The power of cyberspace centralisation: analysing the example of data territorialisation

Andreas Baur-Ahrens

IN 2013, SHORTLY after the revelations by Edward Snowden of the existence of mass surveillance programmes operated by his former employer the National Security Agency, Deutsche Telekom as one of the largest European telecommunications providers put forward the idea of a national and eventual Schengen routing of Internet traffic. National routing means that information exchanged between domestic servers and computers should travel only over domestic infrastructure and therefore remain within territorial borders – borders that traditionally play a minor role in cyberspace. The mobility of data traffic should be limited and regulated for the sake of data security by keeping sensitive information out of the reach of Anglo-American intelligence agencies. The idea of data security is also a driving force behind several similar initiatives and proposals to territorialise Internet traffic routing or data storage and has an impact beyond its technical implications.

As national routing requires changes to the basic functioning of the underlying Internet infrastructure, it affects also some of the core principles of the traditional design of cyberspace: decentrality without hierarchies with the aim of providing high availability and security. I argue that data territorialisation including national routing and storage requirements contributes to a general trend of cyberspace centralisation. Furthermore, I analyse the proposed changes to the Internet infrastructure with regard to power relations.

Power and its analysis is an important part of mobility studies as the regulation and control of mobility reflects and reproduces power relations (Sheller and Urry 2006: 211). Imaginaries of security legitimise the regulation and control of data mobility, which affects also social relations beyond their technical implementations. In the case of data territorialisation, this is done mainly by the use of infrastructure, as well as algorithms and code that organise and steer data traffic flows. This is of particular interest as ‘the founders of the Internet embraced a design that distrusted centralized control’ (Goldsmith and Wu 2006: 23). It was

‘the architecture of the network itself that prevented the exercise of hierarchical organised authority, be it in the way of censorship, inequality, or the creation of commercial monopolies’ (Hofmann and Holitscher 2004: 412, own transl.). Cyberspace was seen by some as a completely power-free space, as the famous ‘Declaration of the Independence of Cyberspace’ by John Perry Barlow (1996) illustrates.

Cyberspace centralisation as limiting and steering information mobility is challenging this traditional architecture and the principles behind it. As we are living in an increasingly interconnected world, changes of power relations within the Internet infrastructure and connected structures and actors should not be underestimated.

The conceptualisation of power that I use is a constitutive one as it looks at the underlying relations of power that structure and shape identities, interests, and meanings in a co-constitutive way, and accepts the relevance and impact that technology has on social relations (and vice versa). As the analysis shows, there are roughly three traceable changes to power relations: (1) telecommunications providers become more important, gain more influence, and their identity as security actors is promoted; (2) government authorities’ possibilities for action are enhanced and states’ interference with the network’s functions as well as the existence of territorial borders and their enforcement is legitimised; (3) data territorialisation is contributing to a general transition from a passive and dumb network to an increasingly intelligent and steering one, leading also to more passive and dependent users.

This chapter is structured as follows. I first give an overview of the concept of cyberspace and its technical basics and then present the conceptualisation of power that I use in order to analyse data territorialisation. In the empirical part I describe (1) the national routing and data localisation initiatives, followed by (2) why data territorialisation is a centralising process, and (3) an analysis of the power relations and changes thereof that are connected to the empirical examples discussed.

Basic concepts: cyberspace, Internet infrastructure, and routing

The term ‘cyberspace’, once coined in science fiction for ‘cybernetic space’, has a long history of describing a virtual and so-called *separate* space from reality. ‘Cyberspace’ has been largely criticised for being too vague and misleading (e.g., Cohen 2007: 227; Thiedeke 2004) and was even called ‘dead’ by Fadi Chehadé, president of the Internet Corporation for Assigned Names and Numbers (ICANN) (Küchemann 2014). Nevertheless, although the idea of a (utopian) parallel world of virtuality has been mostly abandoned, the metaphor of cyberspace is still efficacious, predominant, and consequently worthy of attention (see Cohen 2007: 226, 235). However, the notion of cyberspace needs more

specification. This is why I use the word cyberspace mainly with reference to its technical elements: cyberspace is to be understood as an extending part of social reality, and not as a separate or virtual realm. Following Ronald Deibert and Rafal Rohozinski (2010a: 15–16) ‘[c]yberspace describes the human-made domain for action that exists as a consequence of an interconnected and inter-dependent global communications and computing infrastructure’. Thus, this definition includes all computers, devices, and servers, their connecting commercial or public infrastructure (routers, wires, data centres), as well as traffic protocols and standards. Following Mimi Sheller and John Urry (2006: 210, 212; see also Söderström et al. 2013: 7), it is these ‘multiple fixities and moorings’ materialised by immobile infrastructures, regulatory frameworks, and social practices that organise the flow of information. In order to understand the (irregular) movement of data and also its limitations and regulations, one has to look at the fixed infrastructures and ‘gates’ governing its mobility (Sheller and Urry 2006: 212).

In the following paragraphs I give a brief introduction to the technical basics of the Internet infrastructure and its predecessor Arpanet. These essentials are: (1) in contrast to traditional telephone systems with fixed and linear wires between all points of communication, the Internet consists of a chaotic web of wires, hubs, and nodes; and (2) the communication protocols of the Internet coordinate and govern the traffic routes and determine how data finds its way to its destination within the network and thereby organise the communication flows. The Transmission Control Protocol (TCP) defines how computers may exchange information, whereas the Internet Protocol (IP) defines how computers are addressed and therefore how they can be found. The TCP and IP represent the technical implementation of a relatively simple idea to build an open, minimalistic, and neutral communications platform (Goldsmith and Wu 2006: 23). ‘The core architectural guideline of the Internet is the end-to-end-principle. It is based on the idea that, in a distributed computing network, functionality should be provided by end hosts rather than by the network itself, using ... TCP/IP’ (Glen 2014: 644). While the functions and the governance of the network are performed by the clients, the network provides only the basic and passive foundation for data exchange.

The TCP and IP form a simple, robust, and neutral communications network. Simple since it needs little information and oversight to function, robust since it reacts dynamically to errors and failures and re-establishes connections by routing around the error, and neutral since it does not look at the content of the information exchanged. The aim of its infrastructural design was to secure communications even in cases of attack on or failure of large parts of the system, which is why a self-organising, non-hierarchical, and therefore almost completely decentral technology was developed. The idea behind this principle was to put the functionality of the network with the clients, and not with the network

itself or in central hubs that would be easy to destroy. Security by decentrality was one of the main driving forces behind its development as the Internet's predecessor Arpanet was a military communications network. Put differently, the original Internet 'is based on the idea of smart terminals and a dumb network' (Glen 2014: 644). 'Like a daydreaming postal worker, the network simply moves the data and leaves interpretation of the data to the applications at either end' (Lessig 2006: 44). This design made it possible to develop a diverse range of applications, including ones that nobody could have imagined when the Internet was invented – for example email, the World Wide Web (WWW), instant messaging, video-streaming, video-calling, and so on. All of them function on the basis of the same and practically unchanged infrastructure.

As the examples provided partly focus on changes to traffic routing, a more fundamental assessment of the technical characteristics of routing is necessary: data traffic, such as an email or a picture, is split into little data packages that find their way autonomously from the sender to the recipient. It is perhaps easier to understand if one imagined a book with all its pages separated, glued onto postcards, and sent to the recipient, who then puts all the pages back together again. Thereby, '[r]outing ... is the act of finding a path from one place to another on which a packet can travel' (Schluting 2006). In contrast to the postcard example, the packets are not travelling on the same and already known path determined by the mailing company, but each and every packet determines its own route and jumps dynamically from node to node, the so-called routers. Every router decides to which connected router it passes on the packet until it reaches its destination.

Furthermore, the Internet is not a homogeneous (cyber)space but rather a conglomeration of about 50,000 distinct subnetworks (Pohlmann et al. 2014: 113). Those subnetworks, the networks of Internet service providers or universities, for example, together form the Internet. They are connected via more than 500,000 handover points enabling communication between two or more networks. In simplified terms there are three different ways of connecting subnetworks: transit connections as well as public or private peering agreements. A transit agreement means that a smaller subnet, for instance a small Internet service provider or a data centre, pays a larger provider for access to other networks in accordance to the amount of data handled. In contrast to that, with peering agreements subnetworks connect to each other at handover points and forward traffic from the respective partner networks at no cost – a more equal arrangement than a transit connection. However, there are two versions of peering. Private peering is a bilateral connection between two networks, whilst public peering is peering at a central handover point where several providers can connect. Handover points with public peering are called *Internet Exchange Points* (IXP), and the world's largest IXP is DE-CIX (German Commercial Internet Exchange) in Frankfurt, Germany. To get a better idea of the functioning of an

IXP, one can compare it to a roundabout: a specialised company runs a roundabout where subnetworks can add their roads and connect their traffic. Traffic exchange between all the roads connecting to the roundabout is free, providers have to pay only for their infrastructure and a fee for using the roundabout no matter how much data they exchange.

Thus, between these 50,000 subnetworks there are a great number of connections either by peering or by transit agreements. ‘The interconnection ecosystem is self-organising and highly decentralised. Decisions to interconnect are made independently by the AS [autonomous systems, i.e. subnetworks] ... [E]ven the administrators may not know, a priori, what path traffic will take’ (Hall et al. 2013: 121). ‘[T]he fastest, technically and economically best route’ is calculated dynamically for every packet (Dittler 2013: own transl.). This is why they coordinate their movement in a fraction of a second according to changing capacities and availabilities – yet territorial borders are traditionally not taken into consideration.

Before I turn to the changes that data territorialisation imposes on the traditional network character and data mobility of the Internet, let me first give an overview of the conceptualisation of power used for the analysis.

Constitutive power

The impact of mobility studies lies ‘primarily in their attempt to address explicitly the interplay of mobility and power. They do so with reference to questions of inequality, domination, and constraint’ (Söderström et al. 2013: 6). Furthermore, information technologies have an important impact on our societies and social relations – and how social relations become mirrored in technology:

Struggles over the design and regulation of network protocols and technologies will be a flashpoint for struggles about the shaping of networked space [i.e. social reality enhanced by information technologies] more generally (and vice versa). (Cohen 2007: 255)

It is therefore crucial to investigate how social relations are affected by and affect information technologies, and to track the power of discourses and practices of mobility in creating both movement and stasis (Sheller and Urry 2006: 211). It is also important to analyse what exactly constitutes power relations and how they work. Certainly, power is one of the core concepts of the social sciences and an ‘essentially contested concept’ par excellence (see Swartz 2007: 105). The genealogy of the concept of power is complex and expansive, and here it suffices to focus on a major differentiation in the power debate to clarify my understanding of the concept.

A major divide within power theories lies between a relational and a capacity-based approach (Baldwin (2013: 273–5)). The latter approach implies that

power equals the sum of resources an actor possesses (see for instance Waltz 1979: 131). Based on a relational understanding of power, one can focus on interactions, for example, getting another actor to do something it would not otherwise do (see Dahl 1957: 202–3) or one can look into structural relations, constraints, and empowerment that influence underlying identities and interests themselves (e.g. Lukes 2005). Michael Barnett and Raymond Duvall (2005) provide a comprehensive concept that Stefano Guzzini (2007: 23) calls ‘Lukes-plus-Foucault’: they basically understand ‘power [as] the production, in and through social relations, of effects that shape the capacities of actors to determine their own circumstances and fate’ (Barnett and Duvall 2005: 8). Barnett and Duvall thereby try to capture a very broad range of kinds of power, and also oppose a clear differentiation between actors and structures. For the purpose of this analysis, their constitutive understanding of power¹ provides an appropriate conceptualisation as it is about the general shifts and changes to basic power relations that structure and give meaning to social interaction.

It is from this constitutive understanding of power that I take the idea that power comprises ‘the co-constitutive, internal relations of structural positions ... that define what kinds of social beings actors are’ as well as their ‘social capacities and interests’ (Barnett and Duvall 2005: 18). Furthermore, there are forms of power that constitute ‘all social subjects with various social powers through systems of knowledge and discursive practices of broad and general social scope’ (Barnett and Duvall 2005: 20). These kinds of power are not exercised by specific actors and are not interactional, but work through structural relations, or more diffuse systems of meaning, which is why the authors divide their constitutional power in more structural and productive forms. The latter ties in with post-structural and discursive power concepts. It is influenced for instance by Michel Foucault and conceives of discourse as ‘productive’, as (re)producing meaning systems and as imbued with social power relations. Constitutional power thus (re)produces social identities, practices, and authorisations that exercise discursive forms of power.

In order to investigate constitutive power relations, I analyse the positions of actors and their changes. Questions to be asked are: does the (also perceived) role of an actor change? Do actors have more or fewer options for action? What is their position in relation to other actors, structures, and technology? What general changes to influence and control can be observed? I also look into the more diffuse power relations that can be found in changes of basic identities and meanings. This is done by examining how consequences of data territorialisation have an influence on the exchange of meanings within discourse and on the (re)definition of identities (see Singh 2013). Are there changes to technologies or actors that shape the discourse? This can happen, for example, by giving more authority to a specific meaning or by preferring one meaning over another due to changing technical conditions. In

the following section I take up these types of power as the basis for the empirical analysis of (changing) power relations concerning data territorialisation as an expression of cyberspace centralisation.

National routing initiatives

In the empirical part of this chapter, I analyse data territorialisation and the resulting changes in power relations. The trend of data territorialisation, often called ‘data sovereignty’,² is defined by Dana Polatin-Reuben and Joss Wright (2014: 1) as ‘a catch-all term to describe different state behaviours towards data generated in or passing through national Internet infrastructure [that] has become a topic of significant international debate in the wake of the Snowden revelations’.

Data territorialisation is mostly legitimised by the need to secure cyberspace and contain so-called *cyber threats* (Deibert and Rohozinski 2012: 29–30) such as viruses, attacks, law infringements, fraud, and others that became possible because of the decentral and uncontrolled nature of the Internet. It is with reference to these threats that the structure of the Internet has been changing substantially in favour of further centralisation since the 1990s. But the relation between centrality/decentrality and security is not obvious at all. Both central and decentral designs represent a secure network: decentrality mainly due to the resilience and availability of communication connections, and centrality because of the means of control over actions on the Internet. The idea of a self-healing and self-organising cyberspace where states have at most a gardening and only minimally interfering function has been replaced by the idea of an intensified interventionist function and the need for more control and authority over the network (Dunn Cavelti 2013: 119; Hutter 2014; Mueller et al. 2013: 94).

Examples of centralisation are found in several global trends, for instance in the introduction of filter and gatekeeping technologies (see Deibert et al. 2008), an increased requirement for resilient and accredited infrastructure, and the implementation of de-anonymisation measures (see Kerr and Barrigar 2012), but also in the concentration of the Internet industry, of Internet hubs and data centres (see De Filippi and McCarthy 2012). Moreover, data territorialisation is contributing to cyberspace centralisation.

The process of territorialising data consists of two connected but technologically and regulatory distinct areas: the first one is about the *routing* of data. Roughly speaking, national routing guarantees that data traffic with a domestic origin and destination is not routed via foreign servers. This is sometimes labelled the ‘national Internet’. However, this is misleading as it does not imply a complete shutdown of international data connections. Secondly, data territorialisation is about the location of *data storage*. Some states have already introduced

laws requiring certain data of citizens to be stored on servers that are physically located in their national territories.

Both forced national data storage and national routing initiatives as processes of data territorialisation represent a cyberspace centralisation, although Jack Goldsmith and Tim Wu (2006: 152) describe a form of national routing, the 'bordered Internet', as 'decentralised governance'. My argument is that the centralisation takes place on a deeper level and only thereby allows the kind of decentralisation that Goldsmith and Wu are referring to. They are talking about a dissociation from existing central structures, but in order to achieve that, central structures in the respective area have to be installed first. Furthermore, Goldsmith and Wu's understanding of decentralisation requires a definition of what is 'national' and what is 'international', and one has to gather more detailed information about data traffic: its origin, destination, and possible paths of connection, but also the specific location of data packages, and basic information about the content. To gain this information, the end-to-end-principle (intelligent clients, dumb network) needs to be altered. Centres need to be set up or existing centres have to become smarter in order to evaluate data and apply corresponding rules. There needs to be a centralisation that operates on a much more basic level for the purpose of a seemingly global decentralisation of data storage and routing.

These initiatives ask for predetermined routing lists that are implemented as part of the routers that enable or disable certain routes. Routing becomes less dynamic and needs a categorisation of data packages into foreign ones that travel as dynamically as before and national ones that have to stick to national routes. Data with a domestic origin and destination have to go through national handover points no matter if these are slower, congested, or more expensive.

The advantage claimed by advocates of national routing lies in the fact that data is not passed over to foreign wires and servers and therefore remains physically within the country. In this way it becomes more difficult for foreign authorities to tap, read, or manipulate the data. One of the disadvantages put forward most frequently, however, is a decreasing quality of data traffic as it is more likely to experience overloads and congestions by purposely nationally routed traffic, and on top of that the consequence that alternative routes that increase failure safety and reliability might not be reached. Jonathan Obar and Andrew Clement (2013), for instance, argue for national routing. The authors note that a substantial part of Canadian–Canadian Internet traffic is routed via the United States, and urge for a national routing of Canadian traffic in order to maintain data security.

Yet an important public discussion started in Germany and other European countries after Deutsche Telekom demanded a national and eventual 'Schengen Routing' in a secret meeting at the German Federal Ministry for Economic

Affairs and Energy in October 2013 (see Berke 2013: n.p.). The same demand was put forward publicly at the Cyber Security Summit 2013 (in cooperation with the Munich Security Conference), which 'created a stir and reached high levels of government' (Clauß 2014: n.p., own transl.). The idea made it into the coalition agreement of the new German government in November 2013 (Koalitionsvertrag 2013) and chancellor Angela Merkel claimed that emails of European citizens should not need to travel across the Atlantic and that one had to build up communication networks within Europe (Clauß 2014). Thus, the idea of a national or Schengen routing became a topic within the EU. Whilst Neelie Kroes, the EU Commissioner for Digital Agenda until October 2014, was objecting to national routing, she welcomed European regulations on routing and supported a European cloud infrastructure (see Diersch 2014: 68). These proposals have been debated by US and European information technology industries and the press (see for instance Adhikari 2013; BITKOM 2013; Dittler 2013; Gropp 2014; USTR 2014).

In several other countries national routing has not been put forward as a separate and independent measure, but has been implemented as part of larger isolation and shielding programmes, for instance in China and Iran (see the so-called halal Internet or Great Firewall). However, the foci and purposes of these programmes are not comparable to standalone national routing.

Polatin-Reuben and Wright (2014) as well as Anupam Chander and Uyên Lê (2014) give an overview of regional routing and data localisation regulations in several countries. Since 2010, Malaysia has required data of Malaysian citizens to be stored on domestic servers (Chander and Lê 2014: 21); since 2012 health data of Australians has been subject to national storage regulations; South Korea demands domestic storage of geographic data; and Brazil discussed national storage regulations when passing the Marco Civil in 2013, but weakened the requirements at the last moment (Polatin-Reuben and Wright 2014: 3).

Deutsche Telekom proposed to the German Federal Government and the European Union (EU) to begin with a German national routing and to later extend this to a Schengen routing in order to keep US and British intelligence agencies out of the data flow in the Schengen area. However, there has not been a regulation on European or national routing yet. Deutsche Telekom has introduced in cooperation with other German providers an initiative called 'Email made in Germany' promising that emails are stored on servers on German soil. In November 2014, Deutsche Telekom added the affirmation that all emails sent between their customers' email accounts do not leave the German Internet infrastructure (see Heuzenroth 2014).

In the following section, I analyse the ideas, proposals, and implementations of different forms of data territorialisation with regard to constitutive power relations.

Analysis of the power relations of national routing

As mentioned above, I will analyse in this section (potential) changes in co-constitutive power relations that go along with centralisation processes. For the analysis of structural and material power relations, it is helpful to look at the positions of actors and their (perceived) roles and options for action. One way of analysing courses of action and their transformation within the technical realm of cyberspace is to identify potential points of control and the actors who have access to them (see Clark 2012; Deibert and Rohozinski 2012: 24). In the present case of data territorialisation through routing and storage regulations, the most obvious points of control are routers and national data centres.

Furthermore, technical configurations matter not only by providing the material basis for structural relations, but technology can also have a normalising and empowering impact (see Hofmann and Holitscher 2004: 414; Fuhrmann 2002: 118). In order to capture these productive power relations creating centralisation through data territorialisation, I focus on changing systems of meaning. How are definitions and interpretations altered? How are identities and normalities shaped? How are these meanings and definitions connected to practices and policies that thereby appear as normal, possible, imaginable, legitimate, or desirable (see Barnett and Duvall 2005: 22)?

The following power analysis is made up of three parts with the first focusing on changes to the role of Internet service providers, the second looking into changes to the options and identities of government authorities, and the last providing a more thorough analysis of the fundamental technological changes of the Internet infrastructure and their consequences.

Internet service providers

Internet service providers (ISPs) supervise important data traffic control points by operating the routers where national and international data traffic has or would have to be separated. By introducing national routing, their role then changes from the 'daydreaming postal worker' to a security actor since national routing is framed as significant for data security. By protecting against foreign spying, national security becomes a goal of private telecommunications providers. Having to distinguish between national data worthy of protection and international unprotected data, the self-understanding, identity, and role of ISPs within the telecommunications sector, the media industry, and in relation to government agencies changes. 'ISPs and telecom companies now help to determine the boundaries between security and privacy – indeed they have even begun to shape the national surveillance architecture' (Herrington and Aldrich 2013: 302). Internet service providers become partners in the governmental security apparatus and can exercise a new kind of control over

data traffic, information mobility, and thereby over all Internet users in the relevant area.

A comparison with the development of the Internet in Europe during the 1970s gives interesting insights: the Internet protocol suite (TCP/IP) developed in the United States – and characterised by openness, decentrality, and flexibility – competed for global acceptance with a standard called *x.25*, which was supported by European countries and telecommunications regulatory bodies. ‘Under *x.25* virtual circuits, the control and accountability of the network would be mainly in the hands of public network providers at the expense of private computer owners’ (Castells 2001: 26). European post and telecommunications regulatory bodies wanted public national networks that connected to networks of foreign countries only via a few handover points. On the one hand, public networks could then exclude private and independent networks and on the other hand, they could make possible control over data and networks. Although the American approach succeeded, with the proposals for a national routing this very control over a more centralised network with predetermined handover points to other networks was back on the table. By changing routing practices, telecommunications providers could retrieve at least parts of their former position of power through central network control points that they used to have in the traditional telephone networks.

If one takes into account the internal structure of the telecommunications sector, one can also detect changing positions of actors within the sector itself. Deutsche Telekom stands out as an example in this regard, but this may be applied to other markets and national providers as well. As the primary provider in Germany and one of the largest in Europe the position of Deutsche Telekom as a ‘national champion’ would become even stronger through data territorialisation. This is due to the fact that Deutsche Telekom holds few peering agreements, but forces other Internet providers primarily to pay for transit agreements or to use existing agreements via other providers in the United States or elsewhere in order to connect to their network (see Gropp 2014; Greis 2014). With national or regional routing requirements, ‘more providers would be forced to hand over their data to the wires of Deutsche Telekom’ (König 2013: n.p., own transl.), which has not only economic effects but also concentrates control over data. It is not only that the position of large providers becomes more dominant (see Seiffert 2014; Welcher 2013), but it also expands their position in respect of other actors in the Internet industry, such as highly data-intensive content delivery networks, global transit providers, or IXPs. This may have an impact with regard to struggles over a restructuring of the network by abolishing network neutrality and introducing more steerable networks.

To sum up, the position and action capabilities of the large national providers would increase in comparison to market competitors, but also in relation to other industries, politics, and the public. This applies also to national storage

requirements such as those in Malaysia, Australia, or South Korea: the position of national providers strengthens as their products have to be considered in order to enable communications, even if they cannot compete in the market.

Government authorities

In the second part of this analysis, changes to power relations including those in government authorities are analysed. I start with infrastructural changes with regard to positions of and possibilities for control, and then turn to changing legitimacies.

Although it is relatively complex and costly for governments to control, filter or monitor data traffic in a traditionally decentralised and intermeshed network, it becomes much easier with centralised routing and nodes, a reduction of the meshing, and a hierarchisation of the network architecture. This shift simplifies governmental surveillance and control (see Roberts and Palfrey 2010: 40) as it concentrates data traffic to a few points and a few autonomous systems. It does not mean that authorities obtain the specific tools for surveillance and filtering right away, but with central connection points to foreign countries and limited routing capabilities, the complexity of engaging in surveillance is greatly reduced.

Furthermore, if national routing guidelines are to be actively enforced, the authorities tasked with checking and monitoring the implementation of these guidelines would have to set up something like customs barriers which would give them enormous insight into people's communications. The role of the state would drastically change from that of a gardening state to an interventionist one, and especially the executive branch would gain influence. In a similar vein, guidelines for national storage of certain data increase the positional power of governments by enhancing their possibilities to gain access to the stored data. Because of the limitation of storage to national providers only, data is more concentrated and easier to reach, all relevant data centres being under national jurisdiction. It is not only that data territorialisation generates possibilities and options for traffic control that might be used for filtering or censorship, but the changes to basic functionalities of the Internet affect how the network functions and which interventions are legitimate. In the following, these changes to normal routing practices and opportunities for censorship are discussed. Based on a traditional and decentral understanding, '[t]he Net interprets censorship as damage and routes around it' (Gilmore, quoted in Elmer-Dewitt 1993: n.p.). In case of failures or unavailability it used to be normal that the network, due to the dynamic and decentral architecture, would have provided a path around the error. In fact, this was the core function and aim of the network: availability by autonomous routing adjustments and therefore unrestricted mobility of data and information.

Centralised routing regulations alter this normality by imposing inflexible pre-defined allowed and disallowed routes. This leads to a normalisation of influence on routing, as well as the blocking of paths and content, thereby changing the foundational principles of cyberspace. 'The self-regulating process of the Internet community is based on connectivity which constitutes the "rough consensus" between all shareholders of a public good' (Hutter 2014: 535, own transl.). In other words, the rough consensus was that information mobility should apply to all parts of the network. This consensus is being challenged and the value of connection itself becomes negotiable. Taking up the conceptualisation of fixities (Sheller and Urry 2006), where through the fixities of infrastructure the mobility of information is made possible, one can observe that this mobility will be affected. Data that according to national routing should only be mobile within the national territory and travel on domestic hardware is not as mobile as it used to be. Data mobility is made possible by the material moorings and fixities of the underlying infrastructure, which is organised *nationally* rather than in a more unbounded fashion according to *efficiency and speed* of data exchange.

Through the increased importance of the storage location of data and the crossing of territorial borders of data, location in general, as well as national borders, become more important in a 'global' network. Territorial borders have not existed in cyberspace, but with national routing, political and territorial borders are being imposed on cyberspace or Internet infrastructure and technology. It becomes one of the core characteristics and central functions of the network to ask: is this data traffic domestic or international? Where is data stored? May traffic cross the border, and how are borders to be enforced and where? In its early years, cyberspace was considered to be a 'no-place', a place without governments and territorial borders (see Barlow 1996), but this 'placeless-ness' (Herrera 2007: 74) changes. With national routing, a national identity is attributed to data. Nationality as a concept itself becomes normalised in cyberspace although it was initially not inherent to the Internet's infrastructure.

Furthermore, if the functioning of the Internet infrastructure does not appear as self-organising, but as steerable or even with a normative responsibility to steer (in order to secure data from foreign actors), new possibilities for more and more far-reaching regulation are opened up. Government interference within the telecommunications sector becomes more common and can be legitimised more easily. Traditionally informed by competition law, infrastructure law, and media law, the general understanding of Internet regulation is more and more being characterised by its meaning for and within national security (see also Hall et al. 2013: 140).

Presenting data territorialisation as a means to protect data and citizens against foreign threats increasingly activates an *ingroup/outgroup* logic and fosters the perception of the state as the protector against evolving threats 'from

the outside'. From this perspective, it is only another step, especially in combination with the demands for governmental protection against child pornography or terrorist propaganda, towards a normalisation and legitimisation of governmental content filters. Or, as Deibert and Rohozinski put it:

States no longer fear pariah status by openly declaring their intent to regulate and control cyberspace. The convenient rubric of terrorism, child pornography, and cyber security has contributed to a growing expectation that states should enforce order in cyberspace, including policing unwanted content. (Deibert and Rohozinski 2010b: 4)

National routing is not to be compared to actual censorship, but the general legitimisation of governmental intervention and the technological changes that give more opportunities for control prepare the grounds for censorship. Furthermore, the rough consensus of global data mobility and availability is challenged and nationality of data and the protection of its security by steering the network becomes legitimate and normal.

An intelligent network and dumb clients

The previous two sections took into account changes in the technical infrastructure by analysing the role of ISPs and governments in regulating the Internet. This last part of the analysis is concerned with the more fundamental changes in technology and their governing principles.

Probably the most important technical change accompanying national routing is found in the transformation towards an intelligent network with intelligent centres. As shown above, the Internet was created based on the principle of intelligent clients and dumb and passive networks for different reasons, which is why the end-to-end principle became one of the core characteristics of the network. It has guaranteed openness, decentrality, and the absence of control, and puts the responsibility for and power of the network in the hands of the users. By introducing national routing, central nodes are needed in order to decide over and intervene in data traffic 'intelligently' and to not pass it on passively and without screening. The transition to an intelligent network, also promoted by measures such as 'quality classes' or filters, is perhaps the most important structural change of the network and its meaning. The relation between Internet users, media companies, telecommunications providers, and the state changes. The gardening state and passive Internet providers become partners that operate an intelligent network together. On the other hand, the actors of the Internet that were deemed to be the active and powerful ones, the clients, users, and content producers are turned into more passive consumers and content providers, as they are increasingly depending on central structures. This is not to be understood in a sense that today's computers and devices can

do less than before, but the core of the argument is that more functions are to be relocated to the network itself, so that the network structures become more important for the whole system than the clients in the network.

Taking this argument a bit further: according to the end-to-end principle, the clients of the network are its sovereign. However, by national routing initiatives this sovereignty is and would be more and more transferred to the nodes and data handling points due to the shift to an intelligent, steering, and governing network. Moreover, according to the traditional understanding of the network, data is stored decentrally and processed by the clients and devices; the network is changing to a more centralised construct where clients only display data. (National) data centres become more central as it becomes more important where data is stored and from where it is displayed. And the network itself gains more weight: it organises and governs communication by itself and is not just a passive infrastructure that is used by clients to communicate with each other. To put it on a yet more abstract level: in the traditional network organised by the end-to-end principle, individuals using the network were understood to be its sovereign, to be the core of enabling communication. However, in an intelligent network, the central control mechanisms are in charge of facilitating communication and individuals become merely users. The network changes from a passive to an active actor, and users must get used to playing a more passive part in the game.

There are three connected shifts in power relations to be noted when looking at data territorialisation: (1) a strengthened role and position of national telecommunications providers, thereby also strengthening their identity as security actors; (2) an increased (executive) power for governmental authorities, an expansion of their possibilities for action, which might also be used to censor content, and a general legitimisation of intervention in the network's functions and the imposition of territorial borders on a global network; and (3) a general transition from a passive and dumb network to an increasingly intelligent and steering one regulating and enforcing mobility restrictions, leading also to more passive and dependent users.

Conclusions

I have presented examples of and proposals for data territorialisation and argued that they can be understood as part of a trend of centralising cyberspace and its Internet infrastructure. I showed that these centralisation processes are connected to changing imaginaries of security that have a direct impact on the mobility and free flow of data. The free flow of data was once the main function of the network that was to be secured. National routing initiatives and national storage requirements are supposed to protect data, privacy, and citizens against a new type of threat: foreign intelligence. Furthermore, the original decentralised

set-up of the network was not only inspired by a different idea of security, but also by distinct ideas of power and control within the network. By analysing constitutive power changes that go hand in hand with data territorialisation, I have shed light on some of the very basic changes of the network and its connections to societal actors and social structures.

One of the main observations is the changing role and position of state authorities that not only gain more control over data, providers, and citizens, but also could use this control to monitor and censor content. Furthermore, the shift in meaning that puts states and their assisting providers in the role of protecting citizens from foreign and outside threats is also bringing to the table again the issue of border control. The providers' role changes to increased participation in the security apparatus, thus given them more control over their customers, more influence on the Internet industry, with national champions especially also benefiting economically. The users and citizens, on the other hand, are put in a more passive and dependent position with regard to both the authorities and the providers. Additionally, as decentralised information technologies are seen by some authors as empowering and/or liberating technologies allowing open discourse, including of otherwise marginalised positions (see Singh 2013: 6; Deibert and Rohozinski 2010c: 43), such a development poses problems for democracies as they need decentralised contexts and (political) participation.

The change of the role and functioning of the technical infrastructure is fundamental for many of these initiatives, and also for prospective developments. The increasing demand for an abolition of the end-to-end-principle and decentrality of the network that comes with data territorialisation is not only transforming the network to an 'intelligent' grid with 'dumb' clients, but it also has implications for (and of course is itself influenced by) a range of non-technical and social relations as shown above. The fixities of the Internet not only makes mobility possible, but with data territorialisation, the territorial borders of the infrastructure are also regulating and thus limiting the mobility of data. Further research should look into the role of technology in these developments, notably from a perspective inspired by ideas of material and technological agency, since technology and 'software, we might say, writes mobility' (Hannam et al. 2006: 5).

Cyberspace is not power-free and never will be. My analysis has demonstrated that centralising tendencies entail power shifts that are normatively relevant. Thus, it has become clear that demands for further centralisation such as data territorialisation need adequate critical reflection and public discussion to raise awareness of the structure and organisation of power relations in cyberspace. Information technology is no separate or even virtual space – it rather (re)produces social relations. How much power do we vest in decentral protocols and in intelligent and governing centres? How much influence should

companies and states be allowed to have and what functions and sovereignty do we want clients, and in the end ourselves, to have?

NOTES

- 1 Barnett and Duvall describe a four-by-four matrix of ideal types of power of which only parts are used in this analysis. In their understanding, however, the four types of power are on the one hand the more interactionist types of compulsory and institutional power and on the other hand the more constitutive kinds: structural and productive power (Barnett and Duvall 2005: 12). It is not that interactionist types of power are irrelevant, but they are rather related to the acts of policy implementation or enabled by specific forms of constitutive power.
- 2 Since this term is also (perhaps even more so) used to address the rights of individuals in contrast to companies or state authorities, for reasons of clarity I prefer the term data territorialisation.

REFERENCES

- Adhikari, R., 2013. 'Deutsche Telekom Pitches NSA-Free German Internet', TechNewsWorld. Available at www.technewsworld.com/story/79286.html (accessed 21 October 2014).
- Baldwin, D. A., 2013. 'Power and International Relations', in W. Carlsnaes, T. Risse, and B. A. Simmons, eds, *Handbook of International Relations*. 2nd edn, London: Sage.
- Barlow, J. P., 1996. 'A Declaration of the Independence of Cyberspace'. Available at <https://projects.eff.org/~barlow/Declaration-Final.html> (accessed 15 November 2014).
- Barnett, M. and R. Duvall, 2005. 'Power in Global Governance', in M. Barnett and R. Duvall, eds, *Power in Global Governance*, Cambridge: Cambridge University Press.
- Berke, J., 2013. 'Telekom will innerdeutschen Internetverkehr übers Ausland stoppen', *WirtschaftsWoche*, 12 October 2013. Available at www.wiwo.de/unternehmen/it/spionage-schutz-telekom-will-innerdeutschen-internetverkehr-uebers-ausland-stoppen/8919692.html (accessed 21 October 2014).
- BITKOM, 2013. 'Positionspapier zu Abhörmaßnahmen der Geheimdienste und Sicherheitsbehörden, Datenschutz und Datensicherheit'. Available at www.bitkom.org/Publikationen/2013/Positionen/Positionspapier-zu-Abhoermassnahmen/BITKOM-Positionspapier_Abhoermassnahmen.pdf (accessed 23 October 2014).
- Castells, M., 2001. *The Internet Galaxy: Reflections on the Internet, Business, and Society*, Oxford: Oxford University Press.
- Chander, A. and U. P. Lê, 2014. 'Breaking the Web: Data Localization vs. the Global Internet'. UC Davis Legal Studies Research Paper Series 378. Available at <http://ssrn.com/abstract=2407858> (accessed 2 October 2014).
- Clark, D. D., 2012. 'Control of the Internet – The Core of Cyberspace'. ECIR workshop on: Who Controls Cyberspace? Explorations in Cyber International Relations. Available at: http://ecir.mit.edu/images/stories/FinalWorkshop_2012.pdf (accessed 9 October 2014).

- Clauß, U., 2014. 'So würde Europas "Schengen-Internet" funktionieren', *Die Welt*, 31 March 2014. Available at www.welt.de/126343060 (accessed 9 October 2014).
- Cohen, J. E., 2007. 'Cyberspace as/and Space', *Columbia Law Review* 107(1): 210–56.
- Dahl, R. A., 1957. 'The Concept of Power', *Behavioral Science* 2(3): 201–15.
- De Filippi, P. and S. McCarthy, 2012. 'Cloud Computing: Centralization and Data Sovereignty', *European Journal of Law and Technology* 3(2): 1–18.
- Deibert, R., J. Palfrey, R. Rohozinski, and J. Zittrain, eds, 2008. *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge: MIT Press.
- Deibert, R. and R. Rohozinski, 2010a. 'Risking Security: Policies and Paradoxes of Cyberspace Security', *International Political Sociology* 4(1): 15–32.
- Deibert, R. and R. Rohozinski, 2010b. 'Beyond Denial: Introducing Next-Generation Information Access Controls', in R. Deibert, J. Palfrey, R. Rohozinski, and J. Zittrain, eds, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, Cambridge: MIT Press.
- Deibert, R. and R. Rohozinski, 2010c. 'Liberation vs. control: The future of cyberspace', *Journal of Democracy* 21(4): 43–57.
- Deibert, R. and R. Rohozinski, 2012. 'Contesting Cyberspace and the Coming Crisis of Authority', in J. Palfrey, R. Rohozinski, and J. Zittrain, eds, *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*, Cambridge: MIT Press.
- Diersch, V., 2014. 'Ein Bericht über den Cyber Security Summit 2013 der Münchner Sicherheitskonferenz und der Deutschen Telekom in Bonn', *Zeitschrift für Außen- und Sicherheitspolitik* 7(1): 67–73.
- Dittler, H. P., 2013. 'Balkanisierung des Internet kein geeignetes Konzept für mehr Datenschutz und Datensicherheit'. Internet Society German Chapter e.V. (ISOC.DE e.V.). Available at www.isoc.de/2013/10/balkanisierung-des-internet-kein-geeignetes-konzept-fur-mehr-datenschutz-und-datensicherheit (accessed 23 October 2014).
- Dunn Cavelt, M., 2013. 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse', *International Studies Review* 15(1): 105–22.
- Elmer-Dewitt, P. 1993. 'First Nation in Cyberspace: Twenty million strong and adding a million new users a month, the Internet is suddenly the place to be', *TIME International*, 6 December 1993.
- Fuhrmann, H., 2002. 'Technikgestaltung als Mittel zur rechtlichen Steuerung im Internet', *Zeitschrift für Rechtssoziologie* 23(1): 115–30.
- Glen, C. M., 2014. 'Internet Governance: Territorializing Cyberspace?', *Politics & Policy* 42(5): 635–57.
- Goldsmith, J. L. and T. Wu, 2006. *Who Controls the Internet? Illusions of a Borderless World*, Oxford: Oxford University Press.
- Greis, F., 2014. 'Experten fordern Verschlüsselung und Schengen-Routing'. Golem.de – IT-News für Profis. Available at www.golem.de/news/nsa-totruersten-experten-fordern-verschluesselung-und-schengen-routing-1406-107493.html (accessed 21 October 2014).
- Gropp, M., 2014. 'Woran das europäische Internet noch hängt', *Frankfurter Allgemeine Zeitung*, 19 February 2014. Available at www.faz.net/-gqm-7mjz9 (accessed 6 November 2014).

- Guzzini, S., 2007. 'The Concept of Power: a Constructivist Analysis', in F. Berenskoetter and M. J. Williams, eds, *Power in World Politics*, London: Routledge.
- Hall, C., R. Anderson, R. Clayton, E. Ouzounis, and P. Trimintzios, 2013. 'Resilience of the Internet Interconnection Ecosystem', in B. Schneier, ed., *Economics of Information Security and Privacy III*, New York: Springer.
- Hannam, K., M. Sheller, and J. Urry, 2006. 'Editorial: Mobilities, Immobilities and Moorings', *Mobilities* 1(1): 1–22.
- Herrera, G. L., 2007. 'Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space', in M. Dunn Cavelti, V. Maurer, and S. F. Krishna-Hensel, eds, *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*, Aldershot: Ashgate.
- Herrington, L. and R. Aldrich, 2013. 'The Future of Cyber-Resilience in an Age of Global Complexity', *Politics* 33(4): 299–310.
- Heuzenroth, T., 2014. 'Es nützt nichts, nur latent Angst zu haben', *Die Welt*, 3 November 2014. Available at www.welt.de/133932933 (accessed 6 November 2014).
- Hofmann, J. and M. Holitscher, 2004. 'Zur Beziehung von Macht und Technik im Internet', in U. Thiedeke, ed., *Soziologie des Cyberspace. Medien, Strukturen und Semantiken*, Wiesbaden: Springer VS.
- Hutter, M., 2014. 'Die globale Regulierung des Internet Domain Name Systems. Fünf Lehren aus dem Fall ICANN', in U. Thiedeke, ed., *Soziologie des Cyberspace. Medien, Strukturen und Semantiken*, Wiesbaden: Springer VS.
- Kerr, I. and J. Barrigar, 2012. 'Privacy, Identity and Anonymity', in K. Ball, K. D. Haggerty, and D. Lyon, eds, *Routledge Handbook of Surveillance Studies*, London: Routledge.
- Koalitionsvertrag, 2013. 'Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD'. 18. Legislaturperiode. Available at www.spd.de/linkable-blob/112790/data/20131127_koalitionsvertrag.pdf (accessed 23 October 2014).
- König, S., 2013. 'Warum ein nationales Netz keine Lösung ist', *Der Freitag*. Available at www.freitag.de/autoren/steve-koenig/warum-ein-nationales-netz-keine-loesung-ist (accessed 23 October 2014).
- Küchemann, E., 2014. 'Für ein offenes, freies, stabiles Internet', *Frankfurter Allgemeine Zeitung*, 12 June 2014. Available at <http://faz.net/-gsf-7qapm> (accessed 15 November 2014).
- Lessig, L., 2006. *Code Version 2.0*, Cambridge: Basic Books.
- Lukes, S., 2005. *Power: A Radical View*. 2nd edn. Basingstoke: Palgrave Macmillan.
- Mueller, M., A. Schmidt, and B. Kuerbis, 2013. 'Internet Security and Networked Governance in International Relations', *International Studies Review* 15(1): 86–104.
- Obar, J. A. and A. Clement, 2013. 'Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty'. TEM 2013: Proceedings of the Technology & Emerging Media Track – Annual Conference of the Canadian Communication Association. Available at www.tem.fl.ulaval.ca/www/wp-content/PDF/Victoria_2013/OBAR-CLEMENT-TEM2013.pdf (accessed 15 July 2016).
- Pohlmann, N., I. Siromaschenko, and M. Sparenberg, 2014. 'Direktvermittlung. Das 'Schengen-Routing' zu Ende gedacht', *iX – Magazin für professionelle Informationstechnik* 2014(2): 112–18.

- Polatin-Reuben, D. and J. Wright, 2014. 'An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet'. 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI'14). Available at [www.usenix.org-system7files/conference/foci14/foci14-polatin-reuben.pdf](http://www.usenix.org/system7files/conference/foci14/foci14-polatin-reuben.pdf) (accessed 28 October 2014).
- Roberts, H. and J. Palfrey, 2010. 'The EU Data Retention Directive in an Era of Internet Surveillance', in R. Deibert, J. Palfrey, R. Rohozinski, and J. Zittrain, eds, *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace*, Cambridge: MIT Press.
- Schluting, C., 2006. 'Networking 101: Understanding Routing'. Available at www.enterprisenetworkingplanet.com/netsp/article-php/3607381/Networking-101-Understanding-Routing.htm (accessed 25 October 2014).
- Seiffert, J., 2014. 'Weighing a Schengen zone for Europe's internet data'. DW – Deutsche Welle. Available at <http://dw.de/p/1BBqU> (accessed 28 October 2014).
- Sheller, M. and J. Urry, 2006. 'The New Mobilities Paradigm', *Environment and Planning A* 38(2): 207–26.
- Singh, J. P., 2013. 'Information Technologies, Meta-Power, and Transformations in Global Politics', *International Studies Review* 15(1): 5–29.
- Söderström, O., S. Randeria, D. Ruedin, G. D'Amato, and F. Panese, 2013. 'Of Mobilities and Moorings: Critical Perspectives', in O. Söderström, S. Randeria, D. Ruedin, G. D'Amato, and F. Panese, eds, *Critical Mobilities*, Milton Park/New York: Routledge.
- Swartz, D. L., 2007. 'Recasting Power in its Third Dimension', *Theory and Society* 36(1): 103–9.
- Thiedeke, U., 2004. 'Wir Kosmopoliten: Einführung in eine Soziologie des Cyberspace', in U. Thiedeke, ed., *Soziologie des Cyberspace. Medien, Strukturen und Semantiken*, Wiesbaden: Springer VS.
- USTR, 2014. 'USTR Targets Telecommunications Trade Barriers'. Available at <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2014/March/USTR-Targets-Telecommunications-Trade-Barriers> (accessed 15 November 2015).
- Waltz, K. N., 1979. *Theory of International Politics*, New York: Random House.
- Welchering, P., 2013. 'Daten im Land halten bringt nicht viel', *Frankfurter Allgemeine Zeitung*, 5 December 2013. Available at www.faz.net/-gyc-7jzx8 (accessed 25 October 2014).