B/Ordering the State in Cyberspace

Daniel Lambach[1]

Abstract

Cyberspace is not the 'electronic frontier' that cyberlibertarian utopianists dream about, no distinct and uncivilized space beyond the reach of the state. Instead, cyberspace and the digital have become integral parts of a hybridizing digital/physical lifeworld. States are adapting to this transformation by creating analogies to borders and territory in cyberspace and by adopting deterritorialized and extraterritorial modes of control. To describe state adaptation strategies, this paper first discusses the conceptualization of borders and territory and their relation to order from an International Relations perspective. It then develops the concept of territorial practices as a technique of governance which consists of the reification of spaces, the communication of boundaries, and displays of power.

Keywords: Borders, Cyberspace, Territory, Assemblage, State

1. Introduction

This paper is about how and why states construct borders and territories in cyberspace. Given that cyberspace is not a featureless plain, as the old metaphor of the 'electronic frontier' (Saco 1999) suggests, but rather a complex assemblage that does not conform to Cartesian notions of three-dimensional space (Kitchin 1998), borders in cyberspace are invariably complex. Hence, notions of the border and of territory in cyberspace bear little resemblance to their analogs in the physical world, even though such comparisons are inevitably made. Cybernetic borders and notions of territorial statehood are enacted and reinforced through firewalls, kill switches, national symbols, and legislation. However, despite these differences, cybernetic borders matter a great deal to both states and cyberspace. To states, borders are a competent performance of their existence in, and control over, cyberspace; to cyberspace, borders are a way of ordering the technopolitical assemblage of the internet.

Given how much this paper argues against simplifying analogies of 'the digital' and 'the physical', what does an analysis of state b/ordering practices in cyberspace add to our general understanding of border com-

1 I am indebted to Fabian Reinold for his editorial assistance.

plexities? First, cyberspace is not a separate place 'out there' that is distinct and detached from the real world around us—*Neuland*, as former German Federal Chancellor Angela Merkel famously once called it (Zeh 2013). Instead, we can observe how the digital and the physical world converge and infiltrate one another. This infiltration occurs in both directions. The digital world permeates the physical world via smartphones, the Internet of Things (IoT, i.e. 'smart' physical objects that collect and exchange data over electronic networks) and other, ever smaller devices. This is particularly evident when looking at state borders themselves, which have become a complex assemblage of physical and digital tools, devices, and practices mobilized for purposes of mobility control and data collection. On the other side, the physical world penetrates the digital through techniques such as geolocation, which are increasingly changing the internet's character. Geolocation is a means to establish a user's location and digitally process it. Geolocation can also be used for so-called geo-blocking which regulates access to digital data and content according to a user's physical location. Thus, the boundaries between the digital and the physical are eroded, creating an ever more enmeshed and entangled hybrid world. In addition, societies around the globe are undergoing a wholesale digital transformation (Berg et al. 2020), a large-scale rearrangement of social practices akin to other dramatic societal shifts like urbanization, globalization, or the nascent decarbonization of the economy. Indeed, with digital networks becoming a more and more prominent part of our societies and lifeworlds, a volume on border complexities should also look to cyberspace as an example of how complex such border arrangements can extend beyond the familiar framework of physical geography.

Second, as much as borders in cyberspace do not conform to traditional views of what a border should look like (with walls and barbed wire, designated crossing points, passport checks, etc.), state borders have long ceased to conform to this idealized image. As the entire field of border studies—and even this book itself—demonstrates, the physical borders of the state have become decentralized and their purposes more complex: from 'hard' borders to selective and semi-permeable membranes, from instruments of security to instruments of data collection, from the single boundary line to fluid borderlands (Newman 2006; Paasi 2009; Mau et al. 2012). Digital technologies are part and parcel of this state border transformation—as tools for surveilling borders, regulating mobilities through visa regimes, computerized transport logistics, and many more (Pallister-Wilkins 2016;

Lisle 2017; Martin-Mazé/Perret 2021). Nowadays, borders are sociotechnical assemblages consisting of physical and digital elements.

Third, borders in cyberspace showcase the mutual constitution of borders and orders. Every order has a spatial claim embedded in it: where, and to whom, should it apply? In this sense, bordering is the inevitable byproduct of ordering. Bordering is also constitutive of ordering. Enacting a border in cyberspace is a competent performance of (state) orders in a space that is often otherwise constructed as lawless and threatening. Since there is no way for the state to be as physically present in cyberspace as it is in physical space—where we have government buildings, state agents in official uniforms, and state symbols deployed liberally to remind everyone of the existence and power of the state—the border is one of the relatively few symbols that states can use to perform itself into existence. Not being able to access certain content and/or websites reminds users that the legal geography of the state also applies to cyberspace.

This paper will proceed as follows: in the first section, it will explain the concept of cyberspace as a sociotechnical assemblage. Then, it will discuss why and how states are adapting to the digital transformation of society. The third section introduces a conceptual framework for analyzing borders in cyberspace which is further fleshed out in the fourth section through the concept of territorial practices. The conclusion discusses the implications of this for research into the dis/order of border complexities.

2. Borders, Orders, Territoriality, and the State

Within International Relations and other branches of political science, borders are inextricably bound up with notions of territoriality and sovereign statehood. John Agnew (1994) has criticized the discipline as being in a 'territorial trap' and ignoring other forms of spatiality. I have discussed the limitations of this narrow focus on particular conceptions of space in more detail elsewhere (Lambach 2021b). The purpose of this section is merely to clarify key terms and their relations.

Borders, in the words of David Newman (2003, 123), "demarcate the territories within which we are compartmentalized, determine with whom we interact and affiliate, and the extent to which we are free to move from one space to another". As such, they are a sociopolitical construction, but they are also a necessary implication of political spatiality itself. In other words, if politics are organized according to spatial criteria, as opposed to

relational ones as in the early medieval *Personenverbandsstaat*, for instance, borders need to be imposed. More theoretically, Malpas argues that "extendedness"—as both size and openness—is the essential characteristic of space, which also implies boundedness, i.e., a difference between inside and outside (Malpas 2012, 233–234). In a world of political territory, borders are an essential mechanism through which the principle of territoriality is put into practice. Borders are both material and symbolic, embodied by walls, fences, gates, and checkpoints (Anderson/O'Dowd 1999). They are represented on maps, in Geographic Information Systems, through road signs and other media. While state borders were historically seen as instruments of division, they are also interfaces or zones of contact (Kopytoff 1987).

The border is intimately connected to the notion of order. Every order has specific spatial claims about its reach embedded within it, which require borders to demarcate the order's reach. By dividing the world into inside and outside, borders are an essential instrument for the maintenance of order. In the case of sovereign statehood, this has led to notions of the state as a "territorial container" (Walker 1993, 159) or a "power container" (Giddens 1985, 12–13), with borders serving as the carapace of the hard-shelled state (Herz 1957). As argued above, this also has a performative dimension that is particularly evident in cyberspace as well as other non-terrestrial environments such as the oceans or outer space, where it is difficult to enact a permanent physical presence of symbols, agents, and other representations of the state (Lambach 2021a).

As this discussion shows, borders are a necessary implication of state territoriality and political power. Following Sack (1986), territoriality is to be understood here as the principle through which domination is exercised (or, normatively speaking, *should be* exercised) along spatial criteria (Lambach 2020a). Sack (1986) identifies three dimensions of territoriality: first, a "classification by area" (1986, 21), second, communication of borders, e.g., through boundary markings, and third, the attempt to enforce territorial claims. This approach is valuable because it focuses our attention on the practices of territoriality, especially since territoriality as a principle of political order is rarely explicitly talked about or argued about—neither in practical politics nor in political science (Ruggie 1993, 174). But how should we approach borders and territoriality in conceptual terms? In other words, if borders are a social construct, how are they constructed?

Although authors such as Kahler (2006) have attempted to formulate a concept of territoriality in terms of an international regime, i.e., a set of principles, norms, rules, and procedures formalized in international

treaties and organizations governing a specific issue area, these attempts are not entirely convincing. Regimes are based on multilateral agreements and organizations that are supposed to regulate certain problem areas. While regimes can influence the interests and identities of participating states, they cannot constitute these states or their borders. In addition, there is another objection: there is no clearly definable regime that regulates the territoriality of the international system. Rather, this principle runs like a thread through many regimes. In this way, global regimes reinforce norms and practices of territoriality as they adopt the central normative requirement of the territoriality principle—that rule should be divided and exercised territorially—and map it into their respective rules.

Other contributions suggest an institutionalist approach to borders. Authors such as Feyissa/Hoehne (2010), Carter/Goemans (2014), and Simmons/Goemans (2021) can be grouped under this heading. One such approach is via the English School of International Relations which, through the concept of 'primary institutions', views institutions and members of international society as mutually constitutive. Buzan (2004, 182–184) describes primary institutions as persistent patterns of common practices which are anchored in values shared among members of the international society and includes territoriality as one of the "master" institutions of the current international system which others are derived from. This approach is similar to Ruggie's (1998) social constructivist notion of "constitutive rules" which he describes as the "institutional foundation of all social life" (1998, 873), thereby opening up the possibility of rules that are not subject to political deliberation: "Some constitutive rules, like exclusive territoriality, are so deeply sedimented or reified that actors no longer think of them as rules at all" (1998, 873). But while Buzan's (2004) and Ruggie's (1998) approaches broadly capture the essence of territoriality and borders as deeply internalized norms and rules, they are too theoretically underdeveloped to be of much help.

I argue that we are best positioned to understand state borders and territory through the prism of practice. As the brief survey above indicated, borders—as a concept, not in their specific instances—are rarely openly discussed politically, forcing us to look beyond the realm of political language into concepts of practice, embodiment, enactment, or performance. I use practice mostly because it is the best-developed of these concepts in International Relations in particular (e.g. Büger/Gadinger 2014), although the following discussion could probably also be recast in these other conceptual frames. Following Brighenti (2010), a practice approach asks how

agents constitute spaces through practices and how these spaces impact future practices. A spatial practice can be understood as any practice whose performance is aimed at deconstructing or enacting and thereby (re-)creating spaces. The application of this approach to borders in cyberspace will be further elaborated below.

3. What is Cyberspace?

In his famous *Declaration of the Independence of Cyberspace*, John Perry Barlow (1996) warned the governments of the world: "On behalf of 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" (1996). According to Barlow and others (e.g. Johnson/Post 1996), cyberspace is "a *terra nullius* in which social relations and laws have no historical existence and must be reinvented" (Chenou 2014, 216). Since then, the 'internet exceptionalism' (Farrell 2006; Wu 2010) of Barlow (1996) and his fellow cyber-utopianists has become a marginal position in internet governance discourses. Empirical developments have further put notions of the internet's ungovernability to rest. Cyberspace can no longer be conceived as separate from the offline world but must instead be viewed as part and parcel of it. This will be discussed in more detail in the next section, but in brief terms, internet activity is currently tied to physical geographical location in many ways that were unimaginable to early cyberspace theorists.

Cyberspace is not a static environment, but a dynamic and evolving domain whose parameters shift with each innovation (Deibert/Rohozinski 2010, 45). Definitions of cyberspace typically refer to an assemblage based on data storage and exchange via electronic networks. In this sense, cyberspace consists of physical hardware, code, and data. In addition, cyberspace also encompasses a social space, i.e., a space emerging from social interactions based on relations of social distance and proximity among users (Bourdieu 1989). Hardware includes all the physical objects that form the hubs and spokes of the electronic network, e.g., computers, servers, routers, cables, and satellites. Code includes the software that makes the internet run, from the very basic communication protocols that make data transfer possible to the more specialized applications that are used to offer content on the internet. Data are the manifold bits of information that are generated by machines and users and collected for a variety of purposes.

The social space is the network of relations that emerge in cyberspace, most obviously on social media platforms but also beyond these.

It is important not to view these dimensions as detached from each other because they jointly constitute cyberspace as space and are heavily interlinked. For example, Deibert (2003) points out that states' attempts to exercise control over online social activities have had effects on the material infrastructure of the internet—through the deployment of censorship and surveillance technologies, for instance. Prohibitions on linking to sensitive material have affected the network structure of the World Wide Web. Furthermore, contributions from Science & Technology Studies (STS) highlight that the material infrastructure of the internet exerts its own "sociotechnical agency" (Musiani 2014, 275) and that technologies carry embedded politics (Winner 1980) that pre-structure emerging spaces (Balzacq/Cavelty 2016; Mager 2018). For example, discussions about net neutrality, i.e., the principle that all forms of internet traffic should be treated the same at a technical level (DeNardis 2014, 131–152), show how political processes and material affordances intersect.

Importantly, all four elements—hardware, code, data, and social relations—have some connection to physical space. Hardware (cables, routers, servers, etc.) is situated in specific places, code is being created in specific localities (e.g., *Silicon Valley*), data is stored on physical servers, and social relations exist among people for whom this is but a part of their everyday life experience. In short, cyberspace is not the 'electronic frontier' of the internet exceptionalists.[2] Cyberspace is not out *there* but is right *here* with us, surrounding us. We as citizens, workers, and consumers are connected to cyberspace through hardware like smartphones and other smart devices, desktop computers and notebooks, IoT devices in our homes (e.g., refrigerators, dishwashers, lightbulbs), industrial controllers and more, through code like social media offerings and other software, through datasets and cookies collecting data on our digital behavior. The result is a lifeworld made up of both digital and physical elements that are not neatly separated from each other but are hybridized into a digital-physical whole. We are connected to other people through in-person and digitally mediated

2 The 'electronic frontier' metaphor was deliberately chosen by early Internet theorists to recall Frederick Jackson Turner's famous "frontier history" of the United States (Geiger 2008), i.e., as an unregulated space beyond the control of the state (Saco 1999). Unintentionally, this omitted the part of Turner's thesis whereby the gradual colonization and territorialization of the frontier was a constitutive part of the formation and evolution of the American state, a theme that also fits well with this article.

relationships. Communication moves seamlessly between in-person and digitally mediated forms. The most appropriate visual metaphor for this hybrid is the 'Matrix', in which a layer of data and code permeates the world that we perceive as real. When this paper refers to cyberspace, it is this hybrid, not the older notion of a distinct electronic space that still informs public imagination and discourse.

The digital transformation is changing—although arguably not revolutionizing—society. Digitalization is about much more than merely adding computers to the workplace, a notion that was very popular in the 1990s. Instead, it means introducing digital instruments, technologies, and practices into practically all spheres of social life. Technologies are being developed and adapted for social purposes, but social practices also change to adapt to technological affordances. For example, during the Covid-19 pandemic, videoconferencing software made a shift towards home office work possible, one that was vitally important for keeping certain workplaces going in a safe manner. The social impact of introducing digital technologies is substantial. It has become a truism often repeated by politicians, businesspeople, and researchers that digitalization is reshaping all aspects of our life. In that sense, the digitalization discourse is reminiscent of narratives about globalization of the 1990s, which was also portrayed as a huge challenge that we as a society and as individual citizens must adapt to. Whether this rhetorical move is correct is another matter, but its widespread use is testament to the popularity of the underlying imaginary of the digital transformation. Crucially, as with globalization, the digital transformation is not just a social and economic process but also a political one.

4. Adaptable States

The standard version of the digitalization discourse portrays states as being under threat by the massive disembedding of relations from the familiar territorial framework (Boehme-Neßler 2009), Barlow's (1996) declaration being a case in point. This, too, echoes a familiar trope from the globalization literature, where the concept of the territorial state has been the subject of dismissive critique, as globalization and the gradual if uneven emergence of world society dominated everyone's imagination. Far-reaching arguments about the impending death by obsolescence of the territorial

state were easy to find, at least for a time (Castells 1996; Strange 1996). As we know today, proclamations of the impending death of the territorial state have failed to materialize. Instead, states have managed to adapt to the vicissitudes of globalization—some more successfully than others—and have managed to combine their traditional form of territoriality with extraterritorial and deterritorialized modes of control (Lambach 2020a). The transformation of borders is but one indication of this.[3]

Digitalization presents a similar kind of challenge that states need to adapt to and, indeed, are adapting to. This is driven by the self-conception of the state as the ultimate arbiter of social relations. States' claims to sovereignty do not imply that they must regulate all social behavior, but that, in a pinch, they should be able to have the final say. Hence, in principle, states need to be prepared to intervene in social relations wherever they occur. Where there is human activity, there is a potential need for regulation, especially as a field of relations grows. Of course, there are many examples of spontaneous social ordering, bottom-up cooperative governance, and self-regulation but in the modern international system, all of these, with very few exceptions, occur in the famous 'shadow of hierarchy' cast by the state (Scharpf 1991, 629). Regarding cyberspace, states have developed ways of collecting taxes, clarifying property rights, establishing jurisdiction for content regulation (regarding pornography or harmful speech, for example), and protecting against online security threats (such as cyberattacks, terrorist networks, and organized crime). These are attempts to reterritorialize digital activity into the familiar territorial framework of the state (Lambach 2020b).

All these activities require borders to clarify which state is responsible for what. But borders in cyberspace are difficult to communicate. There are no digital equivalents to gates, fences, walls, or armed guards on the internet. Instead, borders are enacted through practice: not being able to access certain YouTube videos, having to comply with German liability laws such as the necessity for each website to publish an imprint, or being prosecuted for hate speech under the *Netzwerkdurchsetzungsgesetz* reminds us of our territorial embeddedness. State borders become visible the moment

3 When speaking of the state 'acting' I simplify it as a more-or-less coherent collective actor. Obviously, internal factions (ministries, politicians, branches of the military, the judiciary, etc.) within states often pursue divergent policies (Wight 2004).

they impact social behavior but rarely otherwise.[4] These borders may align with physical territoriality, e.g., through the server location principle which holds that states have legal jurisdiction over servers which are physically located within that nation's territory. They may also diverge. Given the requisite resources and power, states can attempt to create regulatory territories which expand the reach of a state's laws and regulations in extraterritorial ways.[5] The structure of cyberspace and of internet governance makes such a differentiated approach possible, sometimes even necessary. States have great control over infrastructure localized in their country but little control over global aspects of cyberspace. However, very powerful countries like the United States or coalitions like the EU can hope to make extraterritorial claims stick.

The creation of regulatory territories rests on an expansive claim to jurisdiction. Jurisdiction is one of the foundational corollaries of sovereignty—the state should have the power to legally arbitrate everything that happens within its territory. The location principle is the traditional way of assigning jurisdiction over acts that involve multiple countries. Cyberspace has made this line of legal reasoning much more complicated because acts on the internet create a multitude of "territorial contacts and thus jurisdiction, for example, on the basis of where the server is located, where the content is viewed, where the content is uploaded, where the content is deliberately directed to, where effects are felt, etc." (Ryngaert 2015, 63; also Berman 2002). Absent a rule for adjudicating between jurisdiction claims, there are few legal limits on states' claims for quasi-global regulatory territories. For instance, there is an unresolved dispute between the French Data Protection Agency (CNIL) and Google relating to the European Union's *Right to be Forgotten*, where the CNIL demands that Google enforce its orders to delist personal information relating to a claimant from Google's search results globally, not just for users geolocated in the EU (Daskal 2018, 214–218).

Regulatory territorialization is but one of the instruments that states have at their disposal, and it is a great example of the overall strategy how states

4 Incidentally, 'corporate borders' are much more easily visible. Having to sign up and/or pay to access a company's 'walled garden' or digital ecosystem creates a system of login screens that are visible manifestations of the borders of this particular company's offer. With the spread of electronic IDs, we may see similar manifestations of state borders when it comes to accessing official services.

5 I use 'extraterritorial' in the legal sense, meaning the ability of a state to apply its laws beyond its borders.

approach cyberspace. Geoffrey Herrera (2007) has aptly summarized this as "a simultaneous double move: the territorialisation of cyberspace and the deterritorialisation of state security" (2007, 68). In other words: states are adapting cyberspace to be more amenable to the territorial framework within which states operate, and states adapt themselves to the decentralized topography of cyberspace.

These practices and strategies did not emerge fully formed and are continually evolving. For example, the system of server-based jurisdiction, which emerged in the 1990s, was being challenged by geographically decentralized cloud computing in the 2000s and 2010s (Amoore 2018), which led to debates whether the cloud transcends geography (Svantesson 2016), whether "independence of the cloud from geography is a fiction because the cloud relies on a physical infrastructure that must be located in an actual physical space" (Trimble 2018, 630), or whether such territorial location should matter at all because of the randomness by which the location of data is assigned (Berman 2018). Legal approaches to the cloud have evolved considerably over the past few years. Some countries use data localization laws to limit data transfer or try to compel companies to surrender data stored in their clouds to national courts and prosecutors. The United States CLOUD Act of 2018 and the European Commission's 'e-evidence' proposal formally empower judiciaries to access cloud-stored data, thus moving away from the territoriality principle of jurisdiction (Berman 2018; Burchard 2018; Daskal 2018).

Beyond these continuously evolving debates, there are nascent, though as yet unrealized possibilities to make cyberspace map even closer to offline geographies by revising fundamental protocols that govern the internet's functionality (Mueller 2017, 81–84). One such proposal would be to move the Domain Name System (DNS), which translates domain names into the numerical format that the Internet Protocol uses, from a global system into a system of interconnected national Domain Name Systems, substantially increasing the scope for control by national regulators.

5. Analyzing State B/Orders in Cyberspace

Just as with cyberspace itself, b/orders in cyberspace must be thought as technopolitical assemblages of hardware/infrastructure, code, data, and social relations (Illustration 1). Borders are specific arrangements of these

four elements whose core purpose is the signaling of an inside and an outside of the state power container, to use Giddens' term.[6]

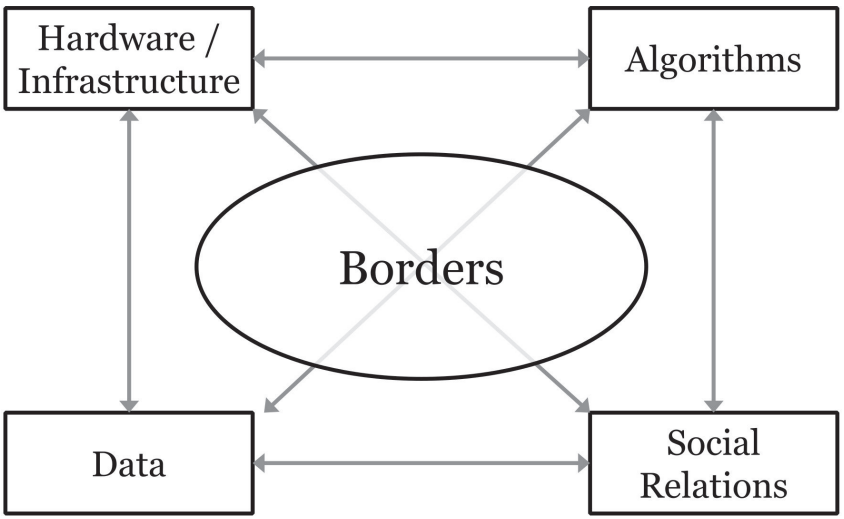

Illustration 1: The Cybernetic B/Order as Technopolitical Assemblage. Source: author.

State borders in cyberspace take a variety of forms. They draw heavily on symbolic and representational elements, but they have the same purposes as any other border: regulating access and enacting territory. All this proceeds from the widespread normative assumption that all online activity that occurs in a country (because users, servers, or data can be located there) should be treated as part of a corresponding cyberspace territory. This approach—which was already prevalent in the early days of the internet—has been facilitated by the growth of geolocation technologies which allows for the mapping of online activity onto physical geographies. Discourses about cybersovereignty, data sovereignty, or digital sovereignty, which are championed by countries as diverse as Russia, China, France,

6 As such, borders are not only employed and enacted by states but also by other actors. Corporations use sign-up and payment requirements to regulate access to their digital spaces. Communities of private users employ social mechanisms of ingrouping and outgrouping, such as the use of slang language, and methods of self-governance like content moderation to regulate membership and belonging.

and Germany, are further evidence of this belief (Couture/Toupin 2019; Pohle/Thiel 2020; Hummel et al. 2021).

There is a variety of instruments available to states seeking to (re-)create borders in cyberspace. National firewalls are one of the best-known ways for governments to both communicate their territorial claim and to display power within the bounded space (Walters 2006). These firewalls combine a range of filtering mechanisms like IP blocking and keyword searches to censor discussions about sensitive topics and deny access to websites deemed subversive. The *Great Firewall of China* is the best-known example, but other countries have developed, or are developing, similar systems of censorship (Jiang 2010). North Korea is probably the most extreme example where, until recently, users could only access the countrywide *Kwangmyong* intranet. Even today, access to select internet sites is only possible under tight restrictions and government scrutiny.

Internet kill switches are the ultimate display of power. Controlling the national telecommunications infrastructure and being able to shut off the entire national internet, or parts thereof, in a controlled fashion and for extended periods of time, demonstrates the sovereign capability of the state (DeNardis 2014, 199–221). And while this is clearly a tactic of last resort, there have been shutdowns lasting days or weeks, partial shutdowns targeting parts of the country or certain times of the day. The difficulty of a shutdown is determined by the network structure: the smaller the number of 'choke points', e.g. Internet Service Providers and autonomous systems, the easier it is to do (Roberts et al. 2011; Belson 2017).

Data localization laws have also become very popular in the wake of the 2013 Snowden revelations of widespread US surveillance of the internet. Their stated aim is to safeguard data protection for citizens and corporations, mandating "that certain types of data collected in a particular country be stored and/or processed within that country" (Bowman 2015) and regulating which companies are allowed to manage these kinds of data based on whether the corporation falls under national jurisdiction. As Baur-Ahrens (2017) points out, the routing and storage requirements of such laws require "changes to the basic functioning of the underlying internet infrastructure" (2017, 37).

National firewalls, kill switches, and data localization laws reinforce container notions of territorial statehood through the enactment of borders. They clearly communicate territorial boundaries and openly display state control over territory. Another way of reifying national territory is

through country-code Top-Level Domains (ccTLDs) such as .ru, .cn, or .de, which symbolically connect a virtual domain to a country (Mueller/Badiei 2017; Schünemann 2019).[7] Nonetheless, ccTLDs have legal repercussions: domain name registries, i.e., the agencies administering ccTLDs, typically mandate through their terms and conditions that registrants of a national domain follow national laws.

Notions of cyberwar, cyberdefense, and cyberdeterrence also reterritorialize cyberspace into separate state containers.[8] First, such discourses and strategies reify certain network nodes, e.g., critical national infrastructures or other assets associated with military or intelligence branches of the state (Stevens 2012, 151), as forming an integral part of a national territory, any attack on which is considered grounds for retaliation. Cyberwar strategists often point to the risks that hostile cyber operations can pose for infrastructure in physical space, such as electrical grids, financial networks, or railways, thus connecting the "national cyber-territory" with physical state territory (Warner 2012, 795–798). Second, even the act of naming certain activities reinforces notions of statehood. In the narrowest sense of the term, 'cyberwar' is reserved for actions conducted by states and state proxies (Lupovici 2016, 326–327), whereas actions by/on private actors are commonly described as 'cyberattacks' or 'cyber operations', although given the widespread state practice of using proxies to complicate attribution and provide plausible deniability, the difference between state and private actors is blurry (Maurer 2017).

Cyberwar and the state territorial container in cyberspace are mutually constitutive. For this reason, national security apparatuses have proclaimed cyberspace to be the "fifth domain of warfare" (after land, sea, air and space) (Manjikian 2010, 384–388; Dunn Cavelty 2015). As a result, many countries have expanded or are expanding their cyberdefense and cyberwarfare capabilities (Fliegauf 2016, 79; Mueller 2017, 73–77). The division

7 This does not apply to all countries. States like Tuvalu or Tonga market their respective ccTLDs, .tv and .to, globally without reterritorializing a national territory in cyberspace.

8 There are opposing views on the likelihood of cyberwar, mostly due to different definitions of the term (Rid 2012; Stone 2013; Warner 2012). These definitional disagreements are further complicated by the fact that cyber operations will be integrated into larger campaigns of information warfare or hybrid warfare (Libicki 2017; Lupovici 2016). Offensive cyber operations are not just conducted by state actors themselves but also by private actors working for, or being tolerated by, a state benefactor. These proxies offer technical aptitude and plausible deniability to states, making the attribution of an attack more complex (Maurer 2017, 22–25).

of inside and outside, which is so fundamental to any notion of statehood (Walker 1993), is also important in doctrinal debates about cyberdefense. In other words, should cyberdefense be solely about protecting the territory, or should it also include active measures ('active defense', 'hacking back', i.e., establishing a permanent forward presence in systems of hostile states) that reach beyond the territory and deterritorialize the site of conflict?

6. Territorial Practices

As the above discussion shows, state borders in cyberspace have a certain ephemeral quality compared to borders in the physical world. They do not exist in fixed places where they can be made easily and permanently visible, they are not subject to diplomatic negotiation and demarcation (at least not in the traditional sense of bilateral treaties and boundary management), and the international body of norms governing what borders are and how they should be managed is difficult to apply to the cybernetic environment. Nonetheless, state borders clearly exist in cyberspace—we simply have to adjust our focus to see them. Cybernetic borders mostly become visible in the moment, in the act of preventing or regulating a certain activity, such as accessing prohibited content or transferring data.

Accordingly, this paper takes a practice-based approach to develop a systematic framework for the study of border assemblages in cyberspace. Inspired by notions of bordering practices (Côté-Boucher et al. 2014; Newman 2006) and the Foucauldian approach to territory as a political technology by Stuart Elden (2013), it introduces territorial practices as a technique of governance (also Painter 2010). Following Brighenti (2010), the aim is to analyze how actors and technologies produce territory (Adamson 2016; Wagner/Vieth 2016, 219–220). Thinking about territorial practices in cyberspace allows us to ask how practices constitute digital territories and how these territories impact future practices. In my understanding of practice, I follow the definition offered by Adler/Pouliot (2011): "practices are socially meaningful patterns of action, which, in being performed more or less competently, simultaneously embody, act out, and possibly reify background knowledge and discourse in and on the material world" (2011, 4). Adler/Pouliot (2011) identify five elements of practice: (1) practices are performative, (2) practices follow regular patterns without determining behavior, (3) practices are interpreted and understood in terms of social relations, (4) practices depend on background knowledge that gives them

a particular purpose, and (5) practices link discourses with the material world because the discourses give meaning to the act (2011, 6–7). Importantly, although it is developed for this particular case, this set of practices is not specific to borders in cyberspace. This taxonomy draws on general geographic literature, and the language used here can be adapted to other non-digital or less digital environments.

So, what can be considered a territorial practice? I have discussed this in greater detail elsewhere (Lambach 2021b) but for the purposes of cyberspace, a territorial practice is defined as any practice whose performance is aimed at deconstructing existing territories or (re-)creating new territories in a digital environment. Based on suggestions from Blacksell (2006, 21–27) and Vollaard (2009), I suggest a threefold taxonomy of territorial practices that are applicable to cyberspace. These kinds of practices mirror Sack's three aspects of territoriality as discussed above—the creation of a space, the delimitation of a space, and control over a space:

1. Reification of a territory, by giving it a name and inscribing it with purpose and meaning, e.g., through political discourse, or as a statistical or administrative category, in art, or in popular media;
2. Communication of territorial boundaries, e.g., through ccTLDs or designation of critical national infrastructure, making a clear distinction between inside and outside possible;
3. Regular displays of power, e.g., through policing of online behavior, geo-blocking of content, taxation of e-commerce, data localization laws and other forms of rulemaking, or surveillance.

Taking cyberwar doctrines as an example of a territorial practice, all three elements can be easily discerned. First, cyberwar doctrines reify certain objects and entities as national territory to be defended against digital attacks and hostile actors. They also create representations of the country in defense doctrines which are then enacted administratively. Second, by designating targets as objects of cyberdefense through strategic doctrines, white papers and other governmental or military speech acts, the border is communicated to would-be attackers. This is frequently tied into public declarations of likely responses to perceived hostile acts such as NATO's 2019 declaration that cyberattacks may trigger collective defense under Article 5.[9] Third, cyberwar doctrines are also displays of power. States create instruments to regulate behavior in these protected spaces through

9 https://www.nato.int/cps/en/natohq/news_168435.htm, 8/5/2021.

the enactment of laws, such as through the development of defensive and offensive cyber capabilities (Dunn Cavelty 2013).

7. Conclusion

This paper has argued for an engagement with borders in cyberspace. This is something that research on the politics of the internet still struggles with, and debates too often recur to internet exceptionalist viewpoints (e.g. Mueller 2020). It is pointless to ask whether states should have a hand in governing cyberspace—they clearly already do. Similarly, the talk of borders leading to a fragmentation or pluralization of the internet is overblown. State borders and bordering are everyday practices in cyberspace, in addition to those enacted by other actors, and so far, the internet has managed to survive more or less intact (Lambach 2020b). Certainly, the character of the internet has changed from the more free-wheeling, user-driven days of Usenet to today's glossier, corporatized version but that has little to do with some supposed introduction of state borders into a pristine electronic wilderness.

This discussion should also be of interest to border studies, which have evolved considerably over the past decades, with this edited volume just one of many attempts to grapple with the arising complexities of contemporary borders. Border studies have highlighted the decentering of borders and the role of technologies in border governance, both also major themes of this paper. And yet, it seems as if border studies approaches the digital mainly as an instrument of border control. This is one important dimension of it, to be sure, and this perspective has been very informative for our understanding of borders as semi-permeable sorting devices and data capturing screens (Mau 2010; Pallister-Wilkins 2016). However, I believe that this perspective somewhat underestimates how the digital is not merely an enhancement of existing borders but the degree to which digital tools and the digital environment are constitutive of these borders. As the digital transformation progresses and digital and physical worlds become ever more enmeshed, borders will continue to become more complex. We might not yet perceive where this process will take us but paying attention to both sides of the coin is surely advisable.

8. References

Adamson, Fiona B. (2016): Spaces of Global Security: Beyond Methodological Nationalism. In: Journal of Global Security Studies 1, no. 1, 19–35.

Adler, Emanuel/Pouliot, Vincent (2011): International Practices. In: International Theory 3, no. 1, 1–36.

Agnew, John (1994): The Territorial Trap: The Geographical Assumptions of International Relations Theory. In: Review of International Political Economy 1, no. 1, 53–80.

Amoore, Louise (2018): Cloud Geographies: Computing, Data, Sovereignty. In: Progress in Human Geography 42, no. 1, 4–24.

Anderson, James/O'Dowd, Liam (1999): Borders, Border Regions and Territoriality: Contradictory Meanings, Changing Significance. In: Regional Studies 33, no. 7, 593–604.

Balzacq, Thierry/Cavelty, Myriam Dunn (2016): A Theory of Actor-Network for Cyber-Security. In: European Journal of International Security 1, no. 2, 176–198.

Barlow, John Perry (1996): A Declaration of the Independence of Cyberspace. 2/08/1996. https://www.eff.org/cyberspace-independence, 01/12/2023.

Baur-Ahrens, Andreas (2017): The Power of Cyberspace Centralisation: Analysing the Example of Data Territorialisation. In: Leese, Matthias/Wittendorp, Stef (eds.): Security/Mobility: Politics of Movement. Manchester: Manchester University Press, 37–56.

Belson, David (2017): The Migration of Political Internet Shutdowns. In: Internet Intelligence 2018: Oracle Dyn Blog.

Berg, Sebastian/Rakowski, Niklas/Thiel, Thorsten (2020): The Digital Constellation. In: Weizenbaum Institute for the Networked Society – Weizenbaum Series, no. 14. Berlin: The German Internet Institute, DOI: 10.34669/wi.ws/14.

Berman, Paul S. (2002): The Globalization of Jurisdiction. In: University of Pennsylvania Law Review 151, no. 2, 311–545.

Berman, Paul S. (2018): Legal Jurisdiction and the Deterritorialization of Data. In: Vanderbilt Law Review 71, no. En Banc 11, 12–32.

Blacksell, Mark (2006): Political Geography. London: Routledge.

Boehme-Neßler, Volker (2009): Das Ende des Staates? Zu den Auswirkungen der Digitalisierung auf den Staat. In: Zeitschrift für Öffentliches Recht 62, no. 2, 145–199.

Bourdieu, Pierre (1989): Social Space and Symbolic Power. In: Sociological Theory 7, no. 1, 14–25.

Bowman, Courtney M. (2015): Primer on Russia's New Data Localization Law. In: Blaney, Ryan P. (ed.): Proskauer on Privacy. https://privacylaw.proskauer.com/2015/08/articles/data-privacy-laws/a-primer-on-russias-new-data-localization-law, 01/12/2023.

Brighenti, Andrea M. (2010): On Territorology: Towards a General Science of Territory. In: Theory, Culture and Society 27, no. 1, 52–72.

Büger, Christian/Gadinger, Frank (2014): International Practice Theory: New Perspectives. Basingstoke: Palgrave Macmillan.

Burchard, Christoph (2018): Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen–Teil 1: Hintergründe des Kommissionsentwurfs zum grenzüberschreitenden Zugang zu elektronischen Beweismitteln im Strafermittlungsverfahren wie auch zum sog. Microsoft Ireland Case. In: Zeitschrift für Internationale Strafrechtsdogmatik 13, no. 6, 191–203.

Buzan, Barry (2004): From International to World Society? English School Theory and Social Structure of Globalisation. Cambridge: Cambridge University Press.

Carter, David B./Goemans, H. E. (2014): The Temporal Dynamics of New International Borders. In: Conflict Management and Peace Science 31, no. 3, 285–302.

Castells, Manuel (1996): The Rise of the Network Society. Malden: Blackwell.

Chenou, Jean-Marie (2014): From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-stakeholderism, and the Institutionalisation of Internet Governance in the 1990s. In: Globalizations 11, no. 2, 205–223.

Côté-Boucher, Karine/Infantino, Federica/Salter, Mark B. (2014): Border Security as Practice: An Agenda for Research. In: Security Dialogue 45, no. 3, 195–208.

Couture, Stephane/Toupin, Sophie (2019): What Does the Notion of "Sovereignty" Mean When Referring to the Digital? In: New Media & Society 21, no. 10, 2305–2322.

Daskal, Jennifer (2018): Borders and Bits. In: Vanderbilt Law Review 71, no. 1, 179–240.

Deibert, Ronald J. (2003): Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. In: Millennium 32, no. 3, 501–530.

Deibert, Ronald J./Rohozinski, Rafal (2010): Liberation vs. Control: The Future of Cyberspace. In: Journal of Democracy 21, no. 4, 43–57.

DeNardis, Laura (2014): The Global War for Internet Governance. New Haven: Yale University Press.

Dunn Cavelty, Myriam (2013): From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. In: International Studies Review 15, no. 1, 105–122.

Dunn Cavelty, Myriam (2015): Die materiellen Ursachen des Cyberkriegs: Cybersicherheitspolitik jenseits diskursiver Erklärungen. In: Journal of Self-Regulation and Regulation 1, no. 1, 167–184.

Elden, Stuart (2013): The Birth of Territory. Chicago: University of Chicago Press.

Farrell, Henry (2006): Regulating Information Flows: States, Private Actors, and E-Commerce. In: Annual Review of Political Science 9, no. 1, 353–374.

Feyissa, Dereje/Hoehne, Markus V. (2010): State Borders and Borderlands as Resources: An Analytical Framework. In: Feyissa, Dereje/Hoehne, Markus V. (eds.): Borders and Borderlands as Resources in the Horn of Africa. London: James Currey, 1–26.

Fliegauf, Mark T. (2016): In Cyber (Governance) We Trust. In: Global Policy 7, no. 1, 79–82.

Geiger, Danilo (2008): Turner in the Tropics: The Frontier Concept Revisited. In: Geiger, Danilo (ed.): Frontier Encounters: Indigenous Communities and Settlers in Asia and Latin America. Copenhagen: International Work Group for Indigenous Affairs, 77–215.

Giddens, Anthony (1985): A Contemporary Critique of Historical Materialism, Vol. 2: The Nation-State and Violence. Cambridge: Polity Press.

Herrera, Geoffrey (2007): Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space. In: Dunn Cavelty, Myriam/Mauer, Victor/Krishna-Hensel, Sai F. (eds.): Power and Security in the Information Age: Investigating the Role of the State in Cyberspace. Aldershot: Ashgate, 67–93.

Herz, John H. (1957): Rise and Demise of The Territorial State. In: World Politics 9, no. 4, 473–493.

Hummel, Patrik/Braun, Matthias/Tretter, Max/Dabrock, Peter (2021): Data Sovereignty: A Review. In: Big Data & Society 8, no. 1, DOI: 10.1177/2053951720982012.

Jiang, Min (2010): Authoritarian Informationalism: China's Approach to Internet Sovereignty. In: SAIS Review of International Affairs 30, no. 2, 71–89.

Johnson, David R./Post, David G. (1996): Law and Borders – The Rise of Law in Cyberspace. In: Stanford Law Review 48, no. 5, 1367–1402.

Kahler, Miles (2006): Territoriality and Conflict in an Era of Globalization. In: Kahler, Miles/Walter, Barbara F. (eds.): Territoriality and Conflict in an Era of Globalization. Cambridge: Cambridge University Press, 1–21.

Kitchin, Robert M. (1998): Towards Geographies of Cyberspace. In: Progress in Human Geography 22, no. 3, 385–406.

Kopytoff, Igor (1987): The Internal African Frontier: The Making of African Political Culture. In: Kopytoff, Igor (ed.): The African Frontier: The Reproduction of Traditional African Societies. Bloomington: University of Indiana Press, 3–84.

Lambach, Daniel (2020a): The Normative Order of the Territorial State. In: Kettemann, Matthias C. (ed.): Navigating the Frontiers of Normative Orders: Interdisciplinary Perspectives. Frankfurt/M.: Campus., 44–58.

Lambach, Daniel (2020b): The Territorialization of Cyberspace. In: International Studies Review 22, no. 3, 482–506.

Lambach, Daniel (2021a): The Functional Territorialization of the High Seas. In: Marine Policy 130, August, DOI: 10.1016/j.marpol.2021.104579.

Lambach, Daniel (2021b): Space, Scale, and Global Politics: Towards a Critical Approach to Space in International Relations. In: Review of International Studies 48, no. 2, 282–300.

Libicki, Martin C. (2017): The Convergence of Information Warfare. In: Strategic Studies Quarterly 11, no. 1, 49–65.

Lisle, Debbie (2017): Failing Worse? Science, Security and the Birth of a Border Technology. In: European Journal of International Relations 24, no. 4, 887–910.

Lupovici, Amir (2016): The "Attribution Problem" and the Social Construction of "Violence": Taking Cyber Deterrence Literature a Step Forward. In: International Studies Perspectives 17, no. 3, 322–342.

Mager, Astrid (2018): Internet Governance as Joint Effort: (Re)ordering Search Engines at the Intersection of Global and Local Cultures. In: New Media & Society 20, no. 10, 3657–3677.

Malpas, Jeff (2012): Putting Space in Place: Philosophical Topography and Relational Geography. In: Environment and Planning D: Society and Space 30, no. 2, 226–242.

Manjikian, Mary McEvoy (2010): From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. In: International Studies Quarterly 54, no. 2, 381–401.

Martin-Mazé, Médéric/Perret, Sarah (2021): Designs of Borders: Security, Critique, and the Machines. In: European Journal of International Security 6, no. 3, 278–300.

Mau, Steffen (2010): Grenzen als Sortiermaschinen. In: WeltTrends 18, no. 71, 57–66.

Mau, Steffen/Brabandt, Heike/Laube, Lena/Roos, Christof (2012): Liberal States and the Freedom of Movement: Selective Borders, Unequal Mobility. Basingstoke: Palgrave Macmillan.

Maurer, Tim (2017): Cyber Mercenaries: The State, Hackers, and Power. Cambridge: Cambridge University Press.

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

Mueller, Milton (2020): Against Sovereignty in Cyberspace. In: International Studies Review 22, no. 4, 779–801.

Mueller, Milton/Badiei, Farzaneh (2017): Governing Internet Territory: ICANN, Sovereignty Claims, Property Rights and Country Code Top-Level Domains. In: Columbia Science & Technology Law Review 18, no. 2, 435–491.

Musiani, Francesca (2014): Practice, Plurality, Performativity, and Plumbing: Internet Governance Research Meets Science and Technology Studies. In: Science, Technology & Human Values 40, no. 2, 272–286.

Newman, David (2003): Boundaries. In: Agnew, John/Mitchell, Katharyne/Tuathail, Gearóid Ó. (eds.): A Companion to Political Geography. Malden: Blackwell, 123–137.

Newman, David (2006): Borders and Bordering: Towards an Interdisciplinary Dialogue. In: European Journal of Social Theory 9, no. 2, 171–186.

Paasi, Anssi (2009): Bounded Spaces in a 'Borderless World': Border Studies, Power and the Anatomy of Territory. In: Journal of Power 2, no. 2, 213–234.

Painter, Joe (2010): Rethinking Territory. In: Antipode 42, no. 5, 1090–1118.

Pallister-Wilkins, Polly (2016): How Walls do Work: Security Barriers as Devices of Interruption and Data Capture. In: Security Dialogue 47, no. 2, 151–164.

Pohle, Julia/Thiel, Thorsten (2020): Digital Sovereignty. In: Internet Policy Review 9, no. 4, DOI: 10.14763/2020.4.1532.

Rid, Thomas (2012): Cyber War Will Not Take Place. In: Journal of Strategic Studies 35, no. 1, 5–32.

Roberts, Hal/Larochelle, David/Faris, Rob/Palfrey, John (2011): Mapping Local Internet Control. Cambridge: Berkman Center for Internet and Society. http://cyber.harvard.edu/netmaps/mlic_20110513.pdf, 01/12/2023.

Ruggie, John Gerard (1993): Territoriality and Beyond: Problematizing Modernity in International Relations. In: International Organization 47, no. 1, 139–174.

Ruggie, John Gerard (1998): What Makes the World Hang Together? Neo-Utilitarianism and the Social Constructivist Challenge. In: International Organization 52, no. 4, 855–885.

Ryngaert, Cedric (2015): The Concept of Jurisdiction in International Law. In: Orakhelashvili, Alexander (ed.): Research Handbook on Jurisdiction and Immunities in International Law. Cheltenham: Edward Elgar, 50–75.

Sack, Robert D. (1986): Human Territoriality: Its Theory and History. Cambridge: Cambridge University Press.

Saco, Diana (1999): Colonizing Cyberspace: 'National Security' and the Internet. In: Weldes, Jutta/Laffey, Mark/Gusterson, Hugh/Duvall, Raymond (eds.): Cultures of Insecurity: States, Communities, and the Production of Danger. Minneapolis: University of Minnesota Press.

Scharpf, Fritz W. (1991): Die Handlungsfähigkeit des Staates am Ende des zwanzigsten Jahrhunderts. In: Politische Vierteljahresschrift 32, no. 4, 621–634.

Schünemann, Wolf J. (2019): Strukturaler Nationalismus in der Internet Governance am Beispiel der Country Codes im Domain-Name-System. In: Borucki, Isabelle/Schünemann, Wolf Jürgen (eds.): Internet und Staat: Perspektiven auf eine komplizierte Beziehung. Baden-Baden: Nomos, 167–190.

Simmons, Beth A./Goemans, Hein E. (2021): Built on Borders?: Tensions with the Institution Liberalism (Thought It) Left Behind. In: International Organization 75, no. 2, 387–410.

Stevens, Tim (2012): A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. In: Contemporary Security Policy 33, no. 1, 148–170.

Stone, John (2013): Cyber War Will Take Place! In: Journal of Strategic Studies 36, no. 1, 101–108.

Strange, Susan (1996): The Retreat of the State: The Diffusion of Power in the World Economy. Cambridge: Cambridge University Press.

Svantesson, Dan J. B. (2016): International Law and Order in Cyberspace—Cloud Computing and the Need to Revisit the Foundations of "Jurisdiction". www.aspen.review/article/2017/international-law-and-order-in-cyberspace-cloud-computing-and-the-need-to-revisit-the-foundations-of-jurisdiction, 01/12/2023.

Trimble, Marketa (2018): Territorialization of the Internet Domain Name System. In: Pepperdine Law Review 45, no. 4, 623–684.

Vollaard, Hans (2009): The Logic of Political Territoriality. In: Geopolitics 14, no. 4, 687–706.

Wagner, Ben/Vieth, Kilian (2016): Was macht Cyber? Epistemologie und Funktionslogik von Cyber. In: Zeitschrift für Außen- und Sicherheitspolitik 9, no. 2, 213–222.

Walker, Rob B. J. (1993): Inside/Outside: International Relations as Political Theory. Cambridge: Cambridge University Press.

Walters, William (2006): Border/Control. In: European Journal of Social Theory 9, no. 2, 187–203.

Warner, Michael (2012): Cybersecurity: A Pre-history. In: Intelligence and National Security 27, no. 5, 781–799.

Wight, Colin (2004): State Agency: Social Action Without Human Activity? In: Review of International Studies 30, no. 2, 269–280.

Winner, Langdon (1980): Do Artifacts Have Politics? In: Daedalus 109, no. 1, 121–136.

Wu, Tim (2010): Is Internet Exceptionalism Dead? In: Szoka, Berin/Marcus, Adam (eds.): The Next Digital Decade. Washington: TechFreedom, 179–188.

Zeh, Juli (2013): Es geht um etwas anderes: Merkel und das "Neuland". www.stern.de/politik/deutschland/merkel-und-das-neuland-es-geht-um-etwas-anderes-2030451.html, 6/27/2013.

Author information

Lambach, Daniel, PD Dr., Political Scientist, Heisenberg Fellow at the Research Centre Normative Orders (University of Frankfurt), *Privatdozent* at the Faculty of Social Sciences and Senior Associate Fellow at the Institute for Development and Peace (both University of Duisburg-Essen); research interests: territoriality, sovereignty, agency, the digital transformation.