the focus of positivist legal scholars from *whether* international law applies in cyberspace toward questions of *how* international law applies.

This chapter explores the gradual shift from an era of *terra nullius* to the current era of widespread recognition that cyberspace is subject to existing rules of international law. Starting from the techno-optimist era of the 1990s elucidated in chapter four, the chapter traces the intellectual and political debates through which this transformation took shape. The chapter thus illuminates how competing visions of cyberspace as either an exceptional, unprecedented domain beyond the scope of existing law (*cyber exceptionalism*), or as a set of new technologies subject to extant regulation (*cyber non-exceptionalism*) have evolved since the techno-optimist era, eventually bringing cyberspace into the realm of international legal discourse. Against this backdrop, the chapter roots the birth of the field of international cyber law in the

social relations between states and their roles in the reproduction of capitalism.

My central claim is that the field of international cyber law emerged in response to the increasing vulnerability of digital infrastructure combined with a declining faith in the proximate universalization of Western liberalism. As the reproduction of capitalism increasingly demanded stability in the digital infrastructure on which global capital accumulation relies, capitalist states sought to increasingly establish adequate protection through international legal discourse. As examined in chapter four, the notion of cybersecurity had already been shaped by the drive to protect digital infrastructures from external intrusions. This same logic migrated into legal discourse. While the birth of international cyber law is neither natural nor inevitable, a determinate legal discourse is depoliticizing the digital landscape by making the protection thereof seem raised above particular interests and concerns. International cyber law thereby serves to reinforce global hierarchies and economic dependencies emerging in the digital era.

Terra Nullius

While the link between international law and information technology appears obvious today, it was far from obvious in the early days of the internet of the 1990s. Then, the internet was widely celebrated as a borderless, decentralized domain. Many early internet users envisioned cyberspace as a world beyond the reach of state authority, in which freedom of thought and expression could flourish without hierarchical control. Optimism thus existed amongst the curious, technically skilled individuals constituting the hacking community that cyberspace – a term that they imported from science fiction – would be an essentially democratic domain in which freedom of thought and expression were the constitutional pillars, with a flat structure with no hierarchical governance.[1] In his famous Declaration of Independence of Cyberspace, John Perry Barlow professed:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of

[1] See Gabriella Coleman, 'From Internet Farming to Weapons of the Geek', *Current Anthropology* 58, no. S15 (2017): S91–102; Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (London & New York: Verso, 2015).

> the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.[2]

Barlow envisioned a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth. He saw in cyberspace a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity, and a world where legal concepts of property, expression, identity, movement, and context do not apply.[3] In a spirit accurately captured in Barlow's declaration, the early internet culture was characterized by a libertarian individualism that generally perceived governments as the main threat to the realization of some relatively undertheorized goal of 'internet freedom'.[4]

The 'cyberspace' metaphor, which gives a sense of a virtual 'space' arising from information technologies, did not only prevail in virtual subcultural communities and movements. It gained a broad, popular appeal and would soon be part of mainstream language and deployed on a political level – as well as in legal academia. On the high political level, the cyber exceptionalism prevailed in a purely neoliberal variant. In the United States, the famously technophile Bill Clinton and Al Gore Administration's 1996 Framework for Global Electronic Commerce manifests this spirit, celebrating the internet for its decentralized nature and its tradition of bottom-up governance.[5] The framework suggested that governments should 'establish a predictable and simple legal environment based on a decentralized, contractual model of law rather than one based on top-down regulation.'[6] Underlying this approach is an assumption that absent the establishment of specific rules that regulate conduct in this domain, no rules apply. The context of the expression is national law rather than international law (the case for much of the early writings on cyberspace and law), but the underlying idea is more

---

[2] John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (Electronic Frontier Foundation, 1996).

[3] Barlow.

[4] Coleman, 'From Internet Farming to Weapons of the Geek', 93; Garry Potter, 'Anonymous: A Political Ontology of Hope', *Theory in Action*, 2015.

[5] The United States, '1997 Framework for Global Electronic Commerce', 1 July 1997; Mueller, 'Against Sovereignty in Cyberspace', 781.

[6] The United States, '1997 Framework for Global Electronic Commerce'; Mueller, 'Against Sovereignty in Cyberspace', 781.

general: As a matter of *lex lata*, cyberspace is fundamentally distinct from 'real space' and therefore exempted extant regulation, and as a matter of *lex ferenda*, we should keep the regulation at a minimum. The same spirit characterized international discussions of the 'information society'. The cyber-exceptionalism should be understood in the context of the market-focused technophilia characterizing the attitudes of many governments of the Global North throughout the 1990s. As we saw in chapter four, a prominent view prevailed in this era that the role of states was to facilitate the best conditions for market forces to do their magic in the development of the digital landscape. States should refrain from any unnecessary regulatory intervention that could burden or restrain these creative forces.

The concept of a borderless domain, reachable across geographic boundaries, quickly became a hot topic within legal academia. A wave of scholarship defended the 'exceptionalist' view that existing legal frameworks were not apt to regulate the new reality of cyberspace because of its profoundly different characteristics. Consequently, new rules would have to be negotiated if cyberspace were not to remain an anarchy.

The most prominent intellectual defense of such cyber exceptionalism was advanced by David Johnson and David Post, who were both associated with the Electronic Frontier Foundation – an organization advocating the freedom of the internet and other technologies from government regulation. Johnson and Post asserted that cyberspace requires rules distinct from those governing physical, geographically defined territories. Their central argument was that laws generally had to consider the characteristics of the space it regulates. Existing laws governing the 'physical' world had not considered the profoundly different features of cyberspace, including the emergence of persons only existing in virtual form and the emergence of new types of property, which would differ from real-world real estate or tangible objects.[7] Such questions of property and personality were intrinsically connected to law-making activity:

> [A]ccommodating conflicting claims, defining property rights, establishing rules to guide conduct, enforcing those rules, and resolving disputes – remain very much alive within the newly defined, intangible territory of Cyberspace.[8]

[7] Johnson and Post, 'Law and Borders - the Rise of Law in Cyberspace', 1401.
[8] Johnson and Post, 1402.

New rules would have to emerge 'separate from doctrine tied to territorial jurisdictions, … to govern a wide range of new phenomena that have no clear parallel in the nonvirtual world.'[9] Yet, a new set of jurisdictional challenges arose from this task. National laws struggled to govern a borderless digital world, leading to conflicts and uncertainties. Johnson and Post therefore advocated for self-regulation within cyberspace, relying on community standards and technical solutions. They called for a decentralized legal system tailored to the unique characteristics and dynamics of cyberspace.

Taking stock of Johnson and Post's claim, another commentator urged for the development of a long-term, international solution in the form of a treaty 'dealing strictly with Cyberspace', governing 'intellectual property issues as well as all other Internet-specific legal issues'.[10] The treaty should define cyberspace as its own jurisdiction and create an international court system with subject matter jurisdiction over cyberspace, thereby resolving the jurisdictional dilemma identified by Johnson and Post.[11] A similar argument was advanced by another commentator that the internet required its own legal institutions.[12] Arguing that the internet had its own culture, characterized by a mistrust for traditional geographically bounded legal and political institutions, the internet challenged traditional notions of sovereignty.[13] Unlike sovereign states tied to geographic boundaries, the Internet was perceived as 'inherently global and indifferent to geographic political boundaries'.[14] Accordingly, the 'evolution of the Internet as a set of virtual legal institutions, as a market, and as a political entity, has enormous implications for the evolution of international law.'[15] Due to its borderless nature, the internet was so profoundly different from the physical world that existing international law was meaningless; it called for the establishment of its own international legal institutions.

Another wave of scholarship contested the exceptionalism advanced by Johnson and Post and their supporters. Emphasizing instead the *non-exceptionality* of cyberspace, these scholars argued that the adoption of new rules and the establishment of new legal institutions was unnecessary.

---

[9] Johnson and Post, 1367.

[10] McGregor, 'Law on a Boundless Frontier', 970.

[11] McGregor, 970.

[12] Perritt, 'Cyberspace and State Sovereignty'.

[13] Perritt, 162.

[14] Perritt, 162.

[15] Perritt, 162.

International law would adapt to new situations and new types of technology. An example of this position is an early contribution by Schmitt addressing the question of the law of warfare (*jus ad bellum* and *jus in bello*) and information technology. As the perhaps single most influential scholar to shape the field of international cyber law since then, there is reason to pay attention to Schmitt's early contributions on the matter. While Schmitt took no explicit position on the question of cyber exceptionality, he deployed a discourse that presupposed non-exceptionality, approaching information technologies as a set of tools, rather than as a distinct, non-territorial space. Recognizing the evolving nature of international law and the 'uncertainty of the future', Schmitt sought to predict the legal evolution based on which interpretation better promoted a particular path of development dictated by the needs and interests of the United States (a maneuver that we recognized in chapter one as *apology*). He reasoned the focus on the United States with the contention that the American vision was 'developmentally mature' and would 'likely exhibit determinative influence over warfare's evolution for the foreseeable future' given its 'significant influence over how even combined operations are executed'.[16] While the latter point may well be descriptively accurate, the former point comes to unravel the unapologetically hegemonic attitude underlying his argument: Not only *will* the United States determine the direction of international law because of its superiority in power, but normatively, the United States *should* determine the law because of its developmental superiority. Information operations would, he predicted, raise serious questions about what constitutes force. As we saw in chapter one, economic damage had historically been kept out of discussions of force, because economic sanctions were important tools of power for advanced capitalist states like the United States. But Schmitt asserted that current notions of lawful behavior in this regard 'are likely to evolve' in light of the risk of hacking attacks on banks, communications networks, or stock exchanges.[17]

Another non-exceptionalist – Anthony D'Amato – argued that the internet had become 'one of our vital national interests'.[18] An absolute prohibition of internet disruption was accordingly 'in the best interests of both sides in the long run and therefore is likely to be soon recognized as a foundational

[16] Michael Schmitt, 'Bellum Americanum: The U.S. View of Twenty-First Century War and Its Possible Implications for the Law of Armed Conflict', *Michigan Journal of International Law* 19, no. 4 (1998): 1053.

[17] Schmitt, 1072.

[18] D'Amato, 'International Law, Cybernetics, and Cyberspace', 69.

principle of international customary law.'[19] His analysis reflects a realist view of international law being a result of the strategic interests of states.

The scholarly debates between the cyber exceptionalists and the cyber non-exceptionalists continued during the first decade of the current millennium. As late as in 2010, a commentator concluded that existing rules of *jus ad bellum* had a limited reach in the digital realm and suggested that a multilateral cyberwarfare treaty should be adopted 'to regulate this method of warfare and its consequences.'[20] Another commentator argued that information warfare's unique nature raised special challenges to the existing legal framework governing warfare, and that its 'varied forms and outcomes pose particularly significant problems for attempts to expand the current law to include [information warfare]'.[21]

Concurrently with these early academic debates, states were generally silent on the question of international law and cyberspace. While we saw in chapter four how information technologies and, increasingly, cybersecurity were prominent themes in international fora, the question of international law remained untouched. In none of the 15 resolutions adopted by the General Assembly on Developments in the field of information and telecommunications in the context of international security in the period from 1998-2012 was there any mention of international law, nor of law more broadly. As mentioned in chapter four, the GGE, established pursuant to a United Nations General Assembly resolution in 2004, published a report in 2010. The Secretary-General held in the foreword to the report that 'we have only begun to develop the norms, laws and modes of cooperation needed for this new information environment.'[22] This notion reflects the view that the new information environment required the development of new law, and thus, that 'existing law' did not apply. The substantial report of the GGE contained no mention of international law nor law more generally. An assumption that cyberspace was a lawless space can thus arguably be deduced from the absence of legal discourse in the international debates. As such, no generally accepted assumption existed in the 1990 and 2000s that cyberspace

[19] D'Amato, 68–69.

[20] Rex Hughes, 'A Treaty for Cyberspace', *International Affairs* 86, no. 2 (2010): 523–41.

[21] Jon P. Jurich, 'Cyberwar and Customary International Law: The Potential of a "Bottom-up" Approach to an International Law of Information Operations Developments', *Chicago Journal of International Law* 9, no. 1 (2009): 284.

[22] Group of Governmental Experts, 'A/65/201', 4.

was regulated by international law. In international fora, the common idea appears to have been that international law did not apply to this new domain. In other words, if cyberspace were not to remain a *terra nullius* – a lawless space – new international law would have to be negotiated.

Taming the Wilderness

As we saw in chapter two, capitalist states generally seek to avoid economic stagnation by maintaining capitalism's constant geographical expansion, thus opening up demand for both investment goods and consumer goods in non-capitalist territories.[23] By seeking out new terrains for capital and facilitating capital's seamless flows, capitalist states can satisfy capital's expansive impulse and sustain economic growth. In this era of cyber exceptionalism, cyberspace was widely conceived as a domain free of the spatial barriers restraining the 'physical world'. In a sense, John Perry Barlow's message to the Governments of the Industrial World had thus been well received – at least for a while. But the absence of governmental control did not leave this new domain free from market forces. On the contrary, this borderless domain represented a terrain into which capital could continue its expansion in a historical era in which the global capitalist economy had already absorbed most of the 'physical world'. Cyberspace was perceived as a rapidly expanding no-man's-land – a 'wild west' open for cultivation. In this era, the *absence* of international legal regulation thus gave way for the rapid, unrestricted development of expansive digital markets. The cyber exceptionalist view supported the narrative of the information society as inherently separate from the conflicts, power struggles, and barriers of various kinds that were shaping the 'physical' world, thus aligning with the vision that we explored in chapter four of the expanding 'information society' as an inherently apolitical development raised above contestation.

We saw in chapter four how a twofold expansion of the information society of this era – not only a geographical expansion but also a gradually expanding commodification of digital space – led to an emerging awareness of digital vulnerabilities from around the new millennium, and how this moment coincided with the declared 'war on terror', leading to discussions of *cybersecurity* around the new millennium. We also saw in chapter four how an idea still prevailed that world was moving toward a universalization of Western liberalism – and thus, toward a universal system of reliable capitalist

[23] Harvey, *The New Imperialism*, 2003, 139.

states. While the discourse in international fora remained cyber exceptionalist in this era of the early 2000s, a regional legal framework was developed in Europe with the active engagement and support of the United States, Canada, and Japan: The Budapest Convention on Cybercrime, which was first signed in 2001 and came into force in 2004. The convention aimed at combatting cybercrime by requiring states to create and strengthen their domestic laws and criminalize interference with digital property relations, reflecting a growing recognition of capital's need for a legal framework in the digital era. By addressing the security threat arising from non-state actors who were increasingly deemed a threat to the reliable functioning of the digital infrastructure on which national economies had become gradually more reliant, European states sought to consolidate the role of the state-system in protecting the social relations of capitalism.

At the outset, the Budapest Convention appears as an exception to the general idea of its time that cyberspace was an inherently free, lawless domain. However, this would be a misunderstanding. In fact, the Budapest Convention was quite symptomatic of the spirit of its time of its adoption in two vital ways. *First,* it perceived non-state groups as the central threat to the 'legitimate interests in the use and development of information technologies'. Considering the intricate ties between digital development and the global expansion of capitalism, the convention can thus be understood as an effort to protect global capitalism against 'cyber criminals' threatening the stability of property relations increasingly contingent on digital technology. Throughout this time, none-state groups were perceived as the central threat to Western liberalism. As we saw in chapter four, this era was marked by a Fukuyaman narrative of an inevitable global expansion of liberal democracy, and the key challenge was seen to arise from individual actors who resisted or sought to undermine this vision through disruptive digital activities. *Second*, its drafting was completed in Europe and only subsequently sought expanded to the rest of the world to guarantee a universal adherence to the European standards for facilitating and safeguarding the twofold expansion of cyberspace. The project thus resembled the broader idea of the time that non-state groups hostile to the West and its institutions were deemed a security threat, while states were required to adhere to an

economic and regulatory standard set by the Global North to keep these malicious non-state actors under control.[24]

Meanwhile, international legal discourse remained absent in global international fora much longer. Despite the adoption of the Budapest Convention on cybercrime, an exceptionalist narrative thus prevailed in terms of the general applicability of international law in cyberspace. However, the cyber-exceptionalism would not last indefinitely. While the boundless expansion of the geography of cyberspace was facilitated and enabled by the exceptionalist discourse, the expanding commodification that followed soon began to create vulnerabilities that states could not ignore. What is more, it gradually became clearer that these threats did not merely arise from singular instances of non-state cyber criminality.

Harold Koh and Beyond

The uncertainties surrounding the international legal status of cyberspace was soon to change profoundly. The 2007 Estonia cyberattack mentioned in chapter four was interpreted by many Western powers as raising pressing questions regarding the threat of 'cyber war' and, with it, the applicability of international laws and norms related to war.[25] In response, analysts linked to the military, intelligence agencies, and national security policy institutes began to increasingly draw on conventional international law concepts, most notably that of sovereignty.[26] The concerns and rationalities shaping the notion of cybersecurity, as we saw in chapter four, began to increasingly migrate into general international legal discourse. In 2009, the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE), an international military organization based in Tallinn, Estonia, invited an 'International Group of Experts' to produce a manual on the law governing cyber warfare.[27] The conclusions of the group were only published three

[24] Ntina Tzouvala, 'The "Unwilling or Unable" Doctrine and the Political Economy of the War on Terror', *Humanity: An International Journal of Human Rights, Humanitarianism, and Development* 14, no. 1 (2023): 19–38.

[25] Mueller, 'Against Sovereignty in Cyberspace', 782; Ilves, 'Address by H.E. Mr. Toomas Hendrik Ilves, President of the Republic of Estonia to the 62nd Session of the United Nations General Assembly'; Rain Ottis, 'Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective'.

[26] Mueller, 'Against Sovereignty in Cyberspace', 782.

[27] Michael Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 1.

years later, but the establishment of its mandate reflects the emerging discursive shift.

In September 2012, an inter-agency legal conference on the roles of cyber in national defense took place at Fort Meade - the epicenter of the American cybersecurity industry. Here, United States legal advisor Harold Koh delivered a speech that would decisively put an end to the cyber-exceptionalism.[28] Koh reiterated how 'cyberspace presents new opportunities and new challenges for the United States in every foreign policy realm, including national defense.' To that he added:

> [F]or international lawyers, it also presents cutting-edge issues of international law, which go to a very fundamental question: *how* do we apply old laws of war to new cyber-circumstances, staying faithful to enduring principles, while accounting for changing times and technologies?[29]

Koh turned to affirm the *general applicability* of international law in cyberspace. He concurrently rejected the idea of cyberspace as a 'law-free zone where everything goes' and suggested that 'we must articulate and build consensus around *how* it applies and reassess from there whether and what additional understandings are needed' with a view to 'promot[ing] stability in this area.'[30] Koh's speech, constituting the first public unilateral position on international cyber law, marks a fundamental shift from the era of widespread cyber-exceptionalism. To Koh, it was suddenly evident that international law generally applied in cyberspace, and a process of articulation and consensus-building was lying ahead regarding *how it applies.*

Shortly after Koh's speech, the International Group of Experts that had been appointed by the NATO CCD COE three years earlier published the *Tallinn Manual on the International Law Applicable to Cyber Warfare.* The International Group of Experts was unanimous in its estimation that both the *jus ad bellum* and *jus in bello* apply to cyber operations, thus supportin the American view.[31] Only a few months after the publication of the *Tallinn Manual on the International Law Applicable to Cyber Warfare,* the second report of the GGE was published. In sharp contrast to the silence on international law in in the

---

[28] Koh, 'International Law in Cyberspace'.

[29] Koh.

[30] Koh. (emphasis mine)

[31] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 3.

report of the GGE published in 2010, the 2013 report holds that consideration should be given to 'common understandings on the application of relevant international law and derived norms, rules and principles of responsible behaviour of States.'[32] The striking shift in the legal assumptions of the time becomes evident when comparing the two reports: While the first report assumes that cyberspace constitutes a lawless space, the latter report assumes the general applicability of international law and calls for the consideration of common understandings thereof as a measure to enhance international peace, stability and security.[33] As such, the trajectory of the work of the GGE elucidates a significant evolution in the perceptions of the legal nature of cyberspace. The 2013 report of the GGE was welcomed by the General Assembly in a subsequent resolution, which authorized the GGE in its next report to study '*how* international law applies to the use of information and communications technologies by States.'[34] The request was met with a third report of the GGE, published in 2015, in which any lingering notions of cyber exceptionalism were decisively dismissed. The report made it clear that international law is not only applicable to cyberspace but also fundamental to maintaining order and security in the digital realm:

> The adherence by States to international law, in particular their Charter obligations, is an essential framework for their actions in their use of ICTs and to promote an open, secure, stable, accessible and peaceful ICT environment. These obligations are central to the examination of the application of international law to the use of ICTs by States.[35]

The 2015 report manifested the idea that cyberspace is not beyond the scope of an extension of existing international obligations. The report's emphasis of '*established* international legal principles' and 'the *inherent* right of States' arguably indicates a sudden eagerness to underscore that nothing had changed. The report also 'recognized the need for further *study* on this matter' – a verb choice denoting that the task ahead is better performed by

---

[32] Group of Governmental Experts, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (United Nations, 24 June 2013), 7.

[33] Group of Governmental Experts, 7.

[34] United Nations General Assembly, 'Res. 69/28', 3. (my emphasis)

[35] Group of Governmental Experts, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (United Nations, 22 July 2015), 12.

qualified legal experts.[36] In other words, the discourse of the report suggests that international cyber law was a merely technocratic exercise detached from politics. Since then, an assumption of international law's general applicability in cyberspace has been dominant. In other words: the field of international cyber law had been born.

I elaborate on the prevalence of this legalistic discourse and discuss its implications later in this chapter. However, let us first dive into the emerging contours delineating the nascent field of international cyber law.

Contours of the Nascent Field

From the very birth of the field of international cyber law, the concept of 'cybersecurity' was fundamental to its delineation. As we saw in chapter four, cybersecurity is a flexible construct, which has evolved in response to the needs of capital. After a decade of widespread promotion of information technologies as key to societal progress and the consequent vulnerabilities arising for a digitally reliant capitalist economy, the concept of cybersecurity had taken shape around the protection of digital infrastructure against external intrusions. When states began to publish unilateral positions on international cyber law, their positions did not address *all* rules of international law, but a selection of rules which was delineated around the rationalities inherited from this dominant notion of cybersecurity.

The field of international cyber law began with a relatively narrow military focus, manifested in Harold Koh's landmark speech mentioned above focusing on the rules governing use of force and armed conflicts (*jus ad bellum* and *jus in bello*). However, the scope of international legal rules deemed relevant to uphold cybersecurity was gradually widened throughout the 2010s. The process of the drafting of the two volumes of the Tallinn Manual is illustrative of this process. The first Tallinn Manual, *Tallinn Manual on the law governing cyber warfare*, was limited to the legal framework regulating cyber operations involving the use of force (*jus ad bellum*), as well as on cyber operations occurring in the context of armed conflict (*jus in bello*). According to the introduction to the manual, the project was motivated by cyber operations against Estonia in 2007 and against Georgia during its war with the Russian Federation in 2008, as well as cyber incidents like the targeting of the Iranian nuclear facilities with the Stuxnet worm in 2010.[37] The

[36] Group of Governmental Experts, 12. (my emphasis)

[37] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 1–2.

international issues that international law should regulate were thus related to the protection of digital infrastructure against external intrusions. This delineation was soon after perceived to be too narrow; paraphrasing Estonian president Toomas Ilves, the very cyber-attacks motivating the analysis of the rules of cyber warfare turned out in retrospect to be 'fairly mild and simple'.[38] The narrow scope of the manual resulted in the exclusion of a range of operations to which an international legal framework would need to respond. This awareness led to the initiation of the drafting process for the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. The scope of the second manual was expanded to include also public international law governing cyber operations during peacetime. The expansion followed from the notion that, although cyber operations involving the use of force and occurring in the context of an armed conflict 'will typically be more worrisome from a national security perspective than those that occur in peacetime, States have to deal with cyber issues that lie below the use of force threshold on a daily basis.'[39] The scope of cyber operations that were perceived as relevant from a national security perspective was thus broader than the most severe cases covered by the first manual. As stated by Ilves:

> At a time when the actions of unscrupulous States and violent extremist groups continue to threaten peace and security internationally, it is even more important that such actions are countered with a strong commitment to existing international law and the values that it represents.[40]

The scope of the second manual was therefore broadened to include discussions of peacetime security measures. The process of the Tallinn manuals reflects how the contours of international cyber law are drawn around the concept of cybersecurity.

As we saw in chapter four, the idea of external intrusions into digital systems constituting a security threat is premised on an appreciation of digital systems as inherently worthy of protection. As we dive into states' positions on international cyber law, the rationalities underlying this dominant notion of cybersecurity shines through in the field. Sometimes, states express their appreciation for digital technologies explicitly. In the prologue to this

[38] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, xxiii.
[39] Schmitt, 1.
[40] Schmitt, xxiv.

dissertation, I quoted the United States legal advisor Brian J. Egan, who introduced the American view on international law in cyberspace in proximity to Silicon Valley with an unhinged appraisal of technological developments, which delivered 'significant economic, social, and political benefits to individuals and societies around the world.'[41] His deliberate appreciation of the innovative whiz kids of Silicon Valley underscores how the need to protect the digital landscape is motivated by a celebration of a neoliberal market economy as the road to universal prosperity. The United Kingdom equally declares its commitment to a 'free, open, peaceful and secure cyberspace' and holds that the 'use of cyberspace is in the interest of States and the international community as a whole'.[42] Germany asserts that 'the vast interconnectedness of networks, technologies and cyber processes across borders has brought societies and individuals from different nations closer together and has opened up new opportunities for cooperation among both State and non-State actors.'[43] The appraisals continue the discourse prominent in the 1990s marked by a market-focused celebration innovation, knowledge- and information sharing, communication, development, and growth. The universalizing discourse suggests an uncontestable interest in the promotion of the information technology landscape.

The celebration of information technologies as a universal good is shaping the notion of cybersecurity, which is delineating international law. As explicitly put by Sweden, the areas of international law on which it presents its views are areas 'relevant to international security', reflecting the 'subjects discussed in the UN forums and those which are commonly covered in other states' position papers'.[44] Denmark, similarly, delineates its position paper as 'cyberspace in the broad context of international peace and security'.[45] Switzerland holds with reference to the GGE that 'the primary focus of states lies on the security-related aspects in the digital space (cybersecurity)

[41] Brian J. Egan, 'International Law and Stability in Cyberspace', 1.

[42] United Kingdom, 'Application of International Law to States' Conduct in Cyberspace: Statement of the United Kingdom', 3 June 2021.

[43] Germany, 'On the Application of International Law in Cyberspace', March 2021.

[44] Ole Engdahl, 'Sweden's Position Paper on the Application of International Law in Cyberspace' (Nordic Journal of International Law, 4 July 2023).

[45] Jeppe Mejer Kjelgaard and Ulf Melgaard, 'Denmark's Position Paper on the Application of International Law in Cyberspace' (Nordic Journal of International Law, 4 July 2023), 447.

and the applicable provisions under international law in this area.'[46] These explicit delineations demonstrate how the notion of cybersecurity is a *raison d'être* of the field. This delineation cannot be explained based on any legal systematicity (they typically cover an array of rules from different bodies of international law, ranging from *jus ad bellum* and *jus in bello* to state responsibility, sovereignty, due diligence, and human rights). It rather reflects a prior idea about what needs protection and what constitutes a security threat. As we saw in chapter four, cybersecurity is understood as equivalent to stability and reliability for digital systems, and any external intrusions to these systems are thus seen as threats.

Clarification or Construction?

We have now seen that the idea of 'cyberspace' as the object of general international law is a quite new one. While I believe this to be a relatively uncontroversial claim for the scholars of the field of international cyber law (after all, the development has happened overtly and within their lifetime), the point is often forgotten. Perhaps more accurately, the point is often being disregarded as irrelevant. The perceived irrelevance of the novelty of the idea reflects an important feature of legal positivism: its tendency to abstract from the process through which rules emerge, evolve, and terminate. As we saw in chapter one, positivist scholars find that this process lies beyond the scope of their key ambition, namely, the identification of *lex lata*. If they are at all bothered by the fact that their methodological framework is inherently incapable of accounting for the process through which rules emerge, evolve, and terminate, they rarely show it. This should not come as a surprise: as we saw in chapter two, the power of law lies precisely in its ability to shield the process of its own emergence, evolution and termination. Once we begin to look into that process – as I have done above – international law's structural indeterminacy becomes strikingly clear. Later in this chapter, I will argue that we can make sense of this process – in other words, understand the emergence of the field *despite* the structural indeterminacy – through a Marxist lens. Before that, this section explores the discursive strategies employed within the field of international cyber law in relation to the emergence of the field. The aim of the section is to illuminate how the positivist

[46] Switzerland, 'Switzerland's Position Paper on the Application of International Law in Cyberspace (Annex to the United Nations Group of Governmental Experts 2019/2021)', May 2021.

tendency to abstract form the process through which rules emerge plays out in the context of international cyber law, masking an inherently political process as a technocratic exercise.

Despite the overt nature of the legal development occurring since the 1990s, the field of international cyber law deploys a discourse of denial, addressing the current state of affairs as if it were always given. Crucial points that were overtly contentious until very recently are presented as objective facts, and when uncertainty is acknowledged on discussions of precise legal norms, an assumption prevails that a correct answer exists which can and will be identified. For example, scholars may recognize 'the need for further study'[47], thus implying that a thorough study of this or that ambiguous rule will eventually reveal its correct content. The social arrangements being promoted and upheld through international legal discourse are thereby made to appear as *the only rational outcome*.

Through this discourse, international legal regulation of cyberspace is framed as a natural interpretative result. In his 2016 speech, United States legal advisor Brian J. Egan noted in a jovial tone:

> It says a lot about where we were four years ago that the first two questions Koh addressed in his speech were as fundamental as "Do established principles of international law apply to cyberspace?" and "Is cyberspace a law-free zone, where anything goes? (So as not to leave you hanging, the answers to those questions are an emphatic "yes" and "no" respectively!)[48]

We have, Egan noted, made 'significant progress since then.'[49] Egan asserted how the recognition of the general applicability of international law 'is the easy part, at least for most like-minded nations', the more challenging part is 'identifying how that law applies to specific cyber activities'.[50] As such, only six years after the assumption of the GGE that cyberspace is a lawless space, the general applicability was now an 'easy' matter for 'like-minded nations'. The process to follow was an exercise of 'identifying' how specific rules of international law apply to cyberspace. A process of 'identification' suggests that a correct answer exists, and that competent experts in

---

[47] Group of Governmental Experts, 'A/70/174', 12.

[48] Brian J. Egan, 'International Law and Stability in Cyberspace'.

[49] Brian J. Egan.

[50] Brian J. Egan.

the field will be capable of eventually determining what interpretation and application is correct.

The United Kingdom, while acknowledging that international law is undergoing development, similarly speaks of this development in a legalistic discourse that suggests the development process being the result of an almost mechanical interpretative endeavor. The process thus has the purpose of ensuring 'a better understanding', 'facilitate greater transparency' and greater 'clarity' on the specific international legal regulation.[51] Estonia similarly notes how 'cyber still leaves a lot of grey areas, including on how precisely international law applies in cyber sphere', and declares its intention to contribute to 'further clarifying this issue and leading the way together with other allies.'[52] The Netherlands encourages 'international debate on ways to *clarify* the application of international law in cyberspace. *Clarity* and *consensus* on these points are essential to the international legal order.'[53] Denmark speaks of 'unanswered questions' regarding the 'precise interpretation' and of 'lack of clarity'.[54] Poland holds that the 'specific nature [of cyberspace] requires explanation, sometimes also clarification, as to how norms of international law can be applied in the context of activities in cyberspace.'[55] The determinate discourse is also prevalent in the March 2021 Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the context of International Security (OEWG).[56] The OEWG was established by the United Nations on the initiative of Russia pursuant to a failure of reaching consensus in the latest

---

[51] United Kingdom, 'Application of International Law to States' Conduct in Cyberspace: Statement of the United Kingdom'.

[52] Kersti Kaljulaid, 'President of the Republic of Estonia at the Opening of CyCon 2019' (Tallinn, 29 May 2019).

[53] The Netherlands, 'Appendix: International Law in Cyberspace', 5 July 2019. (My emphasis)

[54] Kjelgaard and Melgaard, 'Denmark's Position Paper on the Application of International Law in Cyberspace'.

[55] Poland, 'The Republic of Poland's Position on the Application of International Law in Cyberspace', 29 December 2022.

[56] Open-ended working group on developments in the field of information and telecommunications in the context of international security, 'Final Substantive Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' (United Nations, 10 March 2021).

GGE. The OEWG concluded that 'additional neutral and objective efforts to build capacity in the [area] of international law' were needed to 'deepen [States'] understandings of how international law applies to the use of [information and communication technologies]'.[57] One body that has emerged in response to this call for 'neutral and objective' efforts is the Oxford Process on International Law Protections in Cyberspace. With a mission of 'deepening understanding on the application of international law and to provide clarity on how this body of law governs and prohibits a range of cyber threats', the Oxford Process claims to have established itself as 'one of the key neutral capacity-building initiatives aimed at the clarification of international law.'[58] As these textual examples illustrate, the field masks the process of constructing international cyber law as a neutral interpretative process through the deployment of words such as *clarifying*, *identifying*, *examining*, *explaining*, and *ensuring precision in* law.

Positivist international legal scholars simulate the determinate discourse of states. Ever since the emergence of consensus amongst (Western) states that international law applies in cyberspace, a wealth of scholars has focused their attention on specific ambiguities in the international legal framework – 'the grey zone landscape'[59] or the 'less well-understood aspects'[60] of international cyber law. The task ahead of them is seen as one of 'unblurring the lines'[61] or clearing the 'normative fog'[62]. Such metaphors indicate that the process playing out is merely intended to remove a layer of blur from the picture to reveal an underlying truth about international legal rules applicable in cyberspace.

The determinate discourse allows the dominant forces of the field to call out states with a different view than that of 'likeminded' Western states as bad actors. Schmitt, for example, presupposes that states whose views differ from the views of Western, liberal states, are acting in bad faith. They are 'strategically exploiting' international law principles and rules that are still

---

[57] Open-ended working group on developments in the field of information and telecommunications in the context of international security, 6.

[58] 'The Oxford Process on International Law Protections in Cyberspace: A Compendium' (Oxford Institute for Ethics, Law and Armed Conflict, 2022), 11.

[59] Schmitt, 'Grey Zones in the International Law of Cyberspace'.

[60] Kubo Mačák, 'Unblurring the Lines: Military Cyber Operations and International Law', *Journal of Cyber Policy* 6, no. 3 (2021): 412.

[61] Mačák, 412.

[62] Schmitt, 'The Law of Cyber Conflict'.

'poorly demarcated or are subject to competing interpretations'.[63] Schmitt even goes so far as to suggest that 'Russia's grey zone operations amount to a form of 'asymmetrical lawfare.' Russia's strategy is conceived as asymmetrical in the sense that 'States committed to the rule of law are less likely to operate in the grey zone than States that do not share this rule of law commitment.'[64] In light of Schmitt's early contribution to the scholarly debate on international cyber law, in which he deliberately predicted that the American view of things would eventually dictate the future international legal framework, one may object that in the case of the United States, committing to the rule of law is largely a self-fulfilling prophecy. A similar view is expressed by Matthew Waxman, who holds that 'America's power in its various forms-and vulnerabilities to power will greatly influence its own interpretive approach to these issues, and because of its relative power globally it will greatly influence international legal movement in this area.'[65] In Schmitt's analysis, Russia's grey zone operations are not seen as relevant state practice in the process of clarification. Russia's behavior instead constitutes an exploitation of the situation in which the United States and its allies are yet uncertain as to what rules to lay out.

The determinate discourse of the field masks the process as a technocratic exercise that is best performed by 'neutral and objective' experts in the field. The eventually emerging rules thus appear as natural results of the rigorous endeavors of experts, raised above political contestation. To illustrate the effect of this discursive maneuver, let us consider the sound of alternative words. Words such as *creating*, *constructing*, *developing*, *discussing*, or *negotiating* would emphasize the indeterminate and open-ended nature of the process. Thereby, the process would appear as what it is: a political process. Individuals and social movements would see a window of opportunity to advocate for policies that favor their interests. And ultimately, when dominant powers would expectedly defeat such rival positions, this defeat would be an overt, political defeat. The eventual outcomes of the political process would be deprived the power legal discourse – that is, its appearance as a regulatory force distinguishable from social relations. By refraining from the use of words that reveal the indeterminate nature of international law, the conclusions eventually reached within the field of international cyber law are made

[63] Schmitt, 'Grey Zones in the International Law of Cyberspace', 1.

[64] Schmitt, 3.

[65] Matthew Waxman, 'Self-Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions', *International Law Studies* 89 (2013): 110.

to seem like the outcome of a neutral, technocratic endeavor - and thereby, they are made to seem politically incontestable.

When we look behind the determinate language and start to see the process of clarifying international law in cyberspace as rather a process of *making international cyber law*, the field reemerges before us as an arena of political negotiation. In international law, states are generally perceived as the central actors. However, as I will show, states meet in the process with the most privileged stakeholders – those who made it to the table of the 'clarification process'. At this table, technology corporations have a central spot.[66] The Oxford Process on International Law Protections in Cyberspace, mentioned earlier in this section, is an illustrative example of the corporate involvement. While the Oxford process mainly involves a long list of international law scholars, the process is sponsored by Microsoft who has, just like a list of other tech companies, been substantially involved in the discussions.[67] The corporate representatives often play the role of technological experts, laying the ground for the legal discussions by elucidating the technical, material reality and practical concerns on which the legal discussions should center. They thus contribute to delineating and defining the problem areas. For example, a discussion of international law and election interferences was commenced with a cryptographer from Microsoft laying out the technical foundation. He emphasized the decentralized structure of presidential elections in the United States as a key security risk. As over 8,000 elections was conducted simultaneously, each with its own procedures, equipment, and auditing techniques, vulnerabilities allegedly emerged. Conveniently, he assured that Microsoft had already built the software to solve the problem; instead of relying on trust in decentralized election administrations, the election system could now rely on trust in Microsoft instead. Security considerations thus allegedly demanded a centralized digital solution reliant on Microsoft software, rather than decentralized procedures. With the caveat that a substantial critique of the technicalities of this assessment is beyond my expertise, it is notable that the Microsoft representative here emphasizes technological *centralization* as a tool for better election security; after all, the general concern around cyber security has been the vulnerabilities *arising from* centralization and connectivity, making vast systems vulnerable to

[66] I owe this point to Henning Lahmann.

[67] 'The Oxford Process on International Law Protections in Cyberspace: A Compendium', 191–92, 206.

singular disruptions. However, the centralization of election management through the standardized deployment of software like Microsoft's was here presented the *solution* to a security challenge. The involvement of Microsoft illuminates how the tech industry gets to contribute to delineating and defining the ever-evolving meaning of cybersecurity underlying the field of international cyber law.

Another forum for discussion of international cyber law is the International Conference on Cyber Conflict (CyCon), which is every year convened in Tallinn. The conference is sponsored by a long list of technology and cyber security companies, including Microsoft, Fortinet, Paloalto, and TREND. While corporations are not usually appearing from the formal proceedings, which are reserved for academic contributions, they are present in the program as keynote speakers, host a myriad of side-events, and facilitate and sponsor closed-door briefings and closed discussions in the margins.[68]

In conclusion, the discourse surrounding international cyber law presents the process of legal development as a matter of clarification rather than negotiation, masking its inherently political nature. By framing politics as an exercise of legal interpretation, the field reinforces existing power structures and marginalizes alternative perspectives. Once we recognize that the so-called 'clarification' of international cyber law is, in fact, an ongoing process of legal construction, the field reveals itself as a political battleground in which powerful stakeholders seek influence. With this reality established, let us now seek to root the operations of this political process in the political economic realities of the digital landscape.

Making Sense of the Birth

I argued in chapter two that the legal form carries a categorical symmetry with the commodity-form and that the content of international law reflects the social relations between states. To understand these relations, we must consider the role of the state-system in the reproduction of the social relations of capitalism. It is now possible to root the contours of the content of international cyber law in the material basis. By doing so, we can not only explain the emergence of the field of international cyber law; we can also explain why it did not emerge sooner.

[68] This observation is based on my personal experience at CyCon 2023.

Let me begin by recapitulating how information technologies emerged and evolved in response to capital's strive for continuous expansion. As we saw in chapter three, digital inventions were key to a profound economic restructuring following the economic recessions of the so-called long downturn in the 1970s.[69] State-financed research went into groundbreaking technological inventions to be transferred to market forces, tasked with turning them into profit.[70] In the years to come, rates of exploitation were increased, and South-to-North value-flows were accelerated. But the rate of profit was also significantly boosted from its lows of the early 1980s.[71] And thus, they were a success. With the fall of the Second World, almost every corner of the globe had been fused into the global capitalist economy. With the emergence of the internet, information technologies were reincarnated in the form of *cyberspace* – not just a set of technologies but as a new, virtual terrain. In this neoliberal era, we saw in chapter four how advanced capitalist states would celebrate and promote the expansion of the 'information society' as an unequivocal solution to any thinkable problem. Worldwide deregulation and removal of barriers went hand in hand with the idea that the emerging new space fashioned by innovative technologies was a distinct space that did not belong under any jurisdiction. Cyberspace was a 'wild west' – a no-man's-land awaiting to be cultivated. In other words, the digital domain made up an arena into which capitalism could continue its expansion in a time when every geographical region of the world was increasingly integrated into the global economy. Throughout this era, the central role of the state-system was to counter capitalism's tendency towards crises and stagnation by facilitating its expansion into new terrains. The absence of legal discourse in this era supported the idea of cyberspace as an open terrain free to be appropriated and cultivated, thus facilitating capital expansion and satisfying growth rates.

Cyberspace soon enabled capitalism's migration into ever-more aspects of life. The emergence of the Web 2.0 gave rise to a new data economy, making even the most intimate details of life transparent to tech corporations to whom it became an extractive resource. Already around the beginning of the 2000s, the emerging awareness of the vulnerabilities arising in digital space gave way for international discussions of cybersecurity, as

---

[69] Brenner, *The Economics of Global Turbulence*.

[70] Tarnoff, *Internet for the People*, 6–7.

[71] McNally, 'From Financial Crisis to World-Slump'.

discussed in chapter four. The central security-threat in this era was perceived to be the terrorist use of hacking.[72] However, in the years to come, information technologies facilitating global supply chains continued to develop into ever-more advanced systems, enabling the centralization of control into fewer hands. Meanwhile, the belief in the universalization of Western liberalism gradually vanished. The cyberoperations against Estonia in 2007 and against Georgia in 2009, which are widely perceived to be attributable to Russia, served as cruel manifestations of the unfulfilled dream. Concurrently, the digital landscape continued to grow ever-more advanced, presenting a rising vulnerability to disruptions.

The role of states in ensuring the stability and predictability which capital needs but lacks, could no longer be sufficiently fulfilled within domestic legal frameworks and enforcement mechanisms; the global nature of information technologies increasingly required the *state system* to work to protect the digital infrastructure on which the economy had become reliant. This key role of the state-system in global capitalism expresses itself in international law: International cyber law emerged as a response to the vulnerabilities to the capitalist system arising from its reliance on a global network of technologies and the role of states in ensuring stability and predictability in the arrangements of capitalism. We can therefore explain the emergence of international cyber law as an expression of the role of the state-system in the reproduction of the social relations of capitalism. *First*, states facilitated economic expansion by keeping cyberspace an open, lawless terrain open for appropriation, reflecting the role of states in seeking out new revenues for capital to avoid stagnation. *Second*, as digital systems became increasingly central to capital circulation, the capitalist economy became vulnerable to external disruptions from states and non-state actors. States sought to guarantee stability by facilitating the migration of international legal discourse into the cyber domain. Capitalism requires the effective protection of the property relations on which the social relations of capitalism rely. As these relations and their transactions are increasingly digital, reliability in digital technologies is key to capitalism. International cyber law has taken shape around the protection of digital infrastructure against external intrusions. The field reflects capitalist states' endeavors to ensure stability to capital by ensuring international legal protection of digital infrastructure.

---

[72] Hansen and Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', 1155–56.

LAW FOR WHOM?

In the modern world, an effective way of establishing and maintaining relations of domination is to make authority seem valid and appropriate through the legality of rules.[73] International law promises the provision of abstract, objective standards against which particular conduct can be evaluated – a 'process that relates neutral principles to concrete occurrences'.[74] The application of international law to information technologies, then, appears as a neutral, technical exercise (albeit sometimes a challenging one), the outcome of which is beyond the scope of debate. Herein lies law's power: As I argued in two, the social character of the relations between states is reflected as natural characteristics of international law, and the sum of these relations come to show themselves as regularities in what we come to accept as rules. As international law presents itself as a regulatory force external to the underlying social relations, these social relations are reified in international law.

In this chapter, I have explored the emergence of the idea that 'cyberspace' is regulated by international law. I have shown how the field of international cyber law tends to shield the indeterminate nature of international law and merely address developments as 'clarifications', as if the correct answer were always present in the background and the technical task of legal interpretation was the key to eventually reveal the correct content of international cyber law. However, once we begin to observe this allegedly autonomous process through which legal ideas emerge, it becomes evident that regularities in what is accepted as law is far from natural interpretative result of an autonomous process.

When international law is thus seen as politics, as it should be, then the very notion of 'law' becomes ambiguous: what kind of law? Law for whom? Law for what? The determinate discourse within the field of international cyber law comes to neglect the social antagonisms within societies within the digital landscape.

The very emergence of international cyber law reflects the intricate relationship between determinacy and indeterminacy in international law. Despite the underlying structural indeterminacy, consensus may crystallize into acceptance of certain ideas as law, reflecting the dynamics of the underlying social relations. This chapter has told the story of how such consensus

---

[73] Marks, *The Riddle of All Constitutions*, 19.

[74] Purvis, 'Critical Legal Studies in Public International Law', 105.

eventually crystallized on the contours of international cyber law. The contours of the field are now established: International cyber law seeks to protect digital systems from external intrusions carried out by states or non-state actors. Within these broad contours, uncertainty remains on the precise interpretation and application of a wide range of extant rules in cyberspace. While a detailed analysis of these uncertainties is impossible within the scope of this dissertation, chapter six zooms in on one of the most striking examples – the doctrine of sovereignty – and analyzes the debates surrounding the concept as a case-study of the international law-making in cyberspace.

CHAPTER VI
DIGITAL SOVEREIGNTY

No international legal concept is as foundational, yet contentious, as the doctrine of sovereignty. Sovereignty has a constitutional role in the positivist methodology which, at least in the traditional doctrine, derives international law from the will of the sovereign state.[1] Yet, the concept of sovereignty has never been a static or universally agreed-upon idea. It is a flexible construct that has evolved in international legal discourse in response to the questions that international lawyers have asked themselves and tried to respond to.[2] Following Antony Anghie, 'doctrinal and institutional developments in international law cannot be understood simply and always as logical elaborations of a stable, philosophically conceived sovereignty doctrine, as an outcome of the continuing attempt to create order among sovereign states.'[3] The digital age has added new dimensions to this complex concept. The geographical borders around which territorial sovereignty has traditionally taken shape are not intuitively transferrable to digital space, which – even if a cloud is always physically located somewhere – is often seen to consist of some intangible reality beyond its physical components. The field of international cyber law has therefore brought sovereignty under renewed

---

[1] See Simma and Paulus, 'The Responsibility of Individuals for Human Rights Abuses in Internal Conflicts'.

[2] Tzouvala, *Capitalism As Civilisation*, 15–16.

[3] Antony Anghie, *Imperialism, Sovereignty and the Making of International Law* (Cambridge: Cambridge University Press, 2005), 6.

scrutiny, raising questions about the application of the sovereignty in an era where interconnected digital infrastructures are causing new vulnerabilities.

In this chapter, we have come to move from that which appears obvious to that which remains ambiguous. Within the now established field of international cyber law, states and legal scholars are debating a wide range of general international legal norms in the context of information technologies. These legal norms span from questions within the regimes of on *jus ad bellum* and *jus in bello* to state responsibility, countermeasures, and international human rights law. The cyber-specific meaning of many of these legal concepts remains overtly contentious. Employing the language of Koskenniemi introduced in chapter one, these ambiguities constitute cases of *substantial indeterminacy*. As such, their 'content' remains unsettled, and states and international legal scholars are overtly debating which interpretation is better. A dissection of every one of these ambiguities exceeds what impossible within the scope of this dissertation. Instead, I will trace the doctrinal discussions about the doctrine of sovereignty, which stands out as a notoriously ambiguous and historically controversial concept. By zoom in on the ambiguities surrounding the question of digital sovereignty through a Marxist lens, the chapter serves as an exemplification of how this lens is not only useful to understand established contours of the field but can also help us understand prevalent ambiguities. The chapter thus aims to illustrate how the concrete dynamics of the field can be understood as a reflection of the role of the state-system in the reproduction of capitalism.

To fully appreciate the contemporary debates surrounding digital sovereignty, it is essential to understand how they mark a continuation of the historical evolution of sovereignty in international law. Since the rise of positivist legal thought during the colonial era, sovereignty has consistently taken shape to reflect the material interests of European states.[4] As I will show, these historical dynamics echo in today's discussions of sovereignty in cyberspace. I therefore begin the chapter by reiterating and elaborating on some of the insights from chapter two to situate the current debates on digital sovereignty within its historical trajectory. The subsequent sections of the chapter trace the doctrinal debates on digital sovereignty. Approaching these debates through a Marxist lens, I suggest that we can understand the

[4] Anghie, *Imperialism, Sovereignty and the Making of International Law*; Tzouvala, *Capitalism As Civilisation*.

ambiguities surrounding the doctrine of sovereignty as a reflection of an apparent contradiction in the functions of the capitalist state in the current era: *on the one hand*, the need to ensure the stability and reliability for capital through the effective protection of property rights in the digital space, and *on the other hand*, the need to satisfy capital's boundless thirst for expansion.

CONTEXTUALIZATION

Understanding the significance of the current debates surrounding sovereignty in cyberspace demands us to take a brief look into its historical trajectory. As elaborated on in chapter one, the positivist methodology relies on an idea that international law consists of those rules which have been agreed upon by sovereign states. The task of defining the sovereign state has thus always been fundamental to positivist jurisprudence. Throughout the 19th century, the jurisprudential task lied in a careful scrutiny of what entities could be regarded as 'sovereign'.[5] The concept of 'civilization' emerged, as we saw in chapter two, as a central argumentative tool in the identification of the sovereign state. While 'civilized states' thus enjoyed full jurisdictional sovereignty as a matter of right, the jurisdiction of the 'semi-civilized polities' remained dependent on their (unequal) treaties with the West. Meanwhile, the jurisdiction of the 'barbarous peoples' was beyond the pale of international law.[6] The colonial confrontation did therefore not unfold between two sovereign states, 'but rather between a sovereign European state and a non-European society that was deemed by jurists to be lacking in sovereignty – or else, at best, only partially sovereign.'[7]

Ntina Tzouvala shows in *Capitalism as Civilization* that the concept of civilization cannot be reduced to a legal concept reserved 19th century jurisprudence. It rather reflects an argumentative practice, which has continued into the present century.[8] Throughout the 19th century, the 'standard of civilization' oscillated between two logics – the 'logic of improvement' and the 'logic of biology'. Within the framework of the former, discussions about civilization centered on the supposed universal validity of specific core

[5] Anghie, *Imperialism, Sovereignty and the Making of International Law*, 56; McKenna, *Reckoning with Empire*, 9.

[6] Tzouvala, *Capitalism As Civilisation*, 52.

[7] Anghie, *Imperialism, Sovereignty and the Making of International Law*, 5.

[8] Tzouvala, *Capitalism As Civilisation*.

institutional and legal prerequisites necessary for the establishment and perpetuation of the capitalist mode of production. The protection of certain rights and liberties, such as property rights, travel, and freedom of commerce, was an essential precondition for conforming with this image of civilized life, and thus, a precondition for sovereignty.[9] The latter logic, the 'logic of biology', constantly negated the possibility of equal recognition of non-Western political communities as sovereigns, demoting them to a subordinate position.

With the decolonization of Asia and Africa in the years following the Second World War, the doctrine of sovereignty reached universal application. But the civilization discourse, oscillating between the 'logic of improvement' and the 'logic of biology', continued. In this era, the overtly racist rhetoric of civilization was gradually replaced with a technical discourse of improvement: evaluations, statistics and rankings were put in place to measure progress towards becoming a capitalist state. The formal equality prescribed by the doctrine of sovereignty was thus accompanied by a constant attempt to condition that equality on the adaptation to a regulatory system in the image of the Global North. The regime of human rights was central in this process. A liberal human rights discourse, focused on an individual-based human rights activism, thus coincided with the universalization of sovereignty.[10] As Miriam Bak McKenna argues, 'the emergence of the sovereignty of colonial people was simultaneous with the creation of international human rights law which sought to condition the character of that sovereignty.'[11] The global extension of an international legal order through the universalization of sovereignty thus went hand in hand with the global expansion of liberal rule.

The historical trajectory of the discourse on sovereignty is a trajectory of the geographical expansion of capitalism. These dynamics echo in today's debates on sovereignty in cyberspace. As I will show, state control with digital infrastructure is thus framed as both a stabilizing necessity and a potential threat to a set of perceived universal liberal norms. We have now come to explore how these competing narratives shape contemporary discussions on digital sovereignty.

---

[9] Tzouvala, 60.

[10] McKenna, *Reckoning with Empire*, 109–10.

[11] McKenna, 111.

Renewed Debates: Digital Sovereignty

While the doctrine of formally equal sovereign states is widely accepted as a foundational principle of the international legal system, the *self-standing* legal implications of the doctrine of sovereignty have been the subject of significant debate in the context of international cyber law. Overall, the debate is divided between those arguing that sovereignty is a legally binding rule and those arguing that sovereignty is a foundational principle from which other rules can be derived. The *first* position holds that sovereignty is a primary rule of international law, which is violated by any cyber activity that infringes the digital territory of another state (the 'pure sovereignty' position). The *second* position, endorsed by the United Kingdom and until recently the United States, holds that sovereignty is a principle of international law, not a primary rule that can be independently violated (the 'sovereignty as a principle' position).[12] While the 'pure sovereignty' position emphasizes security and stability in cyberspace, reflecting an emphasis on the role of the state in the protection of digital property, the 'sovereignty as a principle' position aligns with liberal ideals of a free and open internet, reflecting an emphasis on the role of the state in facilitating the expansion of digital markets. Between these two positions lies a *third* position, which seeks to reconcile the tension between the considerations underlying the two former positions by arguing that while sovereignty is indeed a legally binding rule, a certain threshold applies under which digital interference does not amount to a violation of sovereignty (the 'relative sovereignty' position).

The question of the legal nature of the doctrine of sovereignty in cyberspace is often emphasized by the defenders of the 'pure sovereignty' position to have its practical relevance concerning the international legal classification of so-called low-intensity cyber operations – that is, 'cyberoperations that involve penetrating a computer system located on the territory of another state without its consent but do not qualify as a prohibited intervention or use of force'.[13] In other words, sovereignty represents the 'lowest level' of

[12] Kevin Jon Heller, 'Low-Intensity Cyber Operations and State Sovereignty in Cyberspace' (Djøf Publishing in Cooperation with the Centre for Military Studies, 2023), 16; United Kingdom, 'Application of International Law to States' Conduct in Cyberspace: Statement of the United Kingdom'; Hon. Paul C. Ney, Jr, 'DOD General Counsel Remarks at U.S. Cyber Command Legal Conference'.

[13] Heller, 'Low-Intensity Cyber Operations and State Sovereignty in Cyberspace', 16.

international legal prohibition in cyberspace. Amongst these low intensity cyber operations also lie the so-called influence operations, which we briefly discussed in chapter one.[14] If low-intensity cyberoperations are deemed a violation of a legally binding rule of sovereignty, then the victim state has the right to take countermeasures, that is, to conduct activities otherwise unlawful under international law to bring the violation to an end in accordance with the International Law Commission's Draft Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA). Despite the attraction of legal measures to enforce stability in digital space, some states fear that a legally binding rule on sovereignty legitimizes states' protection of their 'national' digital space in ways that might interfere with the free flow of information, such as the Great Firewall of China, to which I will come back later in this chapter. Those advancing the 'sovereignty as a principle' position thus often emphasize instead how the question of the legal nature of the doctrine of sovereignty in cyberspace is above all a matter of protecting a set of universal liberal values.[15]

As we dive into the different positions on sovereignty in the international legal debates, it becomes visible how these different concerns are reflected in the ambiguity that continues to surround sovereignty in cyberspace. In the following sections, I go through the three positions and the arguments by which they are frequently justified. On this basis, we can elucidate the tension surrounding sovereignty in cyberspace through a Marxist lens.

Emphasizing Security: Pure Sovereignty

Most states contend that sovereignty is a legally binding rule that applies in cyberspace. This view has been adopted by states such as Brazil, China, Estonia, France, Iran, Italy, Japan, the Netherlands, New Zealand, Norway, Romania, Sweden, and the African Union.[16] Amongst those states holding

[14] Schmitt, 'Foreign Cyber Interference in Elections', 754; Sander, 'Democracy Under The Influence'; Lahmann, 'Information Operations and the Question of Illegitimate Interference under International Law'.

[15] United Kingdom, 'Cyber and International Law in the 21st Century'.

[16] GGE compendium of voluntary contributions, 'GGE Compendium of Voluntary Contributions'; Canada, 'International Law Applicable in Cyberspace', April 2022; Richard Kadlčák, 'Statement by Czech Republic' (2nd substantive meeting of the OEWG, UN General Assembly, 11 February 2020); Estonia, 'President of the Republic at the Opening of CyCon 2019' (Tallinn, 29 May 2019); Finland,

that sovereignty is a legally binding rule, some argue that sovereignty is violated by any non-consensual penetration of a computer system located on the territory of another state – what has been called the 'pure sovereignty' position.[17] Others argue that even though sovereignty is a rule, a certain threshold of harm must be met before a cyber operation violates the rule – often termed the 'relative sovereignty' position. In this interpretation, cyber operations are typically deemed wrongful only if they cause physical damage to the territorial state or render its cyberinfrastructure inoperable.[18] In this section, I will focus on the general considerations underlying the need for a rule on sovereignty. These considerations are given decisive weight by those states arguing for the 'pure sovereignty' position, but they also influence the 'relative sovereignty' position, to which we will get back later, which seeks to balance the considerations of the two 'extreme' positions.

An informative entry point into the considerations underlying the emphasis on sovereignty as a rule is the remarks on sovereignty in the Tallinn Manual 2.0. The International Group of Experts behind the manual holds that although 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.[19] It elaborates that the state can exercise sovereignty over cyber

---

'International Law and Cyberspace - Finland's National Positions'; Ministry of Defense of France, 'Perspective of France'; Germany, 'On the Application of International Law in Cyberspace'; Iran, 'Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace', 18 August 2020; Italy, 'Italian Position Paper on "International Law in Cyberspace"', 2021, https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf; Japan, 'Basic Position of the Government of Japan on International Law Applicable to Cyber Operations', 16 June 2021; The Netherlands, 'Appendix: International Law in Cyberspace'; New Zealand, 'The Application of International Law to State Activity in Cyberspace', 1 December 2020; Engdahl, 'Sweden's Position Paper on the Application of International Law in Cyberspace'.

[17] Heller, 'Low-Intensity Cyber Operations and State Sovereignty in Cyberspace', 16.

[18] Heller, 16; The Netherlands, 'Appendix: International Law in Cyberspace'; Richard Kadlčák, 'Perspective of Czech Republic'.

[19] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 16. The implications of the phrase are discussed in Lianne J.M. Boer, '"Spoofed Presence

infrastructure situated in the land territory, internal waters, territorial sea (including its bed and subsoil), archipelagic waters, or national airspace.[20]

As several scholars have pointed out, the language of the manual suggests an insistence on the *physicality* of cyberspace.[21] To the Group of Experts, data is always geographically located somewhere, 'residing' in a particular jurisdiction. The manual thus seems to insist on cyberspace 'having real world geography'. Molly Sauter argues that this geographic emphasis allows 'existing states of conflict and inter-state aggression [to] be seamlessly transferred into the online space, along with existing state-determined structures of enemies and bad actors'.[22] The manual thus rejects those descriptions of cyberspace that emphasize its virtual nature – discourses such as cyberspace as a 'global domain' or 'fifth domain' lacking physicality, which are typically underlying exceptionalist positions that we discussed in chapter five.[23] Underlying this position is therefore an emphasis on political and geographic borders over alternative conceptions of internet organization[24]. The emphasis on the physicality of cyberspace has the effect of situating cyberspace effectively within the territorial lines around which states' sovereignty is structured. This maneuver results in a priority of the states' right to control digital infrastructure within their territory over the regimes of international law that impose restrictions on this right through emphasis on universality, such as international human rights law. As such, sovereignty as a rule follows from an emphasis on physicality, non-exceptionality, and materiality of cyberspace. As Sauter asserts, the position privileges those bodies of policy that are concerned with state security and stability over those concerned with universality, cosmopolitan rights, and connectedness.[25]

Does Not Suffice": On Territoriality in the Tallinn Manual', in *Netherlands Yearbook of International Law 2016: The Changing Nature of Territoriality in International Law*, ed. Martin Kuijer and Wouter Werner (The Hague: T.M.C. Asser Press, 2017), 137; Mueller, 'Against Sovereignty in Cyberspace', 782.

[20] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 16.

[21] Schmitt, 16; Boer, '"Spoofed Presence Does Not Suffice"', 138; Molly Sauter, 'Show Me on the Map Where They Hacked You: Cyberwar and the Geospatial Internet Doctrine', *Case Western Reserve Journal of International Law* 47, no. 1 (2015): 63.

[22] Sauter, 'Show Me on the Map Where They Hacked You', 74.

[23] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 12.

[24] Sauter, 'Show Me on the Map Where They Hacked You', 74.

[25] Sauter, 74.

> When the network infrastructure present in a country is viewed as the unequivocal possession and responsibility of that country, an isolationist internet policy becomes possible. Such a view is inherently encouraged by the geographic metaphor, as well as the assumptions about attribution and locality of action that are implied therein.[26]

A pioneering contribution to the field of international cyber law makes an illustrative explication of the 'pure sovereignty' position: Patrick Franzese, a legal scholar in the United States Air Force, has argued that states must 'establish a cyberspace border that a state can both monitor and control', calling for 'Internet border inspections' and a system of nationally rooted biometric identification that would control access to the internet.[27] Contending that cyberspace is not immune from state sovereignty, he argues that 'financial relationships in cyberspace need laws to govern those relationships and transactions', because otherwise, 'any financial relationship established in cyberspace would be tenuous at best and fraught with peril for either side.'[28] This assertion reflects the crucial role of the state in providing the stable institutional arrangements for capitalist relations. As argued in chapter two, states sustain not only the social relations of capitalism but also its complex contractual apparatus and its intricate financial transactions through the provision of an elaborate legal and institutional framework, backed up by coercive force.[29] These transactions are increasingly facilitated through digital means; as we saw in chapter three, the production and circulation of commodities have been profoundly restructured into automated, computer-driven and streamlined systems. Furthermore, data driven finance has entirely transformed the financial industry, making financial transactions completely reliant on digital infrastructures. In the contemporary economy, capital is thus reliant on stable digital technologies. States can only fulfil its role as the guarantor of stability for capitalism by ensuring that virtual spaces belong to some tangible jurisdiction. States are thus 'increasingly required to assert their presence in cyberspace as a matter of national security', and

---

[26] Sauter, 75.

[27] Patrick W. Franzese, 'Sovereignty in Cyberspace: Can It Exist?', *Air Force Law Review*, no. 64 (2009): 1–43. Quoted in Mueller, 'Against Sovereignty in Cyberspace', 782.

[28] Franzese, 'Sovereignty in Cyberspace', 12.

[29] Wood, *Empire of Capital*, 17.

they 'cannot leave cyberspace ungoverned but must find a way to exert their control and authority to reduce their vulnerability.'[30] Franzeses argument emphasizes the need of the state to effectively control its digital space and ties this need directly to financial relationships' increasing reliance on digital technologies. An emphasis on the physicality of cyberspace thus reflects the need of the state to provide stability in the social relations of capitalism in an era where economic life mainly unfolds in the digital sphere.

In a more recent scholarly defense of the 'pure sovereignty' position, Kevin Jon Heller has further detailed these underlying considerations. Contending that the 'pure sovereignty' position is the better position from both a legal perspective and a policy perspective, he asserts that even 'harmless' cyber espionage, which falls below the threshold of prohibited intervention, poses a threat to even the most powerful and technologically sophisticated states. Such espionage can be 'extremely costly', with the theft of intellectual property from American companies alone amounting to hundreds of billions of dollars per year.[31] Insofar as states 'care about international peace and security,' they should therefore endorse the 'pure sovereignty' position.[32] In this view, the effective protection of intellectual property becomes equivalent to international peace and security, demanding a legally binding rule of sovereignty in cyberspace. This view aligns with the evolution in the concept of cybersecurity following from increasing risks of destruction, disruptions, and theft of digital content. As we saw in chapter four, these vulnerabilities have led to a revised notion of cybersecurity centered on the protection of digital infrastructures against external intrusions. Heller's argument thus reflects how the protection of property in the digital space is key to ensuring stability in the social relations of capitalism.

As similar argument is advanced by Schmitt and Vihul. They assert that there is a need for an international legal protection below the threshold of intervention and support this claim with the example of disruptive cyber operations directed against commercial cyber infrastructure in another state intended to give one's own companies a competitive advantage, as well as operations that are 'merely malicious or vindicative'.[33] Characteristic of

[30] Franzese, 'Sovereignty in Cyberspace', 13–14.

[31] Heller, 'In Defense of Pure Sovereignty in Cyberspace', 1491.

[32] Heller, 1494.

[33] Michael Schmitt and Liis Vihul, 'Respect for Sovereignty in Cyberspace', SSRN Scholarly Paper (Rochester, NY, 2017), 1669.

these operations is that they challenge the property relations underlying the capitalist economy, thus causing instability. The absence of a rule of sovereignty would, to Schmitt and Vihul, amount to a cyber 'wild west'.[34] As aptly put by Henning Lahmann, the 'revived focus on the protective dimension of sovereignty is the most visible expression of European and Western states feeling vulnerable to foreign influence and interference in view of the novel possibilities of digital technologies.'[35] The security concerns underlying the 'pure sovereignty' position can thus be understood as *security of property relations*. The position reflects an emphasis on the need for states to guarantee stability in the social relations of capitalism in a time when economic transactions are entirely reliant on digital infrastructures, making them increasingly vulnerable to cross-border digital intrusions. The absence of a rule of sovereignty amounts to the absence of effective enforcement of digital property relations below the threshold of prohibited intervention and use of force. An insistence on a rule of sovereignty in cyberspace allows states to protect digital infrastructure within its territory against external intrusions. States can thereby fulfil their roles as guarantors of stable and predictable conditions for economic transactions.

Emphasizing Freedom: Sovereignty as a Principle

Despite the advantages of a rule of sovereignty in allowing states to guarantee stability and predictability for digitally reliant transactions, the 'pure sovereignty' position has not been unanimously endorsed by states. In particular, the United Kingdom has famously insisted that sovereignty is merely a principle from which legally binding rules are derived. While sovereignty is fundamental to international law, 'we cannot currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention.'[36] The United Kingdom substantiates this claim with reference to a contradiction allegedly emerging between national security and fundamental rights and freedoms.[37] It thus argues against using the doctrine of sovereignty, online or elsewhere, to

[34] Schmitt and Vihul, 1670.

[35] Lahmann, 'On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace', 90.

[36] United Kingdom, 'Cyber and International Law in the 21st Century'.

[37] United Kingdom.

'undermine fundamental rights and freedoms'.[38] Until 2021, the same position was endorsed by the United States, which held that 'it does not appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law.'[39] Given the advantages of a legally binding rule of sovereignty allowing states to guarantee stable and predictable conditions in digital space, why would states like the United Kingdom and the United States advance the 'sovereignty as a principle' position?

A notable academic contribution on the topic helps us elucidate the rationale behind the rejection of a legally binding rule of sovereignty. Asserting that the sovereignty discourse functions as a *metanarrative,* Lahmann argues that 'the idea of the "free and open internet" as a facilitator of a liberal world order represents one of the last remnants of the post-Cold War story of inevitable progress'.[40] He contrasts this position with the '"Westphalian" camp's self-perceived position within the arena of international politics, in particular as it relates to transnational cybersecurity'.[41] While the 'sovereignty as a rule' position (in Lahmann's terminology, the 'Westphalian camp') thus represented the emphasis on security in cyberspace, the 'sovereignty as a principle' position represents an emphasis on the *free and open internet*. The discourse brings associations to the discourse of the neoliberal era of the 1990s. As we observed in chapter four and five, this era saw the development and proliferation of the 'information society' as integral to the global expansion of capitalism into every corner of the globe – an expansion that was deemed inevitable, given capitalism's perceived triumph as the most effective economic system. The 'sovereignty as a principle' position reflects an emphasis on freedom over security, which is deemed instrumental to avoiding that authoritarian regimes carry on denying their citizens basic human rights in the name of sovereignty.[42] The discourse of the 'sovereignty as a principle' position thus emphasizes cosmopolitan freedoms and universalism over stability and security.

---

[38] United Kingdom.

[39] Hon. Paul C. Ney, Jr, 'DOD General Counsel Remarks at U.S. Cyber Command Legal Conference'.

[40] Lahmann, 'On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace', 85.

[41] Lahmann, 85.

[42] Lahmann, 92.

Let us now take a closer look at the freedoms being promoted by the advocates of the 'sovereignty as a principle' within this universalizing narrative. The proponents of this position typically adhere to a liberal, individual-based human right-discourse that celebrates digital technologies in the promotion of freedom of expression, freedom of opinion, and freedom of information.[43] A rule of sovereignty is seen to risk impeding the free flows of information by giving (illiberal) states the sovereign right to control their digital territories. An explication of the link between fundamental freedoms in the digital space(s) and liberal rule is provided by David Kaye, UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression:

> The private sector's role in the digital age appears pervasive and ever-growing, a driving force behind the greatest expansion of access to information in history. Vast social media forums for public expression are owned by private companies. Major platforms aggregating and indexing global knowledge, and designing the algorithms that influence what information is seen online, result from private endeavour. (…) The contemporary exercise of freedom of opinion and expression owes much of its strength to private industry, which wields enormous power over digital space, acting as a gateway for information and an intermediary for expression.[44]

In this view, digital platform corporations are celebrated as the guarantors and facilitators of fundamental freedoms. At the Human Rights Council session in which the Special Rapporteur presented his report, the United Kingdom tellingly responded by expressing an appreciation of freedom of expression and media freedom as a central driver of innovation and economic growth.[45] The response underscores how the fundamental freedoms invoked in justification of the 'sovereignty as a principle' position is intrinsically

---

[43] For a critical view, see Barrie Sander, 'Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-Based Approach to Content Moderation', *Fordham Int'l LJ* 43 (2019): 939.

[44] David Kaye, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (United Nations, 11 May 2016).

[45] 'Working Group on Transnational Corporations and Special Rapporteur on Freedom of Expression' (13th Meeting 32nd Regular Session of Human Rights Council, United Nations Human Rights Council, 16 June 2016).

connected to the protection of the tech industry. Perhaps unsurprisingly, the 'sovereignty as a principle' position has been endorsed and promoted by social platform corporations which have involved themselves in the law-making process, as we observed in chapter five. A Twitter (now X) representative thus urges to consider the notion of sovereignty very carefully to avoid that it will 'overcorrect and act to the detriment of the free and global internet'.[46]

Within this paradigm, the main threat to the realization of these fundamental freedoms is perceived to arise from illiberal states' hostile policies that prevent the tech corporations from doing their magic. Such hostile policies include content filtering, network or service shutdowns, excessive intermediary liability, and state surveillance.[47] States are placing 'undeniable pressures on the private information and communication technology sector that often lead to serious restrictions on the freedom of expression.'[48] As the primary bearers of the responsibility to protect and respect the right to exercise freedom of opinion and expression, states must therefore 'not require or otherwise pressure the private sector to take steps that unnecessarily or disproportionately interfere with freedom of expression, whether through laws, policies, or extralegal means.'[49] The illiberal state is thus perceived as the central threat to the realization of fundamental rights. In other words, the road to the realization of these fundamental freedoms unequivocally goes through the universal adoption of a liberal regulatory framework in the picture of the Global North. In that regard, China's substantiation of the 'sovereignty as a rule' position appears as an exemplary materialization of the liberal fear:

> States have the right to make [information and communication technology]-related public policies, laws and regulations to protect legitimate interests of their citizens, enterprises and social organizations. States should refrain from using [information and communication technologies] to interfere in internal affairs of other States and undermine their political, economic and social stability, or to conduct

[46] 'The Oxford Process on International Law Protections in Cyberspace: A Compendium', 202.
[47] Kaye, 'A/HRC/32/38', 22.
[48] Kaye, 22.
[49] Kaye, 22.

> activities that undermine other States' national security and public interests.[50]

Behind China's preference for the 'rule of sovereignty' position lies a domestic practice of extensive use of laws and technologies to monitor and censor content, often referred to as the Great Firewall of China. These policies are being justified in the language of sovereignty and non-intervention; Chinese President Xi Jinping has emphasized 'the right of individual countries to independently choose their own path of cyber-development,' warning against foreign interference in the internal affairs of other states.[51] The policies and practices of China's illiberal capitalist regime, justified by the 'rule of sovereignty' position, clash with the interests of liberal capitalist states in boundless, free flows of information – and thus also with the boundless export of digital content to Chinese internet users (as well as the concurrent import of their data).

Before we can understand this clash, let me briefly explicate how the 'sovereignty as a principle' position is rooted in the role of the state-system in the reproduction of the social relations of capitalism – a point that I will unfold in more detail below but that deserves mentioning already here. As we saw in chapter three, the business model underlying the 'web 2.0' is reliant on corporations' access to internet users and their data. This also applies to the platform corporations praised as the guarantors of fundamental freedoms online. Platform users' attention to digital content has become a commodity, which platform corporations sell on the basis of a complex algorithmic monitoring. Their business model depends on their access to a market of users in every geographical corner of the globe. When local states invoke their sovereignty to impose restrictions on individuals' access to social platforms, they essentially restrict the free flow of commodities on which global capitalism relies. Let us now turn to explore how the clash between the two positions on digital sovereignty plays out in states' policies, as illustrated by recent polemics around Chinese and American internet policies.

While China's 'sovereignty as a rule' position prioritizes sovereign control and restriction of external influence over free flows of information, it is

---

[50] China, 'China's Positions on International Rules-Making in Cyberspace', 20 October 2021.

[51] Elizabeth C. Economy, 'The Great Firewall of China: Xi Jinping's Internet Shutdown', *The Guardian*, 29 June 2018, sec. News.

notable that many Chinese platforms are just as dependent on global access to users as their Western counterparts. The success of TikTok, owned by the Chinese company ByteDance, illuminates a tension in the American celebration of the free flow of digital content underlying the 'sovereignty as a principle' position.[52] 16.75% of TikTok's users are from the United States, making the platform's growth reliant on access to American audiences.[53] While the United States generally champions free global flows of content and commodities of 'its' platform corporations as quintessential to freedom of expression and the liberal international order, TikTok's popularity amongst American citizens has been conceived as concerning from the perspective of 'national security'.[54] Caught between a rock and a hard place, the United States passed a law in 2024 that required ByteDance to sell the app to a buyer from the United States or one of its allies.[55] This dynamic underscores a key contradiction: *On the one hand*, the United States advocates for the free export of its own digital content and services as intrinsic to freedom of expression and information. *On the other hand*, it resists unrestricted imports of Chinese platforms, which are seen as a threat to American control over digital infrastructure and data flows. It is notable that the United States's attempt to resolve the national security threat lies in moving (part of) the corporate ownership over TikTok to a tech corporation located the United States or its allies. Such a solution presupposes that corporate power located in the Global North is a guarantor of national security. In turn, China's policies seek to expand its digital exports, like TikTok, while shielding its domestic digital ecosystem from foreign influence. Ultimately, the two states are thus facing parallel dilemmas between expansion and control – the central difference between the two being that China's priority appears to lie more decisively on the latter rather than the former.

---

[52] Even though the United States has moved away from the 'extreme' sovereignty as a principle position, it remains somewhere on the scale that is certainly closer to the United Kingdom than to China. See the most recent American position in GGE compendium of voluntary contributions, 'GGE Compendium of Voluntary Contributions'.

[53] 'How Many Users on TikTok? Statistics & Facts (2025)', accessed 21 January 2025, https://seo.ai/blog/how-many-users-on-tiktok.

[54] Clare Duffy and David Goldman, 'Trump Signs Promised Executive Action to Delay TikTok Ban for 75 Days', *CNN*, 20 January 2025.

[55] Duffy and Goldman.

By interpreting sovereignty as a principle, emphasis is put on the importance of the protection of liberal individual freedoms from state intervention over states' sovereign freedom to regulate their 'national digital space'. The position marks a continuation of the historical trajectory of sovereignty in which sovereignty long remained contingent the adoption of a capitalist regulatory framework and, when sovereignty was universalized, was contingent on the imposition of a liberal right-based regulatory framework.[56]

Seen in this light, the position of the African Union on digital sovereignty provides a notable pushback against this liberal discourse. Embracing a 'pure sovereignty' position, the African Union criticizes the attempt at establishing a threshold of harm that reduces the protective scope of the rule of sovereignty:

> Given the vast disparities of technical capabilities between States, such rules would, as noted by the International Court of Justice in the Corfu Channel Case, "from the nature of things, be reserved for the most powerful States," which could give rise to serious abuses that would undermine the principles of the independence and sovereign equality of States.[57]

The African Union thus motivates a binding rule of sovereignty with the blunt observation that the permission of a certain level of digital interference inevitably perpetuates unequal power dynamics on the basis of states' diverging capacities. In other words, the African Union expounds how the abstract sovereign equality of states shields over their underlying material inequalities.[58]

Let me end this section by returning to the fundamental freedoms typically invoked in justification of the 'sovereignty as a principle' position. When advocates of the position emphasize freedom of expression and information, they often disregard how the privatized structure of the internet allows near-complete corporate control over digital content. As I argued in

---

[56] Tzouvala, *Capitalism As Civilisation*; McKenna, *Reckoning with Empire*.

[57] African Union Peace and Security Council, 'Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace', 29 January 2024.

[58] I owe this point to Henning Lahmann.

chapter three, private corporations monitor what content we are exposed to. Internet users' attention to content has become a commodity, which is owned, managed, and sold by social media platform corporations on the basis of profit-driven algorithmic control and opaque content moderation policies. Individuals in today's digital sphere have, as Barrie Sander emphasizes, 'little choice but to participate on online platforms, whose design choices shape what is possible, content policies influence what is permissible, and personalization algorithms determine what is visible.'[59] Online platforms are used every day by billions of people to express themselves through virtual debates, to search information, create and share content and views.[60] In this contemporary data economy, the power of the platform corporations follow from their control over a wide range of resources crucial to information search and public participation in the online realm.[61] Under the guise of freedom of information, the 'sovereignty as a principle' position ultimately protects the free global flows of commodities, including data and attention to digital content.

These tendencies are causing increasing concerns that 'platform moderation is being driven to a significant extent by corporate imperatives for growth and profit at the expense of the public interest.'[62] Barrie Sander emphasizes the importance of identifying 'a way to re-align the private incentives of platform governance with the broader public interest.'[63] While he is obviously right to point to the extant contradictions, his call for a regulatory re-alignment of interests only distracts us from the fact that the task is impossible: as we saw in chapter three, the conflicting interests around digital platforms are *profound*. If there can be said to exist such thing as a 'broader public interest' in the context of platform governance, it would thus lie in the dismantling of the power of the corporate governors of platforms. Plainly, this goal cannot possibly be aligned with the incentives of the governors.

---

[59] Sander, 'Freedom of Expression in the Age of Online Platforms', 939.

[60] Rikke Frank Jørgensen, 'Human Rights and Private Actors in the Online Domain', in *New Technologies for Human Rights Law and Practice*, ed. Jay D. Aronson and Molly K. Land (Cambridge: Cambridge University Press, 2018), 244.

[61] Jørgensen, 243.

[62] Sander, 'Freedom of Expression in the Age of Online Platforms', 942.

[63] Sander, 942.

By only identifying the illiberal state as the threat to the exercise of fundamental freedoms, the 'sovereignty as a principle'-position disregards how the corporate control over and commodification of social life is, in itself, profoundly impeding freedom. I discuss possible paths ahead for those seeking emancipation from these structures in chapter seven. Here, it suffices to underscore that such emancipatory ends are by no means achieved through a 'sovereignty as a principle' position. The position merely reflects a priority of the expansion of liberal rule to uphold the global circulation of capital.

Middle Way: Relative Sovereignty

Between the 'pure sovereignty' position and the 'sovereignty as a principle' position lies a middle way: The 'relative sovereignty' position, which enjoys broadest support amongst states. The 'relative sovereignty' position refuses to reduce sovereignty to a principle but insists that not any digital intrusion violates a state's sovereignty. According to the 'relative sovereignty' position, a low-intensity cyber operation is only internationally wrongful if it causes some kind of harm to the territorial state or interferes with or usurps one of its inherently governmental functions.[64] States such as Austria, Canada, Germany, New Zealand, and Czech Republic highlight the requirement of a certain level beyond 'negligible' or *de minimis* effects before the rule of sovereignty is triggered.[65] They thus agree that sovereignty applies as a rule in cyberspace but that some activity falls below the threshold. Czech Republic emphasizes that cyberspace is a 'global and open domain' and that states often exercise their jurisdiction in another state's territory without legal repercussions, suggesting that cyber activities only constitute a violation of the rule of sovereignty above a certain threshold, thus bringing the liberal discourse of globalization and openness into the rule of sovereignty.[66] Some states give indications as to where the threshold of sovereignty lies. For example, New Zealand hold that there is a 'range of circumstances – in

[64] Heller, 'Low-Intensity Cyber Operations and State Sovereignty in Cyberspace', 28.
[65] Canada, 'International Law Applicable in Cyberspace'; Germany, 'On the Application of International Law in Cyberspace'; New Zealand, 'The Application of International Law to State Activity in Cyberspace'; Czech Republic, 'Position Paper of the Czech Republic on the Application of International Law in Cyberspace', 1 March 2024.
[66] Czech Republic, 'Position Paper of the Czech Republic on the Application of International Law in Cyberspace'.

addition to pure espionage activity – in which an unauthorised cyber intrusion, including one causing effects on the territory of another state, would not be internationally wrongful.'[67] To Canada, 'territorial sovereignty is not violated by virtue merely of remote activities having been carried out on or through the cyber infrastructure located within the territory of another State', thus ensuring a room for maneuver in digital space across geographical territory. Meanwhile, Canada also mentions the disruption of economic and societal activities as factors to take into account in the assessment of whether a violation of the territorial sovereignty of the affected state has taken place, thus emphasizing the value of stability in social relations.[68] As such, the states placing themselves somewhere in between the 'pure sovereignty' position and the 'sovereignty as a principle' position appear interested in allowing for the free flow of information, while preserving their right to protect their digital territories from the cyber operations that are deemed severe. Often, it is emphasized that the threshold must be assessed on a case-by-case basis, thus giving a certain flexibility in the application of the rule of sovereignty in cyberspace to specific scenarios.[69]

These positions somewhere on the middle way between 'pure sovereignty' and 'sovereignty as a principle' reflect an attempt to resolve the tension around sovereignty arising from the fact that both of the 'extreme' positions respond to an essential role that states must fulfill for a functioning capitalist economy. The attraction of this middle- way position can thus be understood as an attempt to ensure an interpretation of international law that reconciles the roles of the state-system in contemporary capitalism. I will explore this tension in further detail in the subsequent section.

---

[67] New Zealand, 'The Application of International Law to State Activity in Cyberspace'.

[68] Canada, 'International Law Applicable in Cyberspace'.

[69] Ministry of Defense of France, 'Perspective of France'; Finland, 'International Law and Cyberspace - Finland's National Positions'; New Zealand, 'The Application of International Law to State Activity in Cyberspace'; Finland, 'International Law and Cyberspace - Finland's National Positions'; Canada, 'International Law Applicable in Cyberspace'; Engdahl, 'Sweden's Position Paper on the Application of International Law in Cyberspace'; Kjelgaard and Melgaard, 'Denmark's Position Paper on the Application of International Law in Cyberspace'; Switzerland, 'Switzerland's Position Paper on the Application of International Law in Cyberspace (Annex to the United Nations Group of Governmental Experts 2019/2021)'.

The Tension around Sovereignty

Based on this detailing of the considerations underlying the 'pure sovereignty' position and the 'sovereignty as a principle' position, which are sought reconciled in the 'relative sovereignty' position in between, it is possible to root the prevalent ambiguity surrounding digital sovereignty in the material basis. I will argue that the ambiguity reflects a general tension in international law. This tension appears, at first, simply as a reflection of a general dichotomy between state sovereignty and fundamental freedoms.[70] Within this dichotomy, too much emphasis on sovereignty is seen to collide with some 'cosmopolitan human rights law', while too much emphasis on freedom is seen to pose a security risk.[71] However, as I aim to show, the dichotomy is more accurately conceptualized as a tension in the role of the capitalist state. The dichotomy between sovereignty and 'cosmopolitan freedoms' thus strikingly reflects another dichotomy that we have seen before in this dissertation: *On the one hand*, the need of the state to ensure stability and reliability in the social relations of capitalism and, *on the other hand*, the need of the state to facilitate the constant expansion of capitalism.

The *former* consideration is underlying the 'pure sovereignty' position, allowing states to ensure a stable and secure digital sphere through the effective enforcement of property relations reliant on digital infrastructure. As we saw in chapter four and five, the field of international cyber law has been delineated around a notion of 'cybersecurity', which has taken shape around a particular set of ideas about what needs protection and what constitutes a threat. The contemporary notion of cybersecurity thus perceives cybersecurity as tantamount to stable and reliable conditions for technology systems, whereas the risk of external intrusions carried out by states or none-state actors constitute a security threat. As information technologies have been vital tools in the global expansion of capitalism, the reproduction of capitalism is entirely reliant on the stability and reliability of digital systems. These

---

[70] This understanding is reflected in the reasoning of the United Kingdom. United Kingdom, 'Cyber and International Law in the 21st Century'. See also Justin Conlon, 'Sovereignty vs. Human Rights or Sovereignty and Human Rights?', *Race & Class* 46, no. 1 (2004): 77.

[71] Jean L. Cohen, 'Whose Sovereignty? Empire Versus International Law', *Ethics & International Affairs* 18, no. 3 (2004): 2; Conlon, 'Sovereignty vs. Human Rights or Sovereignty and Human Rights?', 79.

considerations point to the need of effective state protection of digital infrastructure against external intrusions.

The *latter* consideration is underlying the 'sovereignty as a principle' position, allowing the global flows of capital and commodities even if at variance with the policies of (illiberal) states, thus enabling the expansion of digitally reliant markets into every corner of the globe without interventions from states. As we saw in the introduction, capital is not a thing, but a process; namely, the process of putting money into circulation to make more money.[72] This process entails an inherent strive for expansion into new terrains.[73] The reproduction of capitalism thus requires states to establish the conditions needed to sustain this expansion whenever these conditions are not already in place. As we saw in chapter four, the endeavor to seek out new terrains for capital motivated the expansion of the 'information superhighway' into new geographical corners. Quoting Hansen and Nissenbaum, the 'modern economic system is, like the cyber network, constituted by trans-border flows, and authority and sovereignty is more ambiguously located than in traditional national-military security.'[74] From this perspective, a rule of sovereignty risks impeding the transborder flows of capital on which the modern economy is deeply dependent. The attempt to align the interpretation of sovereignty in cyberspace with capital's expansive tendency thus continues the historical trajectory in which sovereignty has been conditioned on the establishment of a regulatory framework favorable for capital.

* * *

While sovereignty is a foundational concept in international law, its meaning and nature has always been controversial. In recent years, the emergence of cyberspace has given rise to renewed debates, dividing states and legal scholars. I have argued that the prevalent ambiguities surrounding the concept can be understood in light of the changes in the capitalist economy brought about with the rise of information technologies. Global flows of capital must be both facilitated and protected for capitalism to function. We can thus understand the ambiguities surrounding digital sovereignty as a

[72] Harvey, 'The Enigma of Capital and the Crisis This Time'.

[73] Marx, *Grundrisse*, 524.

[74] Hansen and Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', 1162.

manifestation of a dual imperative of the capitalist state: It must, *on the one hand*, ensure the stability and reliability for capitalist social relations through the effective protection of digital property. It must, *on the other hand*, facilitate the free flow of capital to enable its continuous expansion. The need to ensure stability and reliability calls for strict control with 'national digital territory', which translates into an emphasis on sovereignty as a rule. The need to facilitate the free flow of capital and enable its continuous expansion demands a limit to states' sovereign right to control their digital territory to avoid the doctrine of sovereignty being used to justify illiberal policies that impede capital expansion. The problem for capitalism? Plainly, it needs both. For that reason, it remains an unsettled question which interpretation the advanced capitalist states will ultimately prefer – and the status of the concept of sovereignty in cyberspace remains ambiguous.

CHAPTER VII
ANOTHER CLOUD IS POSSIBLE

In my experience, critical interventions into international law often provoke a familiar and pointed question from certain scholars – especially from the positivists, those who are participating in what Andrea Bianchi calls the 'game of international law': *But what's the alternative?* Concretely, if *our way* of playing the game merely upholds relations of domination and exploitation, then what does *your way* look like? Within these critique-skeptical questions often lies an implicit proposition that an imperfect system is better than no system – and that working constructively to improve that system is better than merely critiquing it. Critical legal scholarship's tendency to refrain from engaging with questions of emancipation and post-emancipatory realities has sometimes given rise to a critique that this body of scholarship is largely irrelevant to social movements and individuals struggling for emancipation. As Naz K Modirzadeh writes it in a recent critique of the Third World Approaches to International Law (TWAIL) movement:

> [I]t is … extremely difficult to "use" TWAIL scholarship politically or programmatically. Without such a programmatic vision of what a just, moral international order would look like, those seeking to reform international law according to TWAIL's commitments are left with little guidance.[1]

---

[1] Naz K. Modirzadeh, '"Let Us All Agree to Die a Little": TWAIL's Unfulfilled Promise', *Harvard International Law Journal*, 2023, 90.

This objection, which could easily apply to the Marxist tradition of international legal scholarship as well, gives rise to the important question of what role international law(yers) can play in a struggle for emancipation. When confronted with such questions, my usual reaction has been to conform to a traditional Marxist refusal of writing recipes for the 'cookshops of the future', emphasizing the intrinsic value of critique – that it is not necessarily the role of critical scholarship to chart a clear path toward a post-emancipatory order, nor to provide blueprints for utopias.[2] The critical diagnosis is valuable in and of itself.

However, such a rejection of engaging with questions of emancipatory strategies and ends is dissatisfactory in a number of ways. Questions about where the critical diagnosis leaves individuals and social movements who struggle for change are important not only because the different attempts to exercise resistance make a crucial part of the story, but also because our answers to these questions illuminate and strengthen the critique itself. Pointing to possible alternative digital futures may elucidate the historical contingency of the current technological landscape. Furthermore, an examination of international law's emancipatory potential may elucidate – in ways that are not always clear in the critical analysis of *lex lata* – how the legal form itself constrains the possible legal outcomes.

This final chapter is therefore an attempt to confront some of these questions within the realm of international cyber law. If my arguments in the preceding chapters are correct, then international cyber law is currently taking shape to sustain the reproduction of capitalism in an era where capital accumulation is increasingly relying on stable and predictable global digital infrastructures. The present chapter turns away from this deconstructive endeavor and asks, instead, how international cyber law positions those who seek emancipation from the exploitative dynamics underlying the information technology landscape. As such, the chapter also moves beyond the research question that has guided the preceding chapters, offering instead some reflections on possible paths ahead of us. While I will not pretend to provide any definite answers, I hope to contribute to an ongoing conversation – one that insists on imagining that critical endeavors of various kinds may, eventually, lead to material change. Central to the Marxist lens through which this dissertation has been written is the insistence that every

[2] Karl Marx, 'Preface to the Second Edition', in *Capital: A Critique of Political Economy, Vol. 1*, by Karl Marx, Penguin Classics (London: Penguin in association with New Left Review, 1990).

social form is historical. This insistence implies that existing systems of domination are specific to the current era and thus by no means natural. It follows from the historical specificity of social forms that existing systems are reversable. In that spirit, I begin this chapter by diving into the question of alternative digital futures, exploring past, present and imagined attempts at constructing another digital landscape than the current one. I then turn to discuss the possible role of international cyber law in struggles for emancipation, bringing general debates on international law's emancipatory potential to live by illuminating what radical strategies of advocacy might look like in the context of international cyber law. Concluding that material change must ultimately precede legal change, I turn to explore existing attempts at exercising resistance against the digital landscape through disruptive cyber operations. I conclude the chapter by suggesting what role international legal scholarship can play in a struggle for emancipation.

Emancipatory Ends

In mainstream discourse, the term 'digital revolution' is often invoked to describe the major technological advancements of the past half century. The revolutionary narrative typically celebrates breakthroughs in connectivity and automation as inherently transformative and liberatory forces. However, as should now be clear, the so-called digital revolution is better understood as a counterrevolution. The technological advancements of this era are profoundly shaped by the social relations of capitalism from which they have emerged. Rather than disrupting existing power structures, digital technologies have served to exacerbate and expand them. They have enabled the standardization, concentration, and monopolization of critical infrastructures and the commodification of nearly every aspect of human life. They have aggravated existing inequalities, intensified the vulnerability and precarity of life for the working class, and contributed to an ecological deterioration of the planet through unsustainable resource extraction and accelerating energy consumption. There is thus nothing remotely revolutionary about the current information technology landscape.

By making this claim, I do not mean to sound pessimistic about technologies *as such*. As I argued in chapter three, humans cannot survive without technologies; humans are a 'tool-making animal'.[3] There is therefore nothing inherently problematic about technological development. The central

[3] Marx, *Capital: A Critique of Political Economy. Volume One*, 286.

problem arises from the economic system out of which the current information technology landscape has arisen.[4] In other words, the problem is not technology, but *who* technology serves and for *what* purposes.[5]

In the shadows of the mainstream technophile celebrations of the brilliant minds of Silicon Valley's jeans-wearing elite, various alternative visions have been formulated for what the 'information society' could look like. The question we should ask is, as Liam Mullaly puts it, ultimately one of social relations: how do we want to organize ourselves?[6] The precise contours of a democratic digital landscape can only be discovered through a truly democratic process.[7] Yet, a few reflections on what alternative digital futures could look like in a society that is liberated from the imperatives of capital are useful, both as a counterpoint to the prominent deterministic universalization of the existing digital landscape and as an elucidation of possible emancipatory ends. In the endeavors to imagine possible digital landscapes of the future, it might be helpful to dive into real attempts at building an alternative digital architecture. I therefore begin in the following with an exploration of one past and one present example of such attempts. I then turn to engage with utopian visions of possible technological futures.

Throughout the short time that information technologies have existed, Project Cybersyn stands as an important, yet often-forgotten tale from the early information age which holds some important lessons for us today.[8] Project Cybersyn was an ambitious initiative in 1970s Chile under Salvador Allende's government. The aim of the project was to build a digital infrastructure designed not for profit maximization but for economic planning. By creating a real-time computer network linking the nationalized factories to a central command in Santiago, the architects envisioned information technology as a key tool in socialist economic planning.[9] In sharp contrast to the imperatives shaping the information technology landscape of capitalist society, which we explored in chapter three, Project Cybersyn aimed to use information technology to create a new relationship between industry

---

[4] Mueller, *Breaking Things at Work*, 7.

[5] Doctorow, *The Internet Con*, 1; Liu, *Abolish Silicon Valley*.

[6] Liam Mullally, '"We Do Not yet Know What a Network Can Do": Steps to a Collective Internet', *The Autonomy Institute* (blog), 2024.

[7] Tarnoff, *Internet for the People*, xvi.

[8] Casper Skovgaard Petersen, 'The Death of Cyber Socialism', *Farsight* (blog), 2024.

[9] Eugene van der Watt, 'Project Cybersyn: The Socialist Internet That Almost Was', Versus, 2024.

and government by allowing the government to monitor real-time industrial production data. Rejecting top-down organizational structures, the project used feedback systems to distribute information and decision-making authority. The idea was to use information technology to allow for everyone to participate in a people-driven socialism.[10]

Project Cybersyn was never integrated fully into Chilean political or economic life, and it was brutally destroyed after the United States-backed coup in 1973, when an authoritarian military government came in place. The basic designs of Cybersyn, structured around economic planning and public participation, made no sense in the context of the new military government.[11] Despite its relatively short life, project Cybersyn gives us a sense that it may be possible to design technologies around a fundamentally different set of societal needs than what is the case under capitalism. The project thus underscores how technological designs reflect historically specific modes of production. Not only is the current information technology landscape by no means natural or uncontestable, but alternative digital futures are also possible in a society characterized by a different mode of production.

Moving from the past to the present, attempts do exist at building alternatives to the otherwise dominant market-driven information technology landscape. We may follow Erik Olin Wright in thinking of these initiatives as 'real utopias' – that is, real emancipatory alternatives to dominant institutions and social structures.[12] The concept of 'the digital commons' serves as a framework for the idea of digital resources being shared by a community instead of being owned by private entities.[13] It denotes a movement towards the development of free and open source software (FOSS) – a category of software that anyone is free to use, modify and distribute without compensating the original developer.[14] The perhaps most striking example of such 'real utopia' is the free online encyclopedia, Wikipedia.[15] Not only is the software that powers Wikipedia open source, but more importantly, all of

---

[10] See Eden Medina, *Cybernetic Revolutionaries: Technology and Politics in Allende's Chile* (Cambridge, Mass: MIT Press, 2011).

[11] Medina, 211.

[12] Erik Olin Wright, 'Real Utopias', *Contexts* 10, no. 2 (2011): 37; Erik Olin Wright, *Envisioning Real Utopias* (London & New York: Verso, 2020).

[13] Benjamin J. Birkinbine, *Incorporating the Digital Commons: Corporate Involvement in Free and Open Source Software* (London: University of Westminster Press, 2020).

[14] Fahad Desmukh, 'Imagining a Socialist Internet', *TRT World* (blog), 2018.

[15] Wright, 'Real Utopias', 40.

its articles are written by volunteers and can be freely copied, enhanced, and shared by anyone without anyone making profit.[16] Quoting Wright:

> Wikipedia is a profoundly egalitarian, anti-capitalist way of producing and sharing knowledge. It is based on the distributive principle "to each according to need, from each according to ability" and organized around horizontal reciprocities rather than hierarchical control. And, in less than ten years, it's basically destroyed the commercial encyclopedia market that had existed since the 18th century.[17]

FOSS technologies give us a glimpse of what a non-commercial digital landscape could look like, helping us to envision alternatives to the otherwise profit-driven technological landscape. Importantly, I am not pointing to FOSS technology to argue that emancipation can happen by appealing to the hearts and minds of the owners of critical software to share some of their valuable ownership with the masses. As 'real utopias', FOSS technologies remain important exceptions to a reality dominated by the imperatives of capital. Emancipation will not arise out of the good will of the capitalist – not because capitalists are bad persons, but because capitalism compels everyone to follow the logics of the market to survive, which entails putting profit above all other considerations.[18] The possibility for building a comprehensive digital alternative thus remains extremely limited within the current political economic reality. What these glimpses can give us is rather a more substantial idea that the digital landscape could look very different from what it does today. Despite these glimpses, a long path remains towards comprehensive emancipation.

Let us therefore turn from these past and present examples of alternative digital infrastructures and look at the future. Several scholars have asked how we can imagine a digital landscape in a future society in which the capitalist mode of production is replaced by an economic system in which the means of production are collectively owned. In these utopian visions, information technologies have sometimes been envisioned as the key to societal prosperity in a technophile spirit that almost resembles the atmosphere in Silicon Valley. The archetypical example of such radical utopian techno-optimism is Aaron Bastani's vision of a 'fully automated luxury communism'

[16] Desmukh, 'Imagining a Socialist Internet'.
[17] Wright, 'Real Utopias'.
[18] Wood, *Empire of Capital*, 10–11.

in which automation will liberate humans from work, new technologies thus making up a path to a world of liberty, luxury and happiness.[19] While Bastani's account has been properly criticized for ultimately offering little more than a reformist variant of the mainstream techno-determinism of our time, thus lacking any consciousness about class or systematic consideration about capitalism, other waves of radical thought have offered rigorous reflections about how information technologies might assist in the future planning and organization of work.[20] As was foreseen by the Allende government, information technologies hold an immense potential to assist in the task of planning production under socialism.[21] By providing the technological tools for detailed planning, information technologies could serve as a cornerstone in the coordination and organization necessary in any society. As Leigh Phillips and Michal Rozworski have argued, algorithmic centralized economic planning is already in place under capitalism, in which the increasing monopolization of retail entail that singular corporations like Walmart and Amazon are facilitating the nation-wide planning of production of everyday goods.[22] These vast planning models characteristic of high-tech monopolized retail are ironically argued to pave the way for the realization of a socialist model of planning.[23] Relatedly, Saros proposes a decentralized system that retains some aspects of the price mechanism, but which replaces key functions with digital 'feedback infrastructure.'[24] In this view, digital technologies are key to running a planned economy. Algorithms can take in information on consumer preferences and industrial production capacities and translate it into the optimal allocations of resources.[25]

---

[19] Aaron Bastani, *Fully Automated Luxury Communism* (London & New York: Verso, 2019).

[20] Pedro HJ Nardelli et al., 'Cyber-Physical Decentralized Planning for Communizing', *Competition & Change* 29, no. 1 (2025): 121–38; Evgeny Morozov, 'Digital Socialism?', *New Left Review*, no. 116/117 (2019): 33–67.

[21] Nardelli et al., 'Cyber-Physical Decentralized Planning for Communizing', 127.

[22] Leigh Phillips and Michal Rozworski, *The People's Republic of Walmart: How the World's Biggest Corporations Are Laying the Foundation for Socialism* (London & New York: Verso, 2019).

[23] Phillips and Rozworski.

[24] Daniel Earl Saros, *Information Technology and Socialist Construction: The End of Capital and the Transition to Socialism* (Routledge, 2014).

[25] Aaron Benanav, 'How to Make a Pencil', *Logic(s) Magazine*, December 2020.

Yet, as several scholars have correctly emphasized, such digitally automated planning also come with the risk of technifying inherently political matters.[26] As Benanave notes, algorithmic planning risks 'constraining the decision-making processes of a future socialist society to focus narrowly on optimization: producing as much as possible using the fewest resources.'[27] Planning remains an inherently political question which cannot be reduced to an algorithmic task. While there is hardly any way around digital technologies playing some role in the construction of a socialist society, their specific role needs to be clarified:

> We do not want software to substitute for the price mechanism. No matter how digitally mediated a socialist society becomes, it will never be able to escape the need for democratic deliberation at all levels. Human beings are never simply rule followers. They look beyond the rules, sometimes for social benefit, sometimes for personal advantage, and often for both.[28]

A better direction than a Walmart-like model of centralized planning is, as Nardelli et. al. propose, a 'decentralized planning constructed as a cyber-physical system to jointly manage supply and demand, including aspects related to production and circulation, without the mediation of money.'[29] In their vision, information technologies are deployed for communizing, rather than centralizing planning.[30] Even if we reject the idea of algorithmic centralized planning – of technologies essentially replacing the price-mechanisms of capitalism – there appears to be an essential need for coordination of work, and information technologies in some form are part of the facilitation thereof in one form or another.

The question of how the technological landscape should be restructured in a post-capitalist reality would ultimately be the result of a real democratic process, and definitive answers to the complex questions touched upon in

---

[26] Benanav; Morozov, 'Digital Socialism?'; Nardelli et al., 'Cyber-Physical Decentralized Planning for Communizing'.

[27] Benanav, 'How to Make a Pencil'.

[28] Benanav.

[29] Nardelli et al., 'Cyber-Physical Decentralized Planning for Communizing'. The theoretical framework, including the concept of cyberphysical systems, is developed in Pedro H. J. Nardelli, *Cyber-Physical Systems: Theory, Methodology, and Applications* (Hoboken: John Wiley & Sons, 2022).

[30] Nardelli et al., 'Cyber-Physical Decentralized Planning for Communizing', 128.

this section exceeds the purpose of this dissertation. Here, I merely want to raise the point that information technologies are not *per se* in opposition to a post-capitalist future. Past, present, and utopian examples suggest that some aspects of information technology could be adapted to suit societal needs of a post-capitalist world. Yet, the information technology landscape would be profoundly restructured around a different set of societal needs, essentially focused on collective ownership and participation rather than private property. The insight that the problem is not technology, but the underlying social relations, underscores the need for an analytical separation of technology as such from the current information technology landscape, and to analyze the *former* as a part of human nature and the *latter* as a reflection of the social relations of capitalism. For the purpose of this chapter, the key point is that alternative digital futures are possible. On the basis of these propositions, we have come to discuss the possible role of international law in a struggle for emancipation.

International Law's Emancipatory Potential

Alternative digital futures are possible, but how is it possible to get there? And what role, if any, can international cyber law(yers) play in a struggle for emancipation? In general, non-cyber-specific terms, the debate over international law's emancipatory potential is long-standing. Some scholars argue that capitalism's foundational structures are so deeply embedded in the legal form that emancipation requires an abolition of this form.[31] Others argue that the content of international law is contestable and that progressive actors may force states to adopt an interpretation that favors progressive interests.[32] Before diving into the question of the emancipatory potentials of international *cyber* law, it is useful to revisit the central arguments underlying these general positions.

Proponents of international law's emancipatory potential often point to its indeterminacy as holding the key to emancipation. As we saw in chapter one, international law's indeterminacy means that every legal doctrine is

---

[31] Miéville, *Between Equal Rights: A Marxist Theory of International Law*. See also Pashukanis, *Law and Marxism*., who argues that law will 'wither away' once capitalism is abolished. See further Fernando Quintana, 'On the Withering Away of Law: Radical Politics Beyond Legal Fetishism', *Legal Form* (blog), 2024.

[32] Marks, *The Riddle of All Constitutions*; Robert Knox, 'Marxism, International Law, and Political Strategy', *Leiden Journal of International Law* 22, no. 3 (2009): 413–36.

entirely reversible – no self-contained legal logic can determine what becomes rules and what becomes violations. While international law can serve to stabilize oppression and obstruct emancipation, it can also serve as a vehicle for progressive change; as Susan Marks puts it, 'indeterminacy is at one level international law's weakness, at another its greatest strength.'[33]

In contrast, Miéville, asserts that the radical indeterminacy of international law does not entail a window of opportunity for progressive actors to push for alternative interpretations; rather, the stronger force in the underlying social relationship will have the power to determine the interpretative outcome:

> This is why strong states are able to enforce their own interpretation of law. Intrinsically to the legal form, a contest of coercion occurs, or is implied, to back up the claim and counterclaim. And in the politically and militarily unequal modern world system, the distribution of power is such that the winner of that coercive contest is generally a foregone conclusion. *The international legal form assumes equality and unequal violence.*[34]

The use of international legal arguments in struggles against prevalent injustices arising from the underlying material relations of inequality are thus inherently hopeless; following Miéville, one can hope, at best, for 'occasional victories in a constant struggle over categories.'[35] I find Miéville's argument overall compelling; there are important limitations to the emancipatory potential of international law, arising in part from the legal form and in part from the social relations that give law its content. However, I also think that scholars such as Knox, Miéville, and Marks are right to point out that Miéville's crude rejection of international law's emancipatory potential misses some nuances. Looking into these scholarly contestations will help us get a better idea of the precise limitations to international law's emancipatory potential.

Knox and Chimni both argue for a broader conceptualization of international legal personality than what is found in Miéville's theory. States, Knox suggests, are not necessarily the primary actors in international law, and progressive actors may be able to constitute themselves as legal

---

[33] Marks, *The Riddle of All Constitutions*, 144.

[34] Miéville, *Between Equal Rights: A Marxist Theory of International Law*, 292.

[35] Miéville, 304.

subjects.[36] Chimni further asserts that there is no reason why the 'practice' making customary international law cannot include the practice of social movements. Non-governmental organizations have increasingly become agents of lawmaking in the international legal order, even if their 'practice' is not currently counted to determine whether a rule of customary international law has emerged.[37] He thus argues for a postmodern doctrine of customary international law, linking its formation to progressive ideas, beliefs, and practices in the global civil society.[38] Similar points about the role of non-state actors in international law, which arguably make a corrective to Miéville's conceptualization of the legal form, have been raised by international legal positivists. In *The International Legal Personality of the Individual*, Astrid Kjeldgaard-Pedersen demonstrates empirically that the international legal personality of an entity is solely dependent on the existence of an international norm directed at it. In other words, there appears to be no conceptual impediments to governing individuals and other non-state actors directly by international law.[39] Some positivist scholars go even further and claim that individuals have a right to international legal personality.[40]

However, even if we accept an argument that social movements may be recognized as international legal subjects, how does such recognition position those seeking emancipation through international law? If the argument is that international legal subjectivity is an emancipatory goal in itself, then the argument is lacking any sense of material rooting. Such an idealistic claim is certainly not the intention of Chimni and Knox. As Knox acknowledges, the recognition of social movements as legal subjects is not sufficient to prove the emancipatory potential of international law: Even if progressive forces are recognized as international legal subjects, international law will only be turned to their ends if they are able to make their particular interpretations 'stick'.[41] The power to determine legal outcomes thus remains in the hands of advanced capitalist states insofar as they possess the greatest

---

[36] Knox, 'Marxism, International Law, and Political Strategy', 418.

[37] Chimni, 'Customary International Law', 42.

[38] Chimni, 42.

[39] Astrid Kjeldgaard-Pedersen, *The International Legal Personality of the Individual* (Oxford: Oxford University Press, 2018).

[40] Anne Peters, *Beyond Human Rights: The Legal Status of the Individual in International Law*, Cambridge Studies in International and Comparative Law (Cambridge: Cambridge University Press, 2016).

[41] Knox, 'Marxism, International Law, and Political Strategy', 423.

capacity for violence.[42] The recognition of the international legal personality of individuals thus merely disproves a claim that the legal form excludes individuals from influencing international law's content already by way of their lacking international legal personality. As will become clear when we attempt to formulate emancipatory arguments within the framework of law, the legal form reveals itself as containing another significant limitation to change – one that arises from its structure around property ownership. However, before we explore the limitations arising from the legal form in our endeavor to develop emancipatory arguments, let us turn to look at the limitations arising from the dynamics of the social relations that are expressed in the content of international law.

As mentioned above, Miéville holds that a contest of coercion occurs to back up the claim and counterclaim, and that the legal interpretation that manages to 'stick' is the interpretation promoted by the winner of that coercive contest. Miéville has been criticized for simplifying the forms of coercion involved in this contest, focusing excessively on war and military coercion and overlooking the prominent usage of economic sanctions in international law.[43] Relatedly, Marks objects that not all outcomes are assimilable to a single logic; if force decides, 'it does not do so always and ever in the same way.[44] Of course, Knox and Marks are correct to assert that Miéville's conception of the real dynamics shaping states' interpretative choices are inadequate. As I argued in chapter two, Miéville's reliance on a Leninist view of imperialism is insufficient to explain the complex dynamics in the relations between states giving content to international law. But crucially, even accepting these nuances, international law remains merely *reactionary* to a change in the underlying forces. As Knox puts it:

> [P]rogressive forces often wield a great deal of economic power internal to the bourgeois state (and internationally). It is possible to imagine a situation in which a pattern of economic "sabotage", strikes, and so on by these actors could force a state to adopt a particular "interpretation" of the law.[45]

---

[42] Knox, 423.

[43] Knox, 425.

[44] Susan Marks, 'International Judicial Activism and the Commodity-Form Theory of International Law', *European Journal of International Law* 18, no. 1 (2007): 208.

[45] Knox, 'Marxism, International Law, and Political Strategy', 428.

Change in law thus requires emancipatory movements' prior mobilization of extralegal force. Through the imposition of sufficient material pressure, progressive forces can compel states to undertake certain progressive interpretations of law. This change does not arise from international law but from shifts in the underlying material power dynamics. Legal outcomes, therefore, are in any case not driven by law's emancipatory potential but by extralegal struggles that reshape the balance of power and, in turn, the interpretations of legal norms that manage to 'stick'. Such a strategy, which Knox calls 'principled opportunism', suggests that 'progressive forces can take advantage of "legal opportunities" and may successfully realize their aims through international law'.[46] Even to scholars such as Marks, Chimni, and Knox, who believe in a certain degree of emancipatory potential of international law, international law thus remains reactive to material conditions rather than being an independent driver of change.

Against the backdrop of these general reflections, we may return to the field of international cyber law and ask the question: are such 'principled opportunistic strategies' useful in seeking emancipation in the conflicts and contestations underlying the contemporary information technology landscape? As I will show, the attempt to formulate concrete emancipatory arguments reveal important limitations to the emancipatory potential of international law which follow already from the legal form.

Opportunist International Cyber Law?

As we have explored in preceding chapters, states are currently expressing their views on the cyber-specific content of general international law, and 'international cyber law' is taking form in this process. In this section, I will draw on the dynamics discussed above to examine the potentials for an opportunistic strategy in the context of international cyber law. As Marc Schack and Astrid Kjeldgaard-Pedersen have suggested, the current state of affairs leaves 'a window of opportunity to push [ambiguous norms of international law] in a direction deemed desirable'.[47] Just like we saw in chapter five how tech corporations and cybersecurity corporations are present in the law-making process, social movements could involve themselves by seeking to nudge states to promote this or that interpretation serving an

[46] Knox, 433.

[47] Marc Schack and Astrid Kjeldgaard-Pedersen, *Modforanstaltninger i cyberdomænet: Den folkeretlige ramme* (Faculty of Law, University of Copenhagen, 2020).

emancipatory end. The first limitation to the degree to which such strategy is fruitful arises from the very challenge of formulating emancipatory goals within international legal discourse. As the legal form has a categorical symmetry with the relationship between commodity owners, the protection of private property remains central to the very form of law. Since the exploitative structures of the digital landscape arise from the very property relations around which the legal form is structured, the legal form might limit to the extent to which we it is possible to convincingly formulate emancipatory goals in the language of law.

Let us explore the limitations arising from the legal form by zooming in on a concrete example. We might, for example, seek to address the profound global restructuring of production and circulation arising from the opportunities unlocked by the digital code. As elucidated in chapter three, the logistics revolution and the emergence of 'lean production' have led to exacerbated forms of class-based exploitation in factories and warehouses. In an endeavor to push back against these new forms of exploitation, we need to translate our concerns into international legal discourse. But how is it possible to bring concerns for high-tech logistics into the scope of the field? The legal vocabulary – sovereignty, non-intervention, due diligence, etc. – does not seem to fit. This is not a result of high-tech logistics being irrelevant to international law. On the contrary, international legal scholars have been highly attentive to the international legal challenges arising from the digital infrastructures underlying contemporary logistics.[48] The challenge in critiquing this exploitation in international legal discourse is rather a reflection of the fact that the very *protection* of high-tech logistics is at the core of the legal form. The legal form's structure around formally equal commodity-owners entails that struggles *arising from* the property relations around which the legal form is structured cannot be systemically addressed in international legal discourse. An operationalization of international cyber law as part of an opportunistic strategy is thus limited because the emancipatory end cannot be described on the premises around which the legal form is structured.

To make a coherent legal argument, we have to follow international law's structure around individual legal subjects with rights at their disposal. In

[48] Michael Schmitt, 'The NotPetya Cyber Operation as a Case Study of International Law', *EJIL: Talk!* (blog), 2017; Bernhards Blumbergs et al., 'NotPetya and WannaCry Call for a Joint Response from International Community', CCDCOE, *CCDCOE* (blog), 2017; Csaba Krasznay, 'Case Study: The NotPetya Campaign', 2020, 485–99.

that effort, we might lower our ambitions and pick a more modest advocacy goal. We could, for example, take a case of a singular Amazon warehouse worker whose bodily functions are being exposed to daily high-tech monitoring and surveillance as part of the logistical transformation of warehouse management.[49] We could seek to deploy international legal discourse to address the exploitative regime to which she is subjected. However, what we can hope to win within this scheme also remains limited by the existing property relations around which the legal form is structured. Amazon owns and controls the labor power of the warehouse worker throughout the hours of the working day. The warehouse is therefore as a main rule a private matter of Amazon, closed to the eyes of the public and outside the scope of interference. As Marx writes: 'In the factory code, the capitalist formulates his autocratic power over his workers like a private legislator, and purely as an emancipation of his own will'.[50] Pashukanis similarly notes how 'control with the enterprise remains the private affair of each individual capitalist. The establishment of labour regulations is an act of private legislation; in other words, it is a piece of pure feudalism.'[51] Exceptions and limitations to the autocratic power of Amazon do exist as a result of the struggles of labor and human rights movements, which have resulted in propertyless individuals possessing – in addition to their only commodity, their labor power – a set of rights, such as the right to privacy as inscribed in the International Covenant of Civil and Political Rights (ICCPR) Article 17. We could thus turn to the regime of international human rights in defense of our client, arguing that ICCPR Article 17 applies to information technologies and prohibits high-tech surveillance. We could thus argue that United States has a positive obligation to ensure that Amazon guarantees the warehouse worker a certain minimum level of privacy protection.

While such advocacy strategies might lead to occasional victories, our legal arguments remain constrained by the property relations around which the legal form is structured. Within a human rights framework, we cannot challenge the systemic exploitation underlying Amazon's profit, nor the imperatives that compel Amazon to continue to seek out new forms of

[49] Chua and Cox, 'Battling the Behemoth'; Oxfam America, 'At Work and Under Watch: Surveillance and Suffering at Amazon and Walmart Warehouses' (Oxfam, 10 April 2024); Sainato, '"You Feel like You'Re in Prison"'.

[50] Marx, *Capital: A Critique of Political Economy. Volume One*, 549–50.

[51] Pashukanis, *Law and Marxism*, 141–42.

exploitation, of which the high-tech surveillance regime is symptomatic. The legal form compels us accept a transformation of the emancipatory struggle into an individualized struggle in which we cannot address how the concrete exploitation of our client, the Amazon warehouse worker, is intrinsically connected to a global restructuring of production and circulation that has exacerbated inequalities, brought much of the world into uncertainty, and fueled the ecological deterioration of the planet. The inherent connections between the urgent challenges surrounding the information technology landscape – which all rise from the same systemic imperative to maximize profit at all costs – cannot be addressed within the legal form. The categorical symmetry between the legal form and the commodity form thus reveals itself in an *a priori* limitation to the arguments we can possibly make. What is more, by opportunistically deploying the language of international law, we inadvertently validate and strengthen the liberal imaginary of free and equal commodity owners. Singular cases of, say, unlawful high-tech surveillance thus become framed as exceptions to a generally well-functioning and fair capitalism, thus sidelining and foreclosing the mundane structural harm arising from the capitalist mode of production.[52]

My considerations so far concern the challenges arising from the legal form and the limits that this form imposes on the arguments that we can possibly formulate in the language of (international) law. However, even if it would to some degree be possible to construct an international legal argument that would serve an emancipatory purpose, the success of an advocacy strategy is entirely dependent on receptiveness of international legal subjects with the power to enforce the interpretation. As Knox acknowledges, the power of progressive movements to influence legal outcomes ultimately depends on their material force, be economic or armed.[53] As such, an opportunistic strategy is only effective if assisted by the coercive power to back the interpretation by force.

This point brings me to another important limitation to the success of an advocacy strategy: States – even powerful, advanced capitalist states – are also not free to choose their favored interpretation of international law.

---

[52] Anastasiya Kotova, 'On Corporate Harm, Mute Compulsion, and Ideology: A Marxist Reading of International Corporate Criminal Responsibility' (PhD dissertation, Lund, Lund University, 2024), 294. See also Grietje Baars, *The Corporation, Law and Capitalism: A Radical Perspective on the Role of Law in the Global Political Economy* (Leiden: Brill, 2019).

[53] Knox, 'Marxism, International Law, and Political Strategy', 428.

States must, as I argued in chapter two, pursue such policies that sustain and support the capitalist system, because they have become dependent upon economic growth for their own existence and functioning.[54] If an advanced capitalist state fails to fulfil the functions required of it to sustain capital accumulation, then capital will seek elsewhere, and the state will lose its powerful position. Just like capitalism entails a compulsion for workers to sell their labor power and for capitalists to follow the laws of the market in order to survive, then capitalism constrains states in their actions, including in their international relations, compelling them to undertake a particular line of policies favorable to capital.

In conclusion, international law's structure around individual commodity owners limits the extent to which it is possible to deploy international legal discourse for emancipatory purposes. Even if we accept that it is to some extent possible to interpret international law in an emancipatory direction, the realization of such a change requires a prior change in the material relations; social movements will only be successful in pushing their interpretations if they have the coercive power to back their interpretations by force. Essentially, material change must precede legal change, and the eventual balancing of legal arguments does not reflect an inner legal logic, but the underlying relations of power. Against this backdrop, the following section explores how the digital landscape has been met with material resistance from individuals and social movements seeking such change.

THE *REAL* DIGITAL REVOLUTION

If the so-called digital revolution of the past half century is, in fact, more of a counterrevolution, then the *real* digital revolution is still ahead of us. As the technological landscape is growing ever bigger, control is concentrating within ever fewer hands, and capitalist societies are becoming ever more dependent on the stability and reliability of information technology systems, emancipatory movements have increasingly approached digital infrastructure as not only a comprehensive system of oppression and exploitation – but also as a window of opportunity. The vulnerabilities arising from the increasing connectivity are thus being reinterpreted as essential chokepoints for resistance in the struggle for emancipation.

Before I begin elucidating this phenomenon of resistance, it is important to reiterate that the fundamental features shaping the current digital

[54] Roberts, 'What Was Primitive Accumulation?', 533.

landscape are, as we saw in chapter three, not specific to the digital domain. Information technologies have been developed in a historical era in which capitalism is the primary mode of production globally, and thus, they have been shaped by the social relations of capitalism. As long as we are living in a capitalist economic system, the pressure will always be on corporations to develop new technologies to maximize profit. It is thus important to bear in mind that resistance against digital systems is one aspect of a broader emancipatory struggle. With this context established, we can now turn to explore how the vulnerabilities inherent in the economy's growing digital dependencies hold a potential for emancipation.

Let me begin by revisiting a fatal day for the Danish shipping giant Maersk in June 2017, which highlighted the fragility of modern digital infrastructure as much as its centrality to global capitalism.[55] NotPetya, a targeted cyberattack against Ukraine, accidentally spiraled into a worldwide outage, crippling Maersk's information technology systems and halting operations in ports across the globe. With 4,000 servers and 45,000 PCs wiped out, the company was unable to process shipping orders until systems were restored, freezing revenue from several of the company's shipping container lines for weeks. Maersk, which operates almost 15 per cent of global shipping, faced losses of around $300 million.[56] NotPetya disrupted digital systems that have been key to the construction of Maersk's shipping empire: innumerable details in the operation of modern shipping – monitoring routes, managing traffic, and reading ships' inventory files – are controlled by information technologies. Operating a shipping business at the capacity of Maersk would simply be impossible without advanced digital systems. Currently, the world's five largest shipping companies control 65 per cent of global shipping, underscoring how modern technology has enabled an unprecedented concentration of control over global supply chains. This situation is aptly summarized in *Wired* journalist Andy Greenberg's notion that 'an attack on Maersk strikes everywhere at once.'[57]

Unsurprisingly, international cyber law scholars have eagerly analyzed the NotPetya attack as a text-book illustration of the 'complexity of applying

[55] Parts of this analysis have been published in a blogpost. See Marie Thøgersen, '"An Attack on Maersk Strikes Everywhere at Once": International Law and the Political Economy of Digitalization', *EJIL: Talk!* (blog), 2024.

[56] Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *Wired*, 22 August 2018.

[57] Greenberg.

international law to factually ambiguous cyber scenarios,' raising 'questions about possible response options of affected states and the international community'.[58] However, NotPetya also illustrates something else: It exposes just how vulnerable the global capitalist economy of today is to digital disruptions.

As we saw in chapter three, many of the new forms of vulnerability arising from digital developments of the past half century have emerged within the logistics sector. Automation and standardization in the global circulation of commodities, of which Maersk is symptomatic, has worsened the conditions for workers all over the world through increased competition and the centralization and maintenance of the control of global supply chains in the hands of imperial powers. However, in the face of that process, critical logistics scholars have argued that key sites for logistical distribution – ports, highways, railways, and other supply chain conduits – have also become *fertile chokepoints for resistance* to capitalist dispossession and exploitation.[59] As Martin Danyluk explains:

> [A] key factor influencing the effectiveness of blockades and similar tactics, it is suggested, is a hightraffic "choke point" location within the supply chain, where commodity flows are particularly vulnerable to disruption.[60]

The increasingly complex high-tech logistics thus represents a vulnerability – a 'high-traffic choke point' – towards which resistance movements are increasingly orienting. People working in the logistics sector are continuously seeking to disrupt commodity flows and construct alternative circulations, intransigent in their claims for economic and social justice.[61] Furthermore, interruptions of supply chains have emerged as a way of expressing immiseration with the global restructuring and automation which has excluded much of the population from the workplace (the relative surplus population).

---

[58] Schmitt, 'The NotPetya Cyber Operation as a Case Study of International Law'; Blumbergs et al., 'NotPetya and WannaCry Call for a Joint Response from International Community'; Kristen E. Eichensehr, 'Ukraine, Cyberattacks, and the Lessons for International Law', *AJIL Unbound* 116 (2022): 145–49.

[59] Kai Bosworth and Charmaine Chua, 'The Countersovereignty of Critical Infrastructure Security: Settler-State Anxiety versus the Pipeline Blockade', *Antipode* 55, no. 5 (2023): 3.

[60] Danyluk, 'Seizing the Means of Circulation', 1369.

[61] Cowen, *The Deadly Life of Logistics*, 20.

Strikes, which have traditionally been the most common means of struggle for the working class, are not available to the part of the population most profoundly affected by globalization and automation: the disposable industrial reserve army, which must be always ready for exploitation by capital.[62] The external interruption of spaces of circulation has become a way of expressing immiseration for those whose lives are being profoundly affected by the structures of global circulation by being put on the side of it.[63] The rise of dense logistical networks have thus been emphasized to hold the possibility of building new solidarities and new modes of political engagement.[64]

While the NotPetya attack was conducted in the context of a regional conflict between Russia and Ukraine and had no revolutionary motives, the attack exposes how global supply chains have become extremely vulnerable to digital disruptions. To quote a warning of two commentators at the World Economic Forum, 'the impact of cybercrime extends far beyond the economic costs. It also degrades trust among internet users, and damages the reputations of public and private service providers.'[65] Pressure on the digital systems underlying and enabling contemporary forms of vulnerability has the effect of causing profound instability of these systems, leading to distrust and, by extension, a loss of power. As reflected in Greenberg's assertion that an attack on Maersk strikes everywhere at once, critical digital infrastructures are arguably beginning to reveal themselves as the Achilles heel of a global capitalist economy. Disruptions of digital infrastructures challenge the stability and reliability on which the global capitalist economy relies. The connectivity of cyberspace can thus be seen as capitalism's strength as much as it is its weakness: *On the one hand*, it allows corporations to dominate global markets through standardization and centralized control, and *on the other hand,* it exposes vulnerabilities to disruption from anywhere at any time. Capitalism in the digital era might therefore provide the key to its own destruction. The vulnerabilities arising from digital infrastructures are accurately captured in by the French group The Invisible Committee:

---

[62]Marx, *Capital: A Critique of Political Economy. Volume One*, 781–94; David McNally, *Global Slump: The Economics and Politics of Crisis and Resistance* (San Fransisco: PM Press, 2011); Dyer-Witheford, *Cyber-Proletariat*, 122–23.

[63] Bosworth and Chua, 'The Countersovereignty of Critical Infrastructure Security', 3.

[64] Chua et al., 'Introduction', 625.

[65] Robert Muggah and Mac Margolis, 'Why We Need Global Rules to Crack down on Cybercrime', *World Economic Forum*, 2 January 2023.

> The technical infrastructure of the metropolis is vulnerable: its flows are not merely for the transportation of people and commodities; information and energy circulate by way of wire networks, fibres and channels, which it is possible to attack. To sabotage the social machine with some consequence today means re-conquering and reinventing the means of interrupting its networks. … How does one find the weak points in computer networks[?][66]

As much as information technologies have been vital in facilitating capital expansion into new territories, emancipatory movements are increasingly directing their attention to the information technology systems whose stable functioning is foundational to the reproduction of contemporary capitalism.[67]

The phenomenon of digital intrusions and disruptions as a way of exercising resistance against the modes of power incarnated in technologies is not particularly new. Ever since the invention of the digital code, computer technology has been vandalized, burned, and otherwise destroyed by students and protesters to whom it symbolized an established system of power with which they were deeply dissatisfied.[68] With the increasing automation of workplaces, workers saw the potential for new forms of resistance by obfuscating and manipulating computers.[69] Once computers started to be connected to each other, new virtual communities of hackers began to arise.[70] At the core of hacking culture was an endeavor to challenge established powers and property relations in the digital domain by exercising resistance *within and through* technology.[71] While hacking communities have always been characterized by a profound skepticism toward institutions and other forms of entrenched power, the progressive nature of this culture has traditionally been limited by a libertarian individualism that sees governments are the main threat to the realization of some undertheorized goal of

---

[66] The Invisible Committee, *The Coming Insurrection* (Cambridge, MA: MIT Press, 2009), 111–12.

[67] Danyluk, 'Capital's Logistical Fix'.

[68] Mueller, *Breaking Things at Work*, 93–94.

[69] Zuboff, *In the Age of the Smart Machine*, 352–53; Mueller, *Breaking Things at Work*, 101.

[70] Garry Potter, 'Anonymous Revolution?: A Hacker Manifesto Revisited', *Fast Capitalism* (blog), 2014.

[71] Mueller, *Breaking Things at Work*, 105.

'internet freedom'.[72] Ironically, much of contemporary Silicon Valley thus emerged as a metamorphosis of hacker culture, which culminated in 'the Californian Ideology': an 'ostensibly laid-back but actually highly aggressive anti-regulatory free enterprise that narcissistically identified its own lucrative technological success as socially liberatory.'[73] Still, part of the hacker culture prevails as antiauthoritarian, non-hierarchical, decentralized communities that seek to interfere and disrupt digital systems of various kinds. Despite the prevalence of a libertarian discourse, the most consistent orientation to action of some of the most prominent hacker collectives such as Anonymous concerns the *property relations of the internet* and are 'grounded in the realities expressed in the Marxist analysis of property and exploitation'.[74] The evolution of FOSS technology, discussed above, is deeply indebted to the hacking movement and its consistent attempts to challenge extant digital property relations.[75] As the global capitalist economy is becoming profoundly reliant on information technology systems, the stakes are clearly much higher than free access to software. Considering the fragility to such interruptions as illustrated by the NotPetya attack, it is likely that those who seek emancipation from the systemic exploitation fueled by digital infrastructures will increasingly approach digital systems as chokepoints for resistance against global capitalism. Standing alone, interruptions of digital systems are no more than disturbances. As Danyluk reminds us, a precondition for the effectiveness of such acts of resistance is the collective organizing around some understanding of shared values, identities, or interests.[76] However, when backed by vigorous organizing and mass solidarity, disruptions contribute to bringing out a political space for change; quoting Danyluk, a 'focus on the generative power of such actions might point a path from resistance and interruption to the more expansive project of imagining and building alternative futures.'[77]

---

[72] Coleman, 'From Internet Farming to Weapons of the Geek', 93; Potter, 'Anonymous'.

[73] Dyer-Witheford, *Cyber-Proletariat*, 64.

[74] Potter, 'Anonymous Revolution?: A Hacker Manifesto Revisited'.

[75] Mueller, *Breaking Things at Work*, 105–7.

[76] Danyluk, 'Seizing the Means of Circulation', 1383.

[77] Danyluk, 1386.

The Task for International Legal Scholarship

If international legal scholars see an injustice in the current information technology landscape, then the conclusion that material change must precede change in international law might feel like a disappointing message. As we are facing an injustice that we cannot address with our skillset, what do we do? I will end this chapter by arguing that there is a crucial role to play for international legal scholarship. However, this role does not lie in seeking change through the language of international law itself, but rather in exposing the ideological operations that sustain the technological landscape of today as it has been shaped by the social relations of capitalism.

As this dissertation has demonstrated, international cyber law is not simply a set of international rules governing digital spaces to ensure universal security. International law expresses the role of the state-system in global capitalism and supports the social relations of capitalism, obscuring the profound social antagonisms embedded in the digital landscape. International legal scholars have a key role to play in exposing the operations of the international legal language and challenging the dominant framing of cyberspace as an apolitical domain. We must continue to ask why certain ideas prevail, whose interests they serve, and what social realities they obscure.

So far, critical international legal scholarship has largely disregarded the emerging field of international cyber law. This may be due, in part, to the relative youth of the field, but perhaps also to a broader hesitation among critical scholars to engage with the seemingly dry doctrinal processes through which international cyber law takes form. This dissertation serves as an invitation to change that neglect and begin elucidating the intricate ways in which legal discourses are intertwined with technological and securitizing discourses in this novel domain, effectively reinforcing and upholding relations of domination in the digital sphere. Meaningful change demands nothing less than a profound restructuring of the digital landscape from a tool for profit and concentration of power into a tool for just distribution and democratic control. Still, while this remains a long-term goal, recognizing, illuminating, and challenging international law's complicity in sustaining these systems is a crucial first step.

CONCLUSION

In a time of unprecedented technological developments, the emerging field of international cyber law represents an equally unprecedented mode of international law-making. Since the invention of the digital code, new technologies have been designed and developed to profoundly restructure the global economy, in turn leading to new forms of precarity, vulnerability, and ecological deterioration. Amidst these developments, states and international legal scholars are debating how international law applies to the new terrain of 'cyberspace'. While states are unilaterally publishing their views on the scope and content of general rules of international law in this new context, legal scholars are analyzing states' emerging positions as expressions of state practice and *opinio juris*. The legal scholars of the field are, however, challenged in this task, as new state practice continues to emerge, confirming or challenging prevalent interpretations. At its core, they are unable to answer the question as to the determination of which interpretation becomes authoritative if several state positions are in contradiction. This implies that they are unable to ascertain why international cyber law develops as it does, or who, or what, is ruling the digital clouds.

My ambition with this dissertation has been to answer this question, and thus, to make a critical intervention into the nascent scholarly field of international cyber law. My central argument is that international cyber law expresses the special role of the state-system in the reproduction of capitalism throughout the changing technological reality: States must, *on the one hand*, enable and facilitate capital's continuous expansion by making digital terrain open and available while, *on the other hand*, upholding stability and reliability in the social relations of capitalism by ensuring effective protection of property relations that rely on digital infrastructures.

RULING THE CLOUD

Far from being an apolitical or uncontestable process, the technological developments accelerating since the invention of the digital code have been designed by the capitalist class to increase capital accumulation on a global scale. In turn, we are witnessing widening global inequalities and worsening conditions for the working class that is exposed to unprecedented regimes of surveillance and new forms of vulnerability, deteriorating ecological crises, and profound democratic challenges. Amidst these developments, existing international legal scholarship has been trapped in the circularity of doctrine. No scholarship has yet looked comprehensively beyond this circularity and elucidated the dynamics shaping the nascent international rules governing cyberspace. The aim of this dissertation has been to fill that void. By approaching the field of international cyber law through a Marxist lens, I have illuminated how international law governing digital technologies is contingent on historically specific social relations.

I have begun the substantial part of the dissertation in ***chapter one*** with a demonstration of the inadequacies of existing scholarship on international cyber law, which is dominated by positivist approaches to law. Through a dissection of their methodological presuppositions, I have demonstrated their methodological inability to explain why certain practices and ideas turn into law, leaving the scholars of the field ultimately unable to justify their ways of generating knowledge: their methodology is inherently circular. Based on this methodological critique, I have argued that we are compelled to search beyond the legal ideas of the field if we want to make sense of them, that is, if we want to understand why some ideas come to be accepted as *international law*. We are compelled, in other words, to ascertain how law responds to material reality.

This insight has motivated the attempt in ***chapter two*** to develop a lens through which we could explain the emergence of international legal rules governing 'cyberspace'. In this endeavor, I have drawn on the work of Pashukanis to argue that the legal form carries a categorical symmetry with the relationship between commodity-owners. In international law, states relate to each other as sovereign equals, which shields over their material inequality. To understand the content of international law arising from these relations, I have suggested that we must move beyond a Pashukanian framework to understand the role of the state-system in contemporary capitalism. Specifically, we must understand the social relations of capitalism shaping

the digital technology landscape and the special role(s) of the state-system in the reproduction of these relations.

This insight motivated an examination in ***chapter three*** of the evolution of the contemporary information technology landscape. I argued that the most groundbreaking technological innovations have been state-funded inventions, which were put into industrial use throughout the 1950s and 1960s. The new technologies unlocked a series of economic opportunities, which became key tools in combatting the economy's tendency towards stagnation from the 1970s onwards. Amongst these opportunities, the most notable transformations took place in the logistics sector and the financial sector. Information technologies have since then been instrumental in sustaining and expanding global capitalism, causing new forms of vulnerability.

Against this backdrop, I have provided in critical (re)reading of the doctrinal debates through which international cyber law has taken shape. Arguing that the field of international cyber law has inherited the rationalities of cybersecurity from international debates preceding the emergence of the legal discussions of cyberspace, I have interrogated the evolving concept of cybersecurity from the end of the 1980s and forward in ***chapter four.*** Whereas the initial discussions of security in relation to information technologies in the end 1980s and the beginning of the 1990s were centered on military technology use, these discussions were on pause throughout the 1990s. Throughout this decade, a market-focused process was unfolding with the key goal of expanding the 'information society' globally. I have demonstrated how the security recurred to the international agenda in a revised form around the end of the 1990s and took shape in the 2000s. In this revised form of cybersecurity, security concerns did not merely relate to military technologies but also to commercial technologies. The stability and reliability of information technology systems was seen to call for protection, while any external intrusion into these systems was framed as a security threat.

In ***chapter five***, I have traced the doctrinal legal debates unfolding throughout the 1990s, 2000s and 2010s in parallel to the evolving notion of cybersecurity. I have argued that the initial scholarly debates on cyberspace were characterized by a widespread cyber exceptionalism, perceiving cyberspace as a distinct, lawless space. This idea went hand in hand with the global expansion of the digital landscape into virtually every corner of the world. An emerging awareness that capitalism's need for stability in digitally dependent property relations was vulnerable to cross-border cyberattacks

first materialized in the Budapest Convention on Cybercrime in 2001. Whereas the main cybersecurity threat at that time was perceived by states to arise from so-called extremist groups, 'cyber terrorists', and cyber criminals, this picture would soon change. Around the beginning of the 2010s, the global expansion of the digital landscape was almost complete, while the need for stability and reliability in the newly established digital property relations were increasing. This development went hand in hand with a growing awareness that threats to the stability of the digital landscape did not only arise from malicious non-state actors; they could also arise from (illiberal) states. This was manifested in two cyberattacks against Estonia and Georgia in 2007 and 2009, widely perceived as attributable to Russia. Soon after, the United States declared its view that cyberspace is regulated by extant rules of international law. Soon after, legal scholarship shifted from their initial focus on *whether* international law applies in cyberspace to discussions of *how* international law applies in cyberspace. Whereas the emergence of the field of international cyber law can thus be seen as a reflection of the evolving role of the state-system in the reproduction of capitalism throughout an era of rapid technological developments, I have demonstrated how the field of international cyber law – states and legal scholarship alike – nonetheless deploys a determinist, legalistic discourse. The field thereby shields the inherently political process of developing international cyber law as an apolitical expert task of 'clarifying' or 'unblurring' how international law applies in cyberspace. Within the broad contours of international cyber law that are now well established – mainly, that international law applies in cyberspace and that the central aim of the field is to ensure adequate protection of digital infrastructures against external intrusions – several questions as to the precise cyber-specific content of general rules of international law remain ambiguous.

In ***chapter six***, I have zoomed in on one of the prevailing ambiguities within the field: the contentious doctrine of (digital) sovereignty. The doctrine of sovereignty has always been a flexible construct in international law, and its evolution has been intrinsically connected to the global expansion of capitalism. As I have shown, the historical controversies surrounding the doctrine echo in the current debates on digital sovereignty. I have argued that it is possible to understand the ambiguities surrounding the doctrine of sovereignty with reference to two roles that states and the state-system fulfill in contemporary capitalism: *First,* states must ensure the stability and reliability in the social relations of capitalism through the effective protection of

property relations reliant on digital infrastructure, which suggests that sovereignty is a legally binding rule of international law allowing states to respond to any external intrusions into digital infrastructure on its territory. But *second,* states must also facilitate and sustain capital's continuous expansion, suggesting that there should be a limit to (illiberal) states' sovereign right to impede the free flows of digital content (and thus, of commodities) within their territory.

In ***chapter seven***, I have offered some reflections on the emancipatory potential of international cyber law. Arguing that the problem is not technology, but *who* technology serves and for *what* purposes, I have explored past, present and utopian attempts at constructing an alternative digital landscape. Turning to international law, I have argued that changes in law will not precede material change because of limitations arising from the legal form as well as from the social forces shaping legal outcomes. I have thus deemed the effectiveness of opportunist strategies limited. Against this backdrop, I have elucidated how the vulnerabilities arising from capitalism's growing dependence on stable digital infrastructure, particularly within the logistics sector, have been approached as chokepoints for resistance.

Triangular Ideological Operation

As I have aimed to show, international cyber law is an inherently political process with profoundly conflicting interests, in which states and tech corporations seek to ensure the best conditions for capital in the digital age. Yet, the field is generally framed in scholarship and public discourse as an apolitical matter of safeguarding a set of universal interests in the digital age. This technocratic framing arises from a *triangular ideological operation* unfolding in international cyber law. Discourses on technology, law, and security each promote and naturalize particular ideas. Being intricately intertwined, the ideas sustained by these three discourses become elevated above the realm of political controversy and contestation. While I have elucidated each of these discourses throughout this dissertation, I will take some space here to reflect on each of them and how their interplay consolidates the power of the field of international cyber law through technocratic depoliticization.

First, a technological determinism makes the very technologies at stake appear uncontestable. Technological developments are perceived as an autonomous force, following an inevitable trajectory along a singular path. This perspective detaches technological progress from the deliberate decisions and actions of agents with power and resources to influence the

technological design process, instead framing information technologies as the product of an unavoidable, natural force. In this view, questions of technological developments become a purely technical matter, which is either too complex or too boring for laypeople to bother. The determinist technology view often leads to a technophile attitude towards new technologies, celebrating technological progress as unequivocal improvements that must be protected and promoted. The responsibility for the actualization of the promising high-tech future is entrusted the brilliant minds of Silicon Valley, in whom humanity places its faith. This determinist, technophile narrative perpetuates the notion that information technologies are inherently apolitical by presenting their evolution as natural, inevitable, and unequivocally good.

Second, and as a direct result of the technological determinism that depoliticizes technology, a securitizing discourse turns international discussions of technology into an exercise of ensuring a high level of cybersecurity – a notion that suggests a universal interest in the protection of the stability of information technology systems. Framing something as a 'security problem' while simultaneously assuming implicitly something else as *not* a security problem has significant consequences. That is, it endows 'the problem' with a status and priority that 'non-security problems' do not have.[1] The securitizing discourse effectively depoliticizes the matter, cloaking particular concerns with an emblem of universality while obscuring their inherently political roots. Any social antagonisms and conflicting interests surrounding technological designs are dismissed as irrelevant to an objective and neutral security assessment conducted by experts in the universal interest of humanity.

And *third*, the notion of cybersecurity has migrated into international legal discourse which offers the promise of abstract, objective standards against which particular conduct can be evaluated. The language of international law makes the ideas of the field appear uncontestable, objective, and neutral. As international law is being presented as an external regulatory force, separate from the social relations it governs, the dynamics of the social relations between states are being reified in the 'content' of international law. This reification depoliticizes relations of conflict and contestation, masking their inherently political nature.

---

[1] Hansen and Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', 1156.

The three ideological operations are intertwined: A determinist technology view is shaping the dominant notion of security, which, in turn, is shaping the contours of the legal field of international cyber law. Within this triangularity of technology, security, and law, the conclusions of the field of international cyber law come to appear politically uncontestable. They are the only possible outcome of a technocratic interpretative endeavor undertaken by experts. The three ideological operations work together in a way that makes it difficult to contest either of them from a singular perspective. For example, if the critical legal scholar asserts that international law's structural indeterminacy reveals itself in the current ambiguities surrounding international cyber law, then the assertion may be met with the objection that the substantial rules crystallizing are essentially apolitical; they merely attempt to ensure an adequate regulatory framework for a technological development that is improving the lives of everyone. No legitimate interests are conflicting, because a universal interest prevails in ensuring a high level of security in the rapidly evolving technological reality. Even if the structural critique of international law is accepted as valid, such a critique becomes toothless in an essentially apolitical domain of technology and security.

In turn, if the critical security scholar were to challenge the dominant notion of cybersecurity, emphasizing how the notion of security is socially constructed to turn particular interests into a legitimate political priority, they would be met with an argument that the dominant notion of security merely follows from an objective interpretation of law. As such, the notion of cybersecurity that we are here dealing with is not a political notion of security – it is a *legal* notion. The Copenhagen School has sometimes been guilty of just that error: They focus on invocations of security as a way of legitimizing *derogations* from law. To them, securitization arises when the priority and urgency of an existential threat enables the 'securitizing actor' – for example a politician – to 'break free of procedures or rules he or she would otherwise be bound by'.[2] They thus deploy a definition of securitization that presupposes the determinacy of rules, enabling a distinction between obeying and disobeying rules.[3] Within the triangular ideological operation characteristic of international cyber law, the notion of cybersecurity is *taking form in the language of law*. The securitizing process is therefore invisible to the critical security scholar unless they cross their disciplinary boundary

[2] Buzan, Wæver, and Wilde, *Security*, 25.

[3] Buzan, Wæver, and Wilde, 25.

and expose how the process of securitization is intertwined with the ideological operation of law.

Finally, if the critical technology scholar were to challenge the naturalization of technology and point out how information technologies are biased towards their designers, they could be met with the objection that this arguable bias is irrelevant to international cyber law, because the field is merely concerned with an interpretation of the rules on which states have agreed. In this interpretative exercise, what is relevant is merely the extant technology landscape and not the dynamics of its creation. Existing rules are simply being neutrally adapted to the changing technological reality. The design of technologies has no relevance to the interpretative endeavor of identifying the correct content of international law in the context of information technologies. Furthermore, to the extent that a security risk arises from these technologies, a universal interest prevails in addressing it regardless of the biases that may underlie the technologies as such. The biases underlying technologies are irrelevant to the universal, societal interest in a high level of security.

The three ideological operations thus work together, ruling the digital clouds in ways that make international cyber law appear uncontestable from singular points of view. Any underlying social antagonism vanishes from the picture. Questions about the architecture of the technological landscape, the risks we should aim to address, and the injustices we should strive to dismantle, are deemed beyond the scope of the field. The process of 'clarifying' the content of international cyber law becomes a technocratic task for experts – experts in international law consulting with experts in cybersecurity and experts in information technology – aiming to analyze pressing threats and identify the correct legal interpretation, adapting law to the rapidly evolving technological landscape in a way that best ensures public security.

Behind this triangular ideological operation lies a social reality in which the very technologies being protected and promoted are being designed and developed on the basis of the imperatives of capital. Most importantly, these imperatives entail that profit must be put above all other considerations.[4] Even the most well-meaning capitalist is only able to take human wellbeing or environmental concerns into account to the extent that it is ultimately deemed profitable. As a result, information technologies are contributing to the rise of global inequalities, the commodification of ever more aspects of

[4] Wood, *Empire of Capital*, 10–11.

life, the emergence of new forms of surveillance, and the concentration of control with the global production and circulation of vital resources within ever fewer hands. These tendencies are bringing the most fundamental aspects of life and its reproduction out of democratic control on a planet that is burning.

The State-System in Global Capitalism

The profound economic restructuring enabled by information technologies was at the center of an academic debate in the beginning of the current century. Some scholars argued that the ever-increasing level of economic globalization cause a progressive decline in the sovereignty of states. As the ease of movement across national borders of money, technology, people, and goods, had been increasing, the power of states to regulate these flows and impose their authority over the economy was allegedly diminishing.[5] As we saw in chapter two, these post-imperialist arguments have been compellingly refuted by numerous imperialism scholars.[6] International legal scholars, in turn, have been relatively absent from the debate on the continuous relevance of the state-system in a world of global capitalism.[7] The absence of legal scholarship in this broader scholarly debate on the imperialism of the 21st century is surprising. No matter if we accept or refute – and if so, *how* we refute – the arguments of the post-imperialists, our answer(s) should induce us to undertake informed reflections on the relation between the power of capital and the power of states in a time of global capitalism as part of any contemporary analysis of international law, including international cyber law.

In this dissertation, I have argued that the state-system continues to play a vital role in the capitalist economy. As perceived 'neutral' entities external to the dynamics of capital accumulation, states and the state-system notably

---

[5] Hardt and Negri, *Empire*, xi.

[6] Harvey, *The New Imperialism*, 2003; Wood, *Empire of Capital*; Ellen Meiksins Wood, 'Logics of Power: A Conversation with David Harvey', *Historical Materialism* 14, no. 4 (2006): 9–34; Sutcliffe, 'Imperialism Old and New'; Callinicos, *Imperialism and the Global Political Economy*.

[7] But see Susan Marks, 'Empire's Law' (2003) 10 Indiana Journal of Global Legal Studies 449. See also Chimni, 'International Institutions Today'; B.S. Chimni, 'Capitalism, Imperialism, and International Law in the Twenty-First Century Symposium: Third World Approaches to International Law (TWAIL) Conference: Capitalism and the Common Good', *Oregon Review of International Law* 14, no. 1 (2012): 17–46.

fulfil two key roles, which are external to capital itself but necessary for the reproduction of capitalism. Throughout the 1990s, capitalist states' imperative to facilitate continuous expansion of capitalism into new territories was reflected in a techno-determinist celebration and promotion of the construction of an 'information superhighway' into new territories in the Global South as the solution to all thinkable problems. The discourse of this era celebrated openness, freedom, expansion, and growth. International law was largely absent from the debates in this era; the 'information society' was embraced as a 'terra nullius'; an exceptional, entirely new, lawless domain upon which the restrictions and power dynamics prevalent in physical domains had no bearing. A libertarian discourse emphasized the importance of keeping 'cyberspace' largely unregulated, allowing for endless expansion and opportunities. Towards the end of the 1990s, countless hopeful tech companies had emerged in this 'new domain'. With the commercialization of the internet, it became increasingly clear how the 'information society' was capitalist more than it was anarchical. It was precisely in the context of this neoliberal era that Hardt and Negri saw an *Empire* materializing before their eyes. The global nature of markets and global circuits of production entailed a fundamental lack of boundaries – 'a regime that effectively encompasses the spatial totality' with no limits.[8]

Had Hardt and Negri's central theses been correct, then this would have been the end of history – or at least, it would have been the end of the story that I have told in this dissertation. International legal norms would not have emerged in cyberspace, because states were redundant. An ever-expanding information technology landscape would continue to make the world smaller and the world economy bigger, fusing the entire globe into one large system of production and circulation.

However, Hardt and Negri were fatally wrong. Capitalism has a profound need for stability and reliability in its social relations, which does not simply vanish in a global domain. It therefore soon became clear that states continued to play an important role by providing effective enforcement systems, ensuring stability in the social arrangements on which capital accumulation relies. What is more, new vulnerabilities began to emerge from the rapid global expansion of the 'information society'. With these vulnerabilities, the stability and reliability of the property relations underlying the social relations of capitalism became an increasingly *international matter.* Digital

[8] Hardt and Negri, *Empire*, xi, xiv.

property relations could not be effectively protected through the institutional and coercive support of one state – they became dependent on the support of a *state-system* that effectively cooperates to uphold the social relations of capitalism across geographical borders. For the global circulation of capital to function in cyberspace, the individual economic actors must have faith in the global protection of digital property.

Thus, the success of virtual systems of finance and trade depend not only on the technical expansion of the virtual infrastructure, highlighted in the 1990s, but also on the global protection of digital infrastructure against external intrusions. From the beginning of the current millennium, states gradually began to talk less about the boundlessness of cyberspace and more about the security of cyberspace. Within this security discourse, the stability and reliability of information technology systems unanimously made up the object of protection, while every external intrusion to their stability was framed as a security threat. These basic assumptions came to shape the contours of the emerging field of international cyber law from the beginning of the 2010s. A militaristic, securitizing discourse was delineating the field from the very beginning. The stability and reliability of information technology systems became the unequivocal end, delineating international legal debates. Meanwhile, any external intrusions into these systems were deemed hostile and problematic, sometimes giving rise to critiques of the 'inadequacy' of the international legal framework in effectively protecting the technological landscape against such threats.

Despite the consensus around these crude contours of the field of international cyber law, the precise legal norms within the field remain overtly ambiguous, reflecting the sometimes-contradictory dual imperatives of capital: *On the one hand*, capital needs continuous expansion, demanding that states keep digital terrains open for accumulation. *On the other hand*, capital needs stability and reliability in the social relations of capitalism, demanding that states effectively protect property relations reliant on digital infrastructure.

In sum, the story that I have told in this dissertation elucidates not only the crystallization of international cyber law, but also how the state-system works through international law to ensure the best conditions for capital to continuously expand and thrive. Capitalist states generally work to ensure the stability in social arrangements that capital needs but lacks. The domestic side of this role lies in the establishment of a legal framework backed by an effective enforcement system that guarantees stable and reliable property

relations. However, with the increasing ease of movement enabled by information technologies, the protection of digital property relations becomes an international concern, and states seek to ensure global stability for capital in their international relations by protecting digital infrastructure through international law. Meanwhile, capitalist states also continue to prevent capitalism's tendency toward crises and stagnation by facilitating and enabling its continuous expansion. Domestically, we have seen states fulfill this role through ambitious investments in new technologies to prevent economic stagnation. Capitalist states facilitate industries' continuous growth through publicly funded technological innovations under a techno-determinist mantra of progress. Externally, capitalist states seek to ensure liberal regulatory policies in other states to allow for the expansion of capital into new markets. Capitalism's dual imperative for states shapes their international relations, in turn shaping international law. International law comes into the picture when property relations are vulnerable, reflecting the legal form's categorical symmetry with the relation between commodity owners. As the most powerful capitalist states are seeking to ensure protection of the digital infrastructures on which their wealth and power is dependent, the content of international cyber law is taking shape. This content comes to suit the needs of capital in an era of global capitalism. The state-system and, by extension, international law therefore continues to be relevant, even in an era in which every corner of the world has been fused into a global capitalist economy.

Future

The historically specific nature of every social form means that none of the developments exposed in this dissertation are irreversible. While humans have always relied on tools for their survival, today's information technology landscape reflects the social relations out of which it has emerged. In a society with an alternative mode of production, information technologies could still exist, but their underlying architecture would likely be fundamentally different – it would no longer be centered around property relations or designed primarily to maximize profits.

I remain skeptical about the potential for international law to serve as a tool for emancipation. If the emancipatory goal is a transformation of the global information technology landscape from a tool for profit into a tool for just distribution and democratic control, then the first step lies in the abolition of the property relations underlying the social relations of capitalism. Property relations are intrinsic to the very structure of law, including

international law. Individual entities with rights at their disposal remain at the center of international legal discourse. It is therefore impossible to challenge the systemic imperatives of capital within the legal form. While it might be possible to provide singular pushbacks, for example by deploying the language of human rights to push for better protection of personal data and digital privacy, such an argument simultaneously accepts the transformation of the individual into an abstract, equal commodity owner, in which all we can hope for is that our rights are assured a satisfactory contractual protection. The emancipatory struggle thereby becomes an individualized struggle, and even if occasional 'victories' exist, the liberal imaginary of free and equal commodity owners also becomes validated. The prospects of effectively using international cyber law as part of an opportunistic strategy in the struggle for emancipation are limited because the emancipatory end cannot be described on the premises around which the legal form is structured.

Because international law is contingent on the relations between states, material change must precede legal change, rather than the other way around. However, this does not render international lawyers irrelevant to the process. The crucial role of lawyers lies in exposing international cyber law as politically contestable. By challenging the naturalization of legal, technological, and securitizing frameworks that sustain global capitalism, legal scholars can help open the space for discussions of alternative digital futures. With this dissertation, I have aimed to break the ground for this important task. I have focused on the large contours of the field of international cyber law, and numerous questions remain unanswered. I will end this conclusion by sketching out some of these questions. I will emphasize three areas that should be addressed as part of a critical research agenda on international cyber law.

First, I have only superficially touched upon the different actors involved in the process of shaping international cyber law. Several questions remain untouched as to the different industries involved and their often overlapping, but likely also frequently conflicting, interests. In addition to the corporations behind technology products, digital platform corporations, and tech-reliant industries such as the logistics sector, a vast industry of cybersecurity is rapidly evolving. Empirical studies on the ways in which different actors seek influence on the law-making process would enable important nuances to this dissertation's rather crude depiction of the corporate stakeholders of the field. Several questions also remain open as to the precise

dynamics within and between specific states. While the abstraction from details has enabled me to paint the large picture of the evolution of the field, these abstractions leave out important questions about the ways in which individual states balance considerations in their positions. Here, case studies that zoom in on the dynamics surrounding specific ambiguities and concerns within the field, including attempts from the Global South to push back against the dominant ideas of the Global North, would make a valuable supplement.

Second, while this dissertation has focused mainly on the imperatives of capital and their influence on international cyber law, it is important to note that capitalism operates alongside and interacts with other social forces. The development of the technological landscape is not only tied to capitalism, but also, as Ambika Tandon argues, to patriarchy, colonialism, racism, and other structural power inequalities.[9] Critical questions therefore arise as to the ways in which the different social forces underlying digital technologies interact in the shaping of international cyber law. The technological landscape has to a large extent been shaped by white men in the Global North, perhaps in part explaining the often immensely masculine discourse surrounding the internet.[10] Postcolonial and feminist perspectives on international cyber law could further elucidate how international cyber law responds to these power structures underlying the digital landscape.

Third, this dissertation has not explored the profound ecological impact of information technologies. As many scholars have demonstrated, global warming is a direct result of the capitalist system and its inherent tendency to overproduction.[11] Information technologies, in turn, have been key to the survival of capitalism as the dominant economic system. The growing energy demands of artificial intelligence and massive data centers contribute to carbon emissions at unprecedented levels that are expected to continue to grow.[12] E-waste, driven by planned obsolescence and rapid technological turnover, is poisoning ecosystems and communities. Furthermore, the extraction of rare minerals like lithium and cobalt – essential for batteries and

---

[9] Ambika Tandon, 'Why Feminists Reject Big Tech', *AWID* (blog), 2023.

[10] Kellner, *Technology and Democracy*, 54.

[11] Andreas Malm, *Fossil Capital: The Rise of Steam Power and the Roots of Global Warming* (London & New York: Verso, 2016); Kohei Saito, *Marx in the Anthropocene: Towards the Idea of Degrowth Communism* (Cambridge: Cambridge University Press, 2023).

[12] Andrew R. Chow, 'How AI Is Fueling a Boom in Data Centers and Energy Demand', *TIME*, 12 June 2024.

semiconductors – fuels environmental destruction particularly in the Global South.[13] These consequences of information technologies are furthering capitalism's tendency towards ecological deterioration. In a striking parallel to the increasing prevalence of transnational threats to stable property relations in digital space, the ecological deterioration of the planet also knows no spatial barriers. Against this backdrop, crucial questions arise as to the (absence of) ecological awareness in the international legal discussions of information technologies. Critical research on international cyber law should elucidate international law's spatial movements in response to these simultaneous territorial restructurings unfolding with regard to technology and ecology, respectively.

These gaps highlight the vast terrain that remains to be explored as part of a critical research agenda on international cyber law. While this dissertation has sought to unravel the imperatives of capital in shaping the field, it also serves as an invitation to further inquiry. Understanding the complex interplay of capitalism, patriarchy, colonialism, and environmental degradation in shaping international cyber law is an urgent task for critical international legal scholarship – broadly understood. These remaining voids are thus to be interpreted as an invitation to my scholarly colleagues to join me in rethinking the dominant narrative on international cyber law. The mainstream story of international cyber law is being written at this very moment. It is therefore a crucial time for critical engagement.

[13] Dyer-Witheford, *Cyber-Proletariat*.

EPILOGUE: A CO-WORKING SPACE IN D.C.

Almost exactly two presidential terms after Brian J. Egan delivered his speech on international cyber law in proximity to Silicon Valley, another government employee took the stage on the opposite coastline. Tech billionaire Elon Musk, who is now officially serving under President Donald Trump as a special government employee, stood before the crowd at the presidential inauguration and proudly proclaimed:

> This was no ordinary victory. This was a fork in the road of human civilization. You know, elections that come and go, some elections are important some are not. But this one, this one really mattered.[1]

Musk may have been right. At least, the insertion of the richest man in the world to lead a new Department of Government Efficiency (DOGE) is no ordinary political appointment. Musk's new office in the White House arguably denotes the erasure of any remaining illusion of a separation between the state and the tech industry. The fusion of state power and corporate power in the United States has possibly never been more overt.

On the day following the inauguration, three other tech giants – OpenAI CEO Sam Altman, SoftBank CEO Masayoshi Son and Oracle Chairman Larry Ellison – appeared at the White House alongside President Donald

---

[1] 'Elon Musk Gives Exuberant Speech at Inauguration' (Washington Post, 20 January 2025), https://www.washingtonpost.com/video/politics/elon-musk-gives-exuberant-speech-at-inauguration/2025/01/20/421e0bea-74bd-4079-b379-f7d559129d08_video.html.

Trump to announce the creation of Stargate, a state-backed corporate entity aimed at expanding artificial intelligence infrastructure in the United States. The project, launched with an initial $100 billion investment and planned to reach $500 billion in the coming years, manifests a reality in which an elite borne out of Silicon Valley works in close cooperation with the American government to design an ever more connected, high-tech reality for humanity. In this era, the once symbolic proximity to Silicon Valley from where Brian J. Egan had eight years before declared the American view on international cyber law – almost seems vanished. Instead, Silicon Valley appears to have relocated itself into a permanent co-working space in Washington, D.C.

I am writing this epilogue in March 2025, a time when everyone is holding their breath, nervous for what will come next from the proclaimed 'leader of the free world'. Crucial questions arise from these developments that arguably challenge some of the key propositions of this dissertation. I will confine myself to offering some preliminary reflections on how recent developments might impact or fit into the story about international cyber law that I have told in the preceding chapters.

A key proposition of this dissertation is that the state-system plays a central role in global capitalism which is external to capital but vital for its reproduction. Almost any theory of the state under capitalism relies on an idea that the state-form presupposes that a separation is upheld between the economic and the political, 'hence the reproduction of the state depends on the continued reproduction of this separation, and so on the reproduction of capitalist social relations of production on which this separation is based.'[2] Throughout this dissertation, I have argued that the crucial roles of the state-system arise exactly from this separation between the economic and the political - from states being external to the individual economic actors involved in the process of capital accumulation. The state-system can thus provide stability and reliability in the social relations of capitalism by ensuring the global enforcement of property relations at arm's length from capital – and from the individual capitalist. States can further sustain economic activity in abstraction from individual branches, thus preventing capitalism's inherent tendency towards stagnation. I have argued that these roles are reflected in international cyber law, where states seek to protect the stability and reliability of digital infrastructures against external intrusions to ensure the global

[2] Clarke, *The State Debate*, 13.

circulation of capital, while seeking to facilitate continuous expansion into every geographical corner of the world. By making these propositions, I have argued against a dominant tendency amongst international legal scholars to neglect the relevance of the economy of the digital landscape, confining their legal analyses to an observation of the positions of states in abstraction from the underlying social relations of capitalism. I have thus sought to show that the political sphere of the relations between states cannot be separated from the economy of the digital landscape.

However, the ties between the tech industry of Silicon Valley and the United States now appear so closely consolidated that this argument almost seems redundant. And more than that: With the overt consolidation of these ties, we might question if it even makes sense to insist that capitalism presupposes the continued separation of the economic and the political? Another key proposition in this dissertation has been that (international) law is an effective way for states to make their authority seem valid and autonomous, formally separate from particular economic interests. Yet, the Trump-administration does not even bother to try framing its international politics in the language of international law, making it relevant to question whether the international legal language has effectively lost power.

Of course, the state-system is more than the United States. We might argue that what seems to be happening is not a profound change in the state-form, but rather one leader making the mistake of stepping beyond his designated role, failing to uphold the general illusion of a neutral, democratic state that operates at arm's length from capital. My cautious prediction is that such unhinged exercise of power, by lacking the level of sophistication traditionally characterizing the state-form, will eventually result in an inability to rule in ways that seem beyond contestation. If this is the case, then rather than signaling the dissolution of the state-system as I have analyzed it, the Trump-Musk era may simply expose its inner workings more explicitly than before. The state has always played a crucial role in maintaining the conditions for capital accumulation, and what we are witnessing now might not be a transformation, but rather a moment of revelation – one in which the veil of neutrality is slipping.

Where power becomes too visible, there is chance that it might lead to resistance. With the apparent relocation of Silicon Valley into a co-working space in Washington, D.C., the conflicts and contestations earlier concealed by the intertwined ideological operations in international cyber law have now become unapologetically overt. This unmasking has the potential to

fuel mobilization of social movements to exercise resistance. In as much as the ever-more complex digital infrastructure of our time is a crucial engine of capital accumulation, it is also a window of opportunity – a choke point of resistance for social movements seeking emancipation. As the veil of neutrality is vanishing, it is plausible that these movements will only grow.

BIBLIOGRAPHY

LITERATURE

Akande, Dapo, Antonio Coco, and Talita de Souza Dias. 'Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies'. *International Law Studies* 99, no. 1 (2022).

Althusser, Louis. *On The Reproduction Of Capitalism: Ideology And Ideological State Apparatuses*. London & New York: Verso, 2014.

———. *Reading Capital: The Complete Edition*. London & New York: Verso, 2016.

Anghie, Antony. *Imperialism, Sovereignty and the Making of International Law*. Cambridge: Cambridge University Press, 2005.

Arrighi, Giovanni. 'Capitalism and the Modern World-System: Rethinking the Nondebates of the 1970's'. *Review (Fernand Braudel Center)* 21, no. 1 (1998): 113–29.

Arruda, William. 'Why Polyworking Is The Future Of Work And How To Become A Polyworker'. Forbes, 5 November 2024.

Arvidsson, Matilda, and Emily Jones. *International Law and Posthuman Theory*. London: Taylor & Francis, 2024.

Arvidsson, Matilda, and Miriam Bak McKenna. 'The Turn to History in International Law and the Sources Doctrine: Critical Approaches and Methodological Imaginaries'. *Leiden Journal of International Law* 33, no. 1 (2020): 37–56.

Baars, Grietje. *The Corporation, Law and Capitalism: A Radical Perspective on the Role of Law in the Global Political Economy*. Leiden: Brill, 2019.

Bagchi, Kanad. 'Marxism and the Cognitive Turn in International Law – Exploring an Uneasy Relationship'. *Amsterdam Law School Research Paper No. 2024-42*, 2024.

———. 'Marxist Approaches to International Law: An Outline'. *Max Planck Institute for Comparative Public Law & International Law (MPIL) Research Paper No. 2022-16, Forthcoming in: OpenRewi Textbook on Public International Law*, 2022.

Balzacq, Thierry, Sarah Léonard, and Jan Ruzicka. '"Securitization" Revisited: Theory and Cases'. *International Relations* 30, no. 4 (2016): 494–531.

Barlow, John Perry. 'A Declaration of the Independence of Cyberspace'. Electronic Frontier Foundation, 1996.

Bastani, Aaron. *Fully Automated Luxury Communism*. London & New York: Verso, 2019.

Bear, Laura. 'Speculation: A Political Economy of Technologies of Imagination'. *Economy and Society* 49, no. 1 (2020): 1–15.

Benanav, Aaron. 'Automation and the Future of Work—1'. *New Left Review*, no. 119 (2019): 5–38.

———. 'How to Make a Pencil'. *Logic(s) Magazine*, December 2020.

Bernes, Jasper. 'Logistics, Counterlogistics and the Communist Prospect'. *Endnotes*, 2013.

Bianchi, Andrea, ed. *Interpretation in International Law*. Oxford: Oxford University Press, 2015.

Biller, Jeffrey. 'The Strategic Use of Ransomware Operations as a Method of Warfare'. *International Law Studies* 100, no. 1 (2023).

Birkinbine, Benjamin J. *Incorporating the Digital Commons: Corporate Involvement in Free and Open Source Software*. London: University of Westminster Press, 2020.

Block, Fred. 'The Ruling Class Does Not Rule'. *Socialist Revolution* 6–28 (1977): 295–305.

Blumbergs, Bernhards, Tomáš Minárik, Kris van der Meij, and Lauri Lindström. 'NotPetya and WannaCry Call for a Joint Response from International Community'. CCDCOE. *CCDCOE* (blog), 2017.

Boer, Lianne J.M. *International Law As We Know It: Cyberwar Discourse and the Construction of Knowledge in International Legal Scholarship*. Cambridge: Cambridge University Press, 2021.

———. '"Spoofed Presence Does Not Suffice": On Territoriality in the Tallinn Manual'. In *Netherlands Yearbook of International Law 2016: The Changing Nature of Territoriality in International Law*, edited by Martin Kuijer and Wouter Werner, 131–45. The Hague: T.M.C. Asser Press, 2017.

Bonefeld, Werner. *Critical Theory and the Critique of Political Economy: On Subversion and Negative Reason*. London & New York: Bloomsbury, 2014.

Bork, R.H., and J.G. Sidak. 'What Does the Chicago School Teach about Internet Search and the Antritrust Treatment of Google?' *Journal of Competition Law and Economics* 8, no. 4 (2012): 663–700.

Bosworth, Kai, and Charmaine Chua. 'The Countersovereignty of Critical Infrastructure Security: Settler-State Anxiety versus the Pipeline Blockade'. *Antipode* 55, no. 5 (2023): 1345–67.

Brenner, Robert. *Property and Progress: The Historical Origins and Social Foundations of Self-Sustaining Growth*. London & New York: Verso, 2009.

———. *The Economics of Global Turbulence: The Advanced Capitalist Economies from Long Boom to Long Downturn, 1945-2005*. London & New York: Verso, 2006.

———. 'The Origins of Capitalist Development: A Critique of Neo-Smithian Marxism'. *New Left Review*, no. 104 (1977): 25-.

———. 'What Is, and What Is Not, Imperialism?' *Historical Materialism* 14, no. 4 (2006): 79–105.

———. 'What Is Good for Goldman Sachs Is Good for America: The Origins of the Present Crisis'. *UCLA: Center for Social Theory and Comparative History*, 2009.

Brewer, Anthony. *Marxist Theories of Imperialism: A Critical Survey*. London: Routledge, 1990.

Brian J. Egan. 'International Law and Stability in Cyberspace'. Berkeley School of Law, 10 November 2016.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998.

Callinicos, Alex. *Imperialism and the Global Political Economy*. Cambridge: Polity Press, 2009.

Chimni, B. S. 'Customary International Law: A Third World Perspective'. *American Journal of International Law* 112, no. 1 (2018): 1–46.

Chimni, B.S. 'Capitalism, Imperialism, and International Law in the Twenty-First Century Symposium: Third World Approaches to International Law (TWAIL) Conference: Capitalism and the Common Good'. *Oregon Review of International Law* 14, no. 1 (2012): 17–46.

———. 'International Institutions Today: An Imperial Global State in the Making'. *European Journal of International Law* 15, no. 1 (2004): 1–37.

———. *International Law and World Order: A Critique of Contemporary Approaches*. 2nd ed. Cambridge: Cambridge University Press, 2017.

China. 'China's Positions on International Rules-Making in Cyberspace', 20 October 2021.

Chow, Andrew R. 'How AI Is Fueling a Boom in Data Centers and Energy Demand'. *TIME*, 12 June 2024.

Chua, Charmaine. *The Logistics Counterrevolution: Fast Circulation, Slow Violence, and the Transpacific Empire of Capital*, Forthcoming.

Chua, Charmaine, and Spencer Cox. 'Battling the Behemoth: Amazon and the Rise of America's New Working Class'. *Socialist Register* 59 (2022).

Chua, Charmaine, Martin Danyluk, Deborah Cowen, and Laleh Khalili. 'Introduction: Turbulent Circulation: Building a Critical Engagement with Logistics'. *Environment and Planning D: Society and Space* 36, no. 4 (2018): 617–29.

Clarke, Simon. 'Introduction'. In *The State Debate*, edited by Simon Clarke. London: Palgrave Macmillan, 1991.

———, ed. *The State Debate*. London: Palgrave Macmillan, 1991.

Cogburn, Derrick L. 'Globalization and Governance in Cyberspace: Mapping the Processes of Emergent Regime Formation in Global Information and Communications Policy'. University of Michigan - School of Information, 2000.

Cohen, Jean L. 'Whose Sovereignty? Empire Versus International Law'. *Ethics & International Affairs* 18, no. 3 (2004): 1–24.

Cohen, Julie E. 'Cyberspace as/and Space'. *Columbia Law Review* 107, no. 1 (2007): 210–56.

Coleman, Gabriella. 'From Internet Farming to Weapons of the Geek'. *Current Anthropology* 58, no. S15 (2017): S91–102.

———. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London & New York: Verso, 2015.

Conlon, Justin. 'Sovereignty vs. Human Rights or Sovereignty and Human Rights?' *Race & Class* 46, no. 1 (2004): 75–100.

Couldry, Nick, and Ulises A. Mejias. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford: Stanford University Press, 2019.

Cowen, Deborah. 'A Geography of Logistics: Market Authority and the Security of Supply Chains'. *Annals of the Association of American Geographers* 100, no. 3 (2010): 600–620.

———. *The Deadly Life of Logistics: Mapping Violence in Global Trade*. Minneapolis: University of Minnesota Press, 2014.

Cox, Robert W. 'Social Forces, States and World Orders: Beyond International Relations Theory'. *Millennium* 10, no. 2 (1981): 126–55.

Crawford, Matthew B. *The World Beyond Your Head: On Becoming an Individual in an Age of Distraction*. Farrar, Straus and Giroux, 2015.

D'Amato, Anthony. 'International Law, Cybernetics, and Cyberspace'. Edited by Michael N. Schmitt and Brian T. O'Donnell. *International Law Studies*, no. 76 (1999).

———. *The Concept of Custom in International Law*. Cornell University Press, 1971.

Danyluk, Martin. 'Capital's Logistical Fix: Accumulation, Globalization, and the Survival of Capitalism'. *Environment and Planning D: Society and Space* 36, no. 4 (2018): 630–47.

———. 'Seizing the Means of Circulation: Choke Points and Logistical Resistance in Coco Solo, Panama'. *Antipode* 55, no. 5 (2023): 1368–89.

Delerue, François. 'Reinterpretation or Contestation of International Law in Cyberspace?' *Israel Law Review* 52, no. 3 (2019): 295–326.

Desmukh, Fahad. 'Imagining a Socialist Internet'. *TRT World* (blog), 2018.

Doctorow, Cory. *The Internet Con: How to Seize the Means of Computation*. London & New York: Verso, 2023.

Duffy, Clare, and David Goldman. 'Trump Signs Promised Executive Action to Delay TikTok Ban for 75 Days'. *CNN*, 20 January 2025.

Dunn Cavelty, Myriam. 'From Cyber-Bombs to Political-Fallout: Threat Representations with an Impact'. *International Studies Review* 15, no. 1 (2013): 105–22.

Dunoff, Jeffrey L., and Mark A. Pollack, eds. *International Legal Theory: Foundations and Frontiers*. 1st ed. Cambridge: Cambridge University Press, 2022.

Durand, Cédric. *How Silicon Valley Unleashed Techno-Feudalism: The Making of the Digital Economy*. London & New York: Verso, 2024.

Dyer-Witheford, Nick. 'Cyber-Marx: Cycles and Circuits of Struggle in High-Technology Capitalism'. *Canadian Journal of Communication* 25, no. 3 (2000).

———. *Cyber-Proletariat: Global Labour in the Digital Vortex*. London: Pluto Press, 2015.

———. 'Empire, Immaterial Labor, the New Combinations, and the Global Worker'. *Rethinking Marxism* 13, no. 3–4 (2001): 70–80.

Eagleton, Terry. *Ideology: An Introduction*. London & New York: Verso, 1991.

Economy, Elizabeth C. 'The Great Firewall of China: Xi Jinping's Internet Shutdown'. *The Guardian*, 29 June 2018, sec. News.

Eichensehr, Kristen E. 'Ukraine, Cyberattacks, and the Lessons for International Law'. *AJIL Unbound* 116 (2022): 145–49.

'Elon Musk Gives Exuberant Speech at Inauguration'. Washington Post, 20 January 2025. https://www.washingtonpost.com/video/politics/elon-musk-gives-exuberant-speech-at-inauguration/2025/01/20/421e0bea-74bd-4079-b379-f7d559129d08_video.html.

Epstein, Gerald. *The Political Economy of Central Banking: Contested Control and the Power of Finance, Selected Essays of Gerald Epstein*. Edward Elgar Publishing, 2019.

Feenberg, Andrew. *Questioning Technology*. London, United Kingdom: Taylor & Francis Group, 1999.

Franzese, Patrick W. 'Sovereignty in Cyberspace: Can It Exist?' *Air Force Law Review*, no. 64 (2009): 1–43.

Fuchs, Christian. 'Critical Globalization Studies and the New Imperialism'. *Critical Sociology* 36, no. 6 (2010): 839–67.

Fukuyama, Francis. *End of History and the Last Man*. Simon and Schuster, 2006.

Geisler, Murray A. 'Logistics Research and Management Science'. *Management Science* 6, no. 4 (1960): 444–54.

Gray, Catriona. 'More than Extraction: Rethinking Data's Colonial Political Economy'. *International Political Sociology* 17, no. 2 (2023).

Greenberg, Andy. 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History'. *Wired*, 22 August 2018.

Haataja, Samuli. 'The 2007 Cyber Attacks against Estonia and International Law on the Use of Force: An Informational Approach'. *Law, Innovation and Technology* 9, no. 2 (2017): 159–89.

Hansen, Lene, and Helen Nissenbaum. 'Digital Disaster, Cyber Security, and the Copenhagen School'. *International Studies Quarterly* 53, no. 4 (2009): 1155–75.

Hardt, Michael, and Antonio Negri. *Empire*. Cambridge, MA: Harvard University Press, 2001.

Harris, Jerry. 'Globalization, Technology and the Transnational Capitalist Class'. *Foresight* 17, no. 2 (2015): 194–207.

———. 'Transnational Capital and the Technology of Domination and Desire'. *Race & Class* 57, no. 1 (2015): 3–19.

Harvey, David. 'The Enigma of Capital and the Crisis This Time'. In *Business as Usual: The Roots of the Global Financial Meltdown*, edited by Craig

Calhoun and Georgi Derluguian, 89–112. New York City: New York University Press, 2011.

———. *The New Imperialism*. Oxford: Oxford University Press, 2003.

———. 'The "New" Imperialism: Accumulation by Dispossession'. *Socialist Register* 40, no. 40 (2009).

Heinrich, Michael. *An Introduction to the Three Volumes of Karl Marx's Capital*. New York City: NYU Press, 2004.

———. *How to Read Marx's Capital: Commentary and Explanations on the Beginning Chapters*. New York City: NYU Press, 2021.

Heintschel von Heinegg, Wolff. 'Territorial Sovereignty and Neutrality in Cyberspace'. *International Law Studies* 89, no. 1 (2013).

Heller, Kevin Jon. 'In Defense of Pure Sovereignty in Cyberspace'. *International Law Studies* 97, no. 1 (2021).

———. 'Low-Intensity Cyber Operations and State Sovereignty in Cyberspace'. Djøf Publishing in Cooperation with the Centre for Military Studies, 2023.

Henkin, Louis. *How Nations Behave: Law and Foreign Policy*. Council on Foreign Relations, 1979.

Henriksen, Anders. *International Law*. Oxford: Oxford University Press, 2021.

Hohmann, Jessie M., and Christine Schwöbel-Patel. 'A Monument to E. G. Wakefield: New and Historical Materialist Dialogues for a Posthuman International Law'. In *International Law and Posthuman Theory*, edited by Mathilda Arvidsson and Emily Jones, 2023.

Holden, Kerry, and Matthew Harsh. 'On Pipelines, Readiness and Annotative Labour: Political Geographies of AI and Data Infrastructures in Africa'. *Political Geography* 113 (2024): 103–50.

Hollis, Duncan. 'The Influence of War; the War for Influence'. *Temple Journal of International & Comparative Law* 32 (2018).

Hollis, Duncan B. 'Why States Need an International Law for Information Operations Symposium: Crimes, War Crimes, and the War on Terror'. *Lewis & Clark Law Review* 11, no. 4 (2007): 1023–62.

Hughes, Rex. 'A Treaty for Cyberspace'. *International Affairs* 86, no. 2 (2010): 523–41.

Johns, Fleur. 'Critical International Legal Theory'. In *International Legal Theory: Foundations and Frontiers*, edited by Jeffrey L. Dunoff and Mark A. Pollack. Cambridge: Cambridge University Press, 2022.

Johnson, David R., and David G. Post. 'Law and Borders - the Rise of Law in Cyberspace'. *Stanford Law Review*, no. 48 (1997).

Jones, Emily. *Feminist Theory and International Law: Posthuman Perspectives*. Routledge, 2023.

Jørgensen, Rikke Frank. 'Human Rights and Private Actors in the Online Domain'. In *New Technologies for Human Rights Law and Practice*, edited by Jay D. Aronson and Molly K. Land, 243–69. Cambridge: Cambridge University Press, 2018.

Jurich, Jon P. 'Cyberwar and Customary International Law: The Potential of a "Bottom-up" Approach to an International Law of Information Operations Developments'. *Chicago Journal of International Law* 9, no. 1 (2009): 275–96.

Kaplan, Esther. 'The Spy Who Fired Me: The Human Costs of Workplace Monitoring'. *Harper's Magazine*, March 2015.

Kellner, Douglas. *Technology and Democracy: Toward A Critical Theory of Digital Technologies, Technopolitics, and Technocapitalism*. Medienkulturen Im Digitalen Zeitalter. Wiesbaden: Springer Fachmedien Wiesbaden, 2021.

Kjeldgaard-Pedersen, Astrid. *The International Legal Personality of the Individual*. Oxford: Oxford University Press, 2018.

Kjelgaard, Jeppe Mejer, and Ulf Melgaard. 'Denmark's Position Paper on the Application of International Law in Cyberspace'. Nordic Journal of International Law, 4 July 2023.

Knox, Robert. 'A Critical Examination of the Concept of Imperialism in Marxist and Third World Approaches to International Law'. Phd, London School of Economics and Political Science, 2014.

———. 'Marxism, International Law, and Political Strategy'. *Leiden Journal of International Law* 22, no. 3 (2009): 413–36.

Koskenniemi, Martti. *From Apology to Utopia: The Structure of International Legal Argument*. Cambridge: Cambridge University Press, 2005.

———. 'What Should Lawyers Learn from Marx?' In *International Law on the Left: Re-Examining Marxist Legacies*, edited by Susan Marks. Cambridge: Cambridge University Press, 2008.

Kotova, Anastasiya. 'On Corporate Harm, Mute Compulsion, and Ideology: A Marxist Reading of International Corporate Criminal Responsibility'. PhD dissertation, Lund University, 2024.

Krasznay, Csaba. 'Case Study: The NotPetya Campaign', 485–99, 2020.

Krause, Keith, and Michael C. Williams. 'Broadening the Agenda of Security Studies: Politics and Methods'. *Mershon International Studies Review* 40, no. 2 (1996): 229–54.

Kugelberg, Elsa. 'Dating Apps and the Digital Sexual Sphere'. *American Political Science Review*, 2025, 1–16.

Kunz, Josef L. 'The Nature of Customary International Law'. *American Journal of International Law* 47, no. 4 (1953): 662–69.

Lahmann, Henning. 'Information Operations and the Question of Illegitimate Interference under International Law'. *Israel Law Review* 53, no. 2 (2020): 189–224.

———. 'On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace'. *Duke Journal of Comparative & International Law* 32, no. 1 (2022): 61–107.

Lamolinara, Guy. 'Wired for the Future - President Clinton Signs Telecom Act at LC'. Library of Congress. Libarary of Congress, 19 February 1996.

Lapavitsas, Costas. *Profiting Without Producing: How Finance Exploits Us All*. London & New York: Verso, 2014.

Levinson, Marc. *The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger*. Princeton: Princeton University Press, 2016.

Li, Darryl. 'How to Read a Case: Ethnographic Lawyering, Conspiracy, and the Origins of Al Qaeda'. *American Anthropologist* 125, no. 3 (2023): 559–69.

Liam Mullally. 'The Actually Existing Internet: Opening the Internet (1969-1991)'. *The Autonomy Institute* (blog), 2024.

Liebetrau, Tobias. 'Problematising EU Cybersecurity: Exploring How the Single Market Functions as a Security Practice'. *Journal of Common Market Studies* 62, no. 3 (2024): 705–24.

Liu, Wendy. *Abolish Silicon Valley: How to Liberate Technology from Capitalism*. London: Watkins Media Limited, 2020.

Mačák, Kubo. 'Unblurring the Lines: Military Cyber Operations and International Law'. *Journal of Cyber Policy* 6, no. 3 (2021): 411–28.

Makely, William. '50 Years of Technological Development'. Cutting Tool Ingeneering, 2005.

Malm, Andreas. *Fossil Capital: The Rise of Steam Power and the Roots of Global Warming*. London & New York: Verso, 2016.

Marketcap. 'Top Public Companies by Total Assets (February 2025)'. Balance sheet, February 2025.

Markoff, John. 'Building the Electronic Superhighway'. *The New York Times*, 24 January 1993.

Marks, Susan. 'Empire's Law'. *Indiana Journal of Global Legal Studies* 10, no. 1 (2003): 449–66.

———. 'International Judicial Activism and the Commodity-Form Theory of International Law'. *European Journal of International Law* 18, no. 1 (2007): 199–211.

———, ed. 'Introduction'. In *International Law on the Left: Re-Examining Marxist Legacies*. Cambridge: Cambridge University Press, 2008.

———. *The Riddle of All Constitutions: International Law, Democracy, and the Critique of Ideology*. Oxford: Oxford University Press, 2003.

Marx, Karl. *Capital: A Critique of Political Economy. Volume One*. Penguin Classics. London: Penguin in association with New Left Review, 1990.

———. *Grundrisse: Foundations of the Critique of Political Economy*. London: Penguin Publishing Group, 1993.

———. 'Letter to Ferdinand Lassalle, February 22, 1858'. In *Marx & Engels Collected Works Volume 40: Letters 1856-1859*. International Publishers, 1975.

———. *Marx & Engels Collected Works Volume 29: Marx 1857-61*. New York: International Publishers, 1987.

———. 'Preface'. In *A Contribution to the Critique of Political Economy*, 1859.

———. 'Preface to the Second Edition'. In *Capital: A Critique of Political Economy, Vol. 1*, by Karl Marx. Penguin Classics. London: Penguin in association with New Left Review, 1990.

———. 'Results of the Immediate Process of Production'. In *Capital. Volume One: A Critique of Political Economy*, by Karl Marx. Penguin Classics. London: Penguin in association with New Left Review, 1990.

Mau, Søren. *Mute Compulsion: A Marxist Theory of the Economic Power of Capital*. London & New York: Verso, 2023.

———. 'The Transition to Capital in Marx's Critique of Political Economy'. *Historical Materialism* 26, no. 1 (2018): 68–102.

Mazzucato, Mariana. *The Entrepreneurial State: Debunking Public vs. Private Sector Myths*. London: Anthem Press, 2015.

McCarthy, Daniel R. *Power, Information Technology, and International Relations Theory*. London: Palgrave Macmillan, 2015.

———. 'Technology and "the International" or: How I Learned to Stop Worrying and Love Determinism'. *Millennium* 41, no. 3 (2013): 470–90.

McDougal, Myres, Harold Lasswell, and W. Michael Reisman. 'Theories About International Law: Prologue to a Configurative Jurisprudence'. *Faculty Scholarship Series*, 1968.

McDougal, Myres S. 'Law and Power'. *The American Journal of International Law* 46, no. 1 (1952): 102–14.

———. 'Perspectives for an International Law of Human Dignity'. *Proceedings of the American Society of International Law at Its Annual Meeting* 53 (1959): 107–36.

McKenna, Miriam Bak. *Reckoning with Empire: Self-Determination in International Law*. Leiden: Brill, 2023.

McGregor, Heather. 'Law on a Boundless Frontier: The Internet and International Law'. *Kentucky Law Journal* 88, no. 4 (2000): 967–86.

McNally, David. 'From Financial Crisis to World-Slump: Accumulation, Financialisation, and the Global Slowdown'. *Historical Materialism* 17, no. 2 (2009): 35–83.

———. *Global Slump: The Economics and Politics of Crisis and Resistance*. San Fransisco: PM Press, 2011.

Medina, Eden. *Cybernetic Revolutionaries: Technology and Politics in Allende's Chile*. Cambridge, Mass: MIT Press, 2011.

Miéville, China. *Between Equal Rights: A Marxist Theory of International Law*. Chicago: Haymarket Books, 2006.

———. 'The Commodity-Form Theory of International Law'. In *International Law on the Left: Re-Examining Marxist Legacies*, edited by Susan Marks, 92–132. Cambridge: Cambridge University Press, 2008.

Ministry of Defense of France. 'International Law Applied to Operations in Cyberspace', 9 September 2019.

Modirzadeh, Naz K. '"Let Us All Agree to Die a Little": TWAIL's Unfulfilled Promise'. *Harvard International Law Journal*, 2023.

Morozov, Evgeny. 'Digital Socialism?' *New Left Review*, no. 116/117 (2019): 33–67.

———. 'The Santiago Boys - the Tech World That May Have Been'. Chora Media, n.d.

Moynihan, Harriet. 'The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace'. *Journal of Cyber Policy* 6, no. 3 (2021): 394–410.

Mueller, Gavin. *Breaking Things at Work: The Luddites Are Right About Why You Hate Your Job*. London & New York: Verso, 2021.

Mueller, Milton. 'Against Sovereignty in Cyberspace'. *International Studies Review* 22, no. 4 (2020): 779–801.

———. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT Press, 2009.

———. *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. London: Polity Press, 2017.

Muggah, Robert, and Mac Margolis. 'Why We Need Global Rules to Crack down on Cybercrime'. *World Economic Forum*, 2 January 2023.

Mullally, Liam. '"We Do Not yet Know What a Network Can Do": Steps to a Collective Internet'. *The Autonomy Institute* (blog), 2024.

Nardelli, Pedro H. J. *Cyber-Physical Systems: Theory, Methodology, and Applications*. Hoboken: John Wiley & Sons, 2022.

Nardelli, Pedro HJ, Pedro E Gória Silva, Harun Siljak, and Arun Narayanan. 'Cyber-Physical Decentralized Planning for Communizing'. *Competition & Change* 29, no. 1 (2025): 121–38.

National Intelligence Council. 'Foreign Threats to the 2020 US Federal Elections'. Intelligence Community Assessment, 10 March 2021.

Neocleous, Mark. *Critique of Security*. Edinburgh: Edinburgh University Press, 2008.

———. 'International Law as Primitive Accumulation; Or, the Secret of Systematic Colonization'. *European Journal of International Law* 23, no. 4 (2012): 941–62.

Nişancıoğlu, Kerem, and Alexander Anievas. *How the West Came to Rule: The Geopolitical Origins of Capitalism*. London: Pluto Press, 2015.

Noble, David F. *Forces of Production*. Transaction Publishers, 1984.

Pal, Maïa. '"My Capitalism Is Bigger than Yours!": Against Combining "How the West Came to Rule" with "The Origins of Capitalism"'. *Historical Materialism* 26, no. 3 (2018): 99–124.

Pashukanis, Evgeniĭ Bronislavovich. *Law and Marxism: A General Theory*. Edited by C. J. Arthur. London: Ink Links, 1978.

———. *Pashukanis, Selected Writings on Marxism and Law*. Edited by Piers Beirne and Robert S. Sharlet. Academic Press, 1980.

Perritt, Henry H. Jr. 'Cyberspace and State Sovereignty'. *Journal of International Legal Studies* 3, no. 2 (1997): 155–204.

Peters, Anne. *Beyond Human Rights: The Legal Status of the Individual in International Law*. Cambridge Studies in International and Comparative Law. Cambridge: Cambridge University Press, 2016.

Petersen, Casper Skovgaard. 'The Death of Cyber Socialism'. *Farsight* (blog), 2024.

Phillips, Leigh, and Michal Rozworski. *The People's Republic of Walmart: How the World's Biggest Corporations Are Laying the Foundation for Socialism*. London & New York: Verso, 2019.

Pinto, Renata Ávila. 'Digital Sovereignty or Digital Colonialism?' *Sur - International Journal on Human Rights*, no. 27 (2018).

Potter, Garry. 'Anonymous: A Political Ontology of Hope'. *Theory in Action*, 2015.

———. 'Anonymous Revolution?: A Hacker Manifesto Revisited'. *Fast Capitalism* (blog), 2014.

Purvis, Nigel. 'Critical Legal Studies in Public International Law'. *Harvard International Law Journal* 32, no. 1 (1991): 81–128.

Puschmann, Cornelius, and Jean Burgess. 'Metaphors of Big Data'. *International Journal of Communication* 8 (2014): 1690–1709.

Quintana, Fernando. 'On the Withering Away of Law: Radical Politics Beyond Legal Fetishism'. *Legal Form* (blog), 2024.

Rain Ottis. 'Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective'. *Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia*, 2008.

Rasulov, Akbar. '"The Nameless Rapture of the Struggle": Towards a Marxist Class-Theoretic Approach to International Law'. *Finnish Yearbook of International Law* 19 (2008): 243–94.

Ratner, Steven R., and Anne-Marie Slaughter. 'Appraising the Methods of International Law: A Prospectus for Readers'. In *The Methods of International Law*. Studies in Transnational Legal Policy ; No. 36. Washington, D.C: American Society of International Law, 2004.

Rehmann, Jan. *Theories of Ideology: The Powers of Alienation and Subjection*. Chicago: Haymarket Books, 2013.

Richard Kadlčák. 'Statement by Czech Republic'. Presented at the 2nd substantive meeting of the OEWG, UN General Assembly, 11 February 2020.

Roberts, Anthea Elizabeth. 'Traditional and Modern Approaches to Customary International Law: A Reconciliation'. *American Journal of International Law* 95, no. 4 (2001): 757–91.

Roberts, William Clare. 'What Was Primitive Accumulation? Reconstructing the Origin of a Critical Concept'. *European Journal of Political Theory* 19, no. 4 (2020): 532–52.

Robinson, William I. *Can Global Capitalism Endure?* Los Angeles: SCB Distributors, 2022.

Robinson, William I., and Jerry Harris. 'Towards a Global Ruling Class? Globalization and the Transnational Capitalist Class'. *Science and Society* 64, no. 1 (2000): 11–54.

Rosenau, James N. 'Information Technologies and the Skills, Networks, and Structures That Sustain World Affairs'. In *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, by J. P. Singh and James N. Rosenau. Albany: SUNY Press, 2002.

Sainato, Michael. '"You Feel like You'Re in Prison": Workers Claim Amazon's Surveillance Violates Labor Law'. *The Guardian*, 21 May 2024, sec. US news.

Saito, Kohei. *Marx in the Anthropocene: Towards the Idea of Degrowth Communism*. Cambridge: Cambridge University Press, 2023.

Sander, Barrie. 'Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections'. *Chinese Journal of International Law* 18, no. 1 (2019): 1–56.

———. 'Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-Based Approach to Content Moderation'. *Fordham Int'l LJ* 43 (2019): 939.

Saros, Daniel Earl. *Information Technology and Socialist Construction: The End of Capital and the Transition to Socialism*. Routledge, 2014.

Sauter, Molly. 'Show Me on the Map Where They Hacked You: Cyberwar and the Geospatial Internet Doctrine'. *Case Western Reserve Journal of International Law* 47, no. 1 (2015): 63.

Schack, Marc, and Astrid Kjeldgaard-Pedersen. *Modforanstaltninger i cyberdomænet: Den folkeretlige ramme*. Faculty of Law, University of Copenhagen, 2020.

Schmitt, Michael. 'Bellum Americanum: The U.S. View of Twenty-First Century War and Its Possible Implications for the Law of Armed Conflict'. *Michigan Journal of International Law* 19, no. 4 (1998): 1051–90.

———. 'Foreign Cyber Interference in Elections'. *International Law Studies* 97, no. 1 (2021).

———. 'Grey Zones in the International Law of Cyberspace'. *Yale Journal of International Law*, 2018.

———. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

———. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.

———. 'The Law of Cyber Conflict: Quo Vadis 2.0?' In *The Future of Armed Conflict*, edited by Matthew Waxman and Thomas Oakley. The Lieber Studies Series. Oxford: Oxford University Press, 2022.

———. 'The Law of Cyber Warfare: Quo Vadis?' SSRN Scholarly Paper. Rochester, NY, 2013.

———. 'The NotPetya Cyber Operation as a Case Study of International Law'. *EJIL: Talk!* (blog), 2017.

Schmitt, Michael, and Liis Vihul. 'Respect for Sovereignty in Cyberspace'. SSRN Scholarly Paper. Rochester, NY, 2017.

Schmitt, Michael, and Sean Watts. 'Beyond State-Centrism: International Law and Non-State Actors in Cyberspace'. *Journal of Conflict and Security Law* 21, no. 3 (2016): 595–611.

Scott, Shirley V. 'International Law as Ideology: Theorizing the Relationship between International Law and International Politics'. *European Journal of International Law* 5, no. 3 (1994): 313–25.

Simma, Bruno, and Andreas L. Paulus. 'The Responsibility of Individuals for Human Rights Abuses in Internal Conflicts: A Positivist View'. *The American Journal of International Law* 93, no. 2 (1999): 302–16.

Smith, Jason E. *Smart Machines and Service Work: Automation in an Age of Stagnation*. London: Reaktion Books, 2020.

Solum, Lawrence B. 'On the Indeterminacy Crisis: Critiquing Critical Dogma'. *University of Chicago Law Review* 54, no. 2 (1987): 462–503.

Srnicek, Nick. *Platform Capitalism*. New York City: John Wiley & Sons, 2016.

Standing, Guy. *The Precariat: The New Dangerous Class*. London: A&C Black, 2011.

Stephens, Dale. 'Influence Operations & International Law'. *Journal of Information Warfare* 19, no. 4 (2020): 1–16.

Sutcliffe, Bob. 'Imperialism Old and New: A Comment on David Harvey's The New Imperialism and Ellen Meiksins Wood's Empire of Capital'. *Historical Materialism* 14, no. 4 (2006): 59–78.

Taha, Mai. 'Reading "Class" in International Law: The Labor Question in Interwar Egypt'. *Social & Legal Studies* 25, no. 5 (2016): 567–89.

Tandon, Ambika. 'Why Feminists Reject Big Tech'. *AWID* (blog), 2023.

Tarnoff, Ben. *Internet for the People: The Fight for Our Digital Future*. London & New York: Verso, 2022.

Teschke, Benno. *The Myth of 1648: Class, Geopolitics, and the Making of Modern International Relations*. London & New York: Verso, 2003.

The Invisible Committee. *The Coming Insurrection*. Cambridge, MA: MIT Press, 2009.

Thøgersen, Marie. '"An Attack on Maersk Strikes Everywhere at Once": International Law and the Political Economy of Digitalization'. *EJIL: Talk!* (blog), 2024.

Thompson, John Brookshire. *Ideology and Modern Culture: Critical Social Theory in the Era of Mass Communication*. Stanford: Stanford University Press, 1990.

Toscano, Alberto. 'Lineaments of the Logistical State'. *Viewpoint Magazine* (blog), 2014.

Tsing, Anna. 'Supply Chains and the Human Condition'. *Rethinking Marxism* 21, no. 2 (2009): 148–76.

Tzouvala, Ntina. *Capitalism As Civilisation: A History of International Law*. 1st ed. Cambridge: Cambridge University Press, 2020.

———. 'The "Unwilling or Unable" Doctrine and the Political Economy of the War on Terror'. *Humanity: An International Journal of Human Rights, Humanitarianism, and Development* 14, no. 1 (2023): 19–38.

Unger, Roberto Mangabeira. *The Critical Legal Studies Movement: Another Time, a Greater Task*. London & New York: Verso, 2015.

Wallerstein, Immanuel Maurice. *World-Systems Analysis: An Introduction*. Durham: Duke University Press, 2004.

Wanshu, Cong. 'Contesting Freedom of Information: Capitalism, Development, and the Third World'. *Asian Journal of International Law* 13, no. 1 (2023): 46–75.

Watt, Eugene van der. 'Project Cybersyn: The Socialist Internet That Almost Was'. Versus, 2024.

Watts, Sean, and Theodore T. Richard. 'Baseline Territorial Sovereignty and Cyberspace'. *Lewis & Clark Law Review*, 2018.

Waxman, Matthew. 'Cyber Attacks as "Force" Under UN Charter Article 2(4)'. *International Law Studies* 87 (2011): 43.

———. 'Self-Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions'. *International Law Studies* 89 (2013): 109.

Waxman, Matthew C. 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)'. *Yale Journal of International Law* 36, no. 2 (2011): 421–60.

Wilén, Carl. 'Formalism and Instrumentalism in the Marxist Critique of Right: With What Must Pashukanian Theory Begin?' *Rethinking Marxism*, Forthcoming.

———. 'Why Pashukanis Was Right: Abstraction and Form in The General Theory of Law and Marxism'. *Capital & Class*, 2023.

Wood, Ellen Meiksins. *Democracy Against Capitalism: Renewing Historical Materialism*. Cambridge: Cambridge University Press, 1995.

———. *Empire of Capital*. 2nd ed. London & New York: Verso, 2005.

———. 'Logics of Power: A Conversation with David Harvey'. *Historical Materialism* 14, no. 4 (2006): 9–34.

———. *The Origin of Capitalism*. New York City: Monthly Review Press, 1999.

Wright, Erik Olin. *Envisioning Real Utopias*. London & New York: Verso, 2020.

———. 'Real Utopias'. *Contexts* 10, no. 2 (2011): 36–42.

Zuboff, Shoshana. *In the Age of the Smart Machine: The Future of Work and Power*. London: Heinemann, 1988.

———. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019*. London: Profile Books, 2019.

Zulfiqar, Ghazal Mir. 'Digital Financialization and Surveillance Capitalism in the Global South: The New Technologies of Empire'. *Sage Journals*, 2023.

POSITION PAPERS

2012

The United States	Koh, Harold Hongju. 'International Law in Cyberspace'. Presented at the USCYBERCOM Inter-Agency Legal Conference, Ft Meade, 18 September 2012.

2016

The United States	Brian J. Egan. 'International Law and Stability in Cyberspace'. Berkeley School of Law, 10 November 2016.

2017	
Australia	'Annex to Australia's National Cyber Engagement Strategy - Australia's Position on the Application of International Law to State Conduct in Cyberspace', 2019 2017.
2018	
United Kingdom	'Application of International Law to States' Conduct in Cyberspace: Statement of the United Kingdom', 3 June 2021.
2019	
The Netherlands	'Appendix: International Law in Cyberspace', 5 July 2019. 'Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace', 5 July 2019.
France	'International Law Applied to Operations in Cyberspace - paper shared by France with the Open-ended working group established by resolution 75/240', 9 September 2019
Czech Republic	Kadlčák, Richard. 'Special Envoy for Cyberspace Director of Cybersecurity Department (Czech Republic)', 11 February 2020.
United States	Hon. Paul C. Ney, Jr. 'DOD General Counsel Remarks at U.S. Cyber Command Legal Conference'. 2 March 2020.
Iran	'Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace', 18 August 2020.
Finland	'International Law and Cyberspace - Finland's National Positions', 15 October 2020.

New Zealand	'The Application of International Law to State Activity in Cyberspace', 1 December 2020.

2020

Australia	'Australia's submission on international law to be annexed to the report of the 2021 Group of Governmental Experts on Cyber'

2021

Italy	'Italian Position Paper on "International Law and Cyberspace"', 2021.
Israel	Schondorf, Roy. 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations'. *International Law Studies* 97, no. 1 (26 January 2021).
Germany	'On the Application of International Law in Cyberspace', March 2021
Switzerland	'Switzerland's Position Paper on the Application of International Law in Cyberspace (Annex to the United Nations Group of Governmental Experts 2019/2021)', May 2021.
United Kingdom	'Application of International Law to States' Conduct in Cyberspace: Statement of the United Kingdom', 3 June 2021.
Japan	'Basic Position of the Government of Japan on International Law Applicable to Cyber Operations', 16 June 2021.
Australia, Brazil, Estonia, Germany, Japan, Kazakhstan, Kenya, Netherlands, Norway, Romania, Russian Federation, Singapore,	'Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General

Switzerland, United Kingdom, United States	Assembly Resolution 73/266'. United Nations, 13 July 2021.
China	'China's Views on the Application of the Principle of Sovereignty in Cyberspace', December 2021.

2022

Canada	'International Law Applicable in Cyberspace', April 2022.
United Kingdom	Braverman, Suella. 'International Law in Future Frontiers (United Kingdom)'. 19 May 2022.
Sweden	'Sweden's Position Paper on the Application of International Law in Cyberspace', July 2022
Poland	'The Republic of Poland's Position on the Application of International Law in Cyberspace', 29 December 2022.

2023

Pakistan	'Pakistan's Position on the Application of International Law in Cyberspace', 3 March 2023.
Denmark	Kjelgaard, Jeppe Mejer, and Ulf Melgaard. 'Denmark's Position Paper on the Application of International Law in Cyberspace'. Nordic Journal of International Law, 4 July 2023.
Finland	Lehto, Marja. 'Finland's Views on International Law and Cyberspace'. Nordic Journal of International Law, 4 July 2023.
Ireland	'Position Paper on the Application of International Law in Cyberspace', 6 July 2023.
Costa Rica	Costa Rica. 'Costa Rica's Position on International Law in Cyberspace', 21 July 2023.

2024

African Union	African Union Peace and Security Council. 'Common African Position on the Application of

	International Law to the Use of Information and Communication Technologies in Cyberspace', 29 January 2024.
Czech Republic	'Position Paper of the Czech Republic on the Application of International Law in Cyberspace', 1 March 2024.
European Union	Council of the European Union. 'Declaration by the European Union and Its Member States on a Common Understanding

2025

Colombia	Torres, Laura Camila Sarabia, Mauricio Jaramillo Jassir, Jhon Jairo Camargo Motta Motta, Laura Quintero Buriticá, Álvaro Frías Galván, Lucía Solano Ramírez, and Nathalia Trujillo Castro. 'Colombia's National Position on the Application of International Law in Cyberspace', 18 February 2025.

Resolutions, Debates, Political Documents

United Nations General Assembly

Scientific and Technological Developments and Their Impact on International Security (Res. 43/77)	07/12/1988
Scientific and Technological Developments and Their Impact on International Security (Res. 45/60)	04/12/1990
Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 53/70)	04/12/1998
Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 54/49)	01/12/1999
Developments in the Field of Information and Telecommunications in the Context of International Security (Res. /55/28)	20/11/2000

Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 56/19)	29/11/2001
Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 57/53)	22/11/2002
Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 58/32)	08/12/2003
Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 59/61)	03/12/2004
Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 60/45)	08/12/2005
Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 61/54)	06/12/2006
Address by H.E. Mr. Toomas Hendrik Ilves, President of the Republic of Estonia. Presented at the 62nd Session.	25/09/2007
Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 62/17)	05/12/2007
Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 63/37)	02/12/2008
Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 64/25)	02/12/2009
Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 65/41)	08/12/2010
Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 66/24)	02/12/2011

Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 67/27) 03/12/2012

Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 68/243) 27/12/2013

Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 69/28) 02/12/2014

Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 70/237) 23/12/2015

Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 71/28) 05/12/2016

Role of Science and Technology in the Context of International Security and Disarmament (Res. 72/28) 04/12/2017

Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (Res. 73/266) 22/12/2018

Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 74/29) 12/12/2019

Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 75/240) 31/12/2020

United Nations Secretary General

Current Developments in Science and Technology and Their Potential Impact on International Security and Disarmament Efforts (A/75/221) 23/07/2020

Current Developments in Science and Technology and Their Potential Impact on International Security and Disarmament Efforts (A/76/182) 19/07/2021

Current Developments in Science and Technology and Their Potential Impact on International Security and Disarmament Efforts (A/77/188) 18/07/2022

Current Developments in Science and Technology and Their Potential Impact on International Security and Disarmament Efforts (A/78/268)	01/08/2023

The United Nations Human Rights Council

Kaye, David. 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression'.	11/06/2016
Working Group on Transnational Corporations and Special Rapporteur on Freedom of Expression: Presented at the 13th Meeting 32nd Regular Session.	16/06/2016

United Nations Groups of Governmental Experts

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security	30/07/2010
Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security	24/06/2013
Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security	22/07/2015
Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security	14/07/2021

Open-ended working group on developments in the field of information and telecommunications in the context of international security

Final Substantive Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security	10/03/2021

European Union

The Information Society and Development: The Role of the European Union (Communication from the Commission to the Council to the European Parliament to the Economic and Social Committee and to the Committee of the Regions)	15/07/1997

International Conferences

G7 Ministerial Conference on the Global Information Society: Round-Table Meeting of Business Leaders. 25-26/02 1995

Information Society and the Developing World (ISAD): Chair's Conclusions. Midrand, South Africa: Gallagher Estate 13/05/1996

Summary Report from Global Knowledge 97: Knowledge for Development in the Information Age'. The International Institute for Sustainable Development (IISD) 22/07/1997

International Law Commission

Draft Conclusions on Identification of Customary International Law 2018

Draft Conclusions on Identification of Customary International Law with Commentaries 2018

National politics and legislation

The United Kingdom: Taylor, Ian. 'Information Society and Development Conference'. House of Commons - Parliament of the United Kingdom. 12/06/1996

The United States: 1997 Framework for Global Electronic Commerce. 01/07/1997

The United States: National Intelligence Council. 'Foreign Threats to the 2020 US Federal Elections'. Intelligence Community Assessment. 10/03/2021

Civil Society Reports

Oxfam America. 'At Work and Under Watch: Surveillance and Suffering at Amazon and Walmart Warehouses'. 10/04/2024

Jensen, Magnus Thorn, Asbjørn Sonne Nørgaard, Anna Viemose, and Julie Løvgren Frandsen. 'Overenskomst giver take-away-bude bedre vilkår og markant bedre løn'. Copenhagen: Cevea. 17/05/2022

'The Oxford Process on International Law Protections in Cyberspace: A Compendium'. Oxford Institute for Ethics, Law and Armed Conflict. 2022

Appendix: Detailed List of Contents

English Summary

Over the past two decades, international cyber law has emerged as a distinct legal field in response to societies' increasing reliance on digital infrastructures. Existing legal scholarship is dominated by positivist approaches that treat international law as a self-contained system of rules that can be readily applied to new technological realities. This dissertation offers a Marxist critique of international cyber law, arguing that the field must be understood as an expression of the role of states in sustaining global capitalism. Situating the development of international cyber law within broader technological and economic transformations of the past half-century, this dissertation challenges the notion that digital technologies evolve independently of political and economic forces. Instead, it argues that major technological innovations have been shaped by the imperatives of capital, emerging in response to the economic stagnation of the 1970s and serving as key instruments for capitalism's reproduction and global expansion. In turn, digital infrastructures have deepened global inequalities, increased vulnerabilities for the working class, commodified ever more aspects of life, and fueled ecological crises. Through a critical (re)reading of international cyber law, this dissertation exposes its underlying assumptions and material foundations. It demonstrates that states shape international cyber law to fulfill two key roles external to capital yet essential to its reproduction: first, providing stability and predictability to digital infrastructures that global capitalism increasingly depends on; and second, ensuring capital's continuous expansion by making digital space accessible to capital accumulation. The dissertation further reveals how legal discourse is closely intertwined with technological and security discourses, reinforcing the illusion that international cyber law is neutral and uncontestable. In doing so, international cyber law universalizes and depoliticizes the interests of those who own, control, and profit from digital infrastructures, obscuring profound conflicts over power and ownership in the digital sphere. The dissertation finally debates the emancipatory potential of international cyber law. Arguing that changes in law will not precede material change, it suggests that emancipation demands a profound restructuring of the digital landscape from a tool for profit and concentration of power into a tool for just distribution and democratic control. In the meantime, the task for international legal scholarship must be to critically expose international law's complicity in sustaining global capitalism in the digital era.

Dansk Resumé

I løbet af de sidste to årtier er international cyberret opstået som et særskilt retligt felt i kølvandet af samfundets stigende afhængighed af digitale infrastrukturer. Den eksisterende juridiske forskning er domineret af positivistiske tilgange, der anskuer folkeretten som et selvstændigt system af regler, der kan anvendes på en ny teknologisk virkelighed. Denne afhandling giver en marxistisk kritik af international cyberret og argumenterer for, at feltet skal forstås som et udtryk for staters rolle i opretholdelsen af global kapitalisme. Afhandlingen anskuer udviklingen af international cyberret i lyset af bredere teknologiske og økonomiske transformationer i det sidste halve århundrede og udfordrer dermed forestillingen om, at digitale teknologier udvikler sig uafhængigt af økonomiske kræfter. I stedet argumenterer den for, at digital teknologi er blevet formet af kapitalens imperativer, og at de mest grundlæggende teknologiske forandringer er opfundet som reaktion på den økonomiske stagnation i 1970'erne. Informationsteknologi har siden da været central for kapitalismens reproduktion og globale ekspansion. Samtidig har informationsteknologier forværret globale uligheder, gjort arbejderklassen mere udsat, kommercialiseret stadig flere aspekter af livet og forværret økologiske kriser. Gennem en kritisk (gen)læsning af international cyberret belyser afhandlingen feltets underliggende antagelser og materielle grundlag. Afhandlingen viser, at international cyberret tager form efter to centrale funktioner for staten under global kapitalisme: For det første at give stabilitet til de digitale infrastrukturer som kapitalismens sociale relationer er afhængig af; for det andet at facilitere plads for kapitalens fortsatte ekspansion ved at støtte fortsat digital ekspansion. Afhandlingen viser yderligere, hvordan en retlig diskurs er tæt sammenflettet med en teknologisk diskurs og en sikkerhedsdiskurs, hvilket forstærker illusionen om international cyberret som politisk ubestridelig. Dermed universaliserer feltet interesserne hos dem, der ejer, kontrollerer og profiterer på digitale infrastrukturer, og skjuler samtidig de dybe interessekonflikter i den digitale sfære. Afhandlingen debatterer til sidst feltets frigørende potentiale. Den argumenterer for, at retlig forandring ikke vil gå forud for materiel forandring, og at frigørelse derfor kræver en fundamental omstrukturering af det digitale landskab fra et redskab til profit til et redskab til retfærdig fordeling og demokratisk kontrol. I mellemtiden må opgaven for den folkeretlige forskning være kritisk at afsløre folkerettens medvirken til at opretholde den globale kapitalisme i den digitale tidsalder.