universität wien

MASTERARBEIT / MASTER´S THESIS

Titel der Masterarbeit / Title of the Master´s Thesis

„A Geography of Globalising Surveillance“

verfasst von / submitted by

Patrick Carlos Petit

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master (MA)

Wien, 2016 / Vienna 2016

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A 067 805
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Individuelles Masterstudium: Global Studies – a European Perspective
Betreut von / Supervisor:	Dr. Jutta Weber, MA

UNIVERSITÄT LEIPZIG

universität wien

MASTERARBEIT / MASTER THESIS

Titel der Masterarbeit /Title of the master thesis

A Geography of Globalising Surveillance

Verfasser /Author

Patrick Carlos Petit

angestrebter akademischer Grad / acadamic degree aspired

Master (MA)

Wien, 2016

Studienkennzahl :	A 067 805
Studienrichtung:	Individuelles Masterstudium: Global Studies – a European Perspective
Betreuer/Supervisor:	Dr. Jutta Weber, MA

Abstract/Zusammenfassung

Diese Thesis untersucht technologische, geo-politische und räumliche Implikationen der Globalisierung von Überwachungsinfrastrukturen. Inspiriert von den *Snowden Leaks* aus dem Sommer 2013, nimmt diese Arbeit globale Überwachungsstrukturen der National Security Agency (NSA) in den Fokus. Untersucht werden NSA Überwachungstechnologien und –infrastrukturen im Kontext der verschiedenen Infrastrukturebenen des Internets, die hier als physische und protokollarische Levels und globale Datenflüsse konzipiert sind. Diese Analyse legt eine Globalisierung von Überwachungsinfrastrukturen nahe, die gleichsam aus dem Hervortreten neuer multidimensionaler, räumlicher Konfigurationen von Überwachung, der transnationalen Kollaboration von Geheimdiensten und den komplexen Liaisons von staatlichen und privaten Akteuren resultiert – und diese Entwicklungen weiter beschleunigt. In diesem Kontext werden Überwachungsinfrastrukturen zunehmend globalisiert und glokalisiert – eine Entwicklung, die die hegemoniale Position der NSA innerhalb globaler Überwachungsstrukturen weiter untermauert.

Die Globalisierung von Überwachungsinfrastrukturen wird hier weiterhin mithilfe von Netzwerktheorien, einem Blick auf die Möglichkeiten protokollarischer Kontrolle sowie der Präponderanz von Netzwerkeffekten innerhalb der Forschungsgegenstände untersucht.

Theoretische Werkzeuge, von denen diese Thesis Gebrauch macht, sind u.a. Assemblage-Theorien (Ong und Collier, Haggerty und Ericson), Manuel Castells‘ *spaces of flows*, die Kontrollgesellschaften in der Philosophie Gilles Deleuzes, sowie die Implikationen von Überwachungshegemonie.

Diese Thesis zeigt auf, dass etablierte Theoreme der Erforschung gegenwärtiger Überwachungsstrukturen keinesfalls überholt erscheinen und eine breite Analyse der Globalisierung von Überwachungsinfrastrukturen ermöglichen. Die Erkenntnisse dieser Thesis verlangen nach ihrer Validierung durch Analysen mit explizit nicht-westlichen Foki, die die gleichsame Globalisierung und Glokalisierung von Überwachungsstrukturen auf globaler Ebene untersuchen.

Keywords: Assamblage, Datenströme, Globalisierung, Glokalisierung, Netzwerkeffekte, NSA, Überwachung.

Abstract

This thesis scrutinises geo-political and technological features of globalising surveillance. Inspired by the intelligence leaks provided by U.S. whistleblower Edward Snowden in the summer of 2013, this thesis takes a NSA-centred approach in the analysis of the globalisation of digital surveillance infrastructures. This thesis provides a detailed study of the multiple ways the NSA penetrates the physical and protocological level of the Internet as well as spaces of global flows inherent to the Internet. Emerging from this analysis is a form of globalisation that simultaneously produces and results from specific and multidimensional spatial configurations of surveillance, collaborations between states and spying agencies and ambiguous liaisons between corporate and state-led surveillance, public and private actors. Surveillance is undergoing contested processes of both globalisation and glocalisation that play into the hands of the NSA which holds a hegemonic position within the world of surveillance.

The globalisation of digital surveillance infrastructures is further studied with a look at network theories, the potential of protocological control and the preponderance of network externalities that drive both surveillance networks and the technological as well as physical infrastructures of the Internet.

Analytical tools deployed in this thesis are (surveillant) assemblage theory (Ong and Collier, Haggerty and Ericson), Castells' spaces of global flows, glocalisation theory (Brenner), Deleuze's society of (rhizomatic) control and surveillance hegemony, protocological control in network theories (Baran, Galloway) and the study of network externalities.

Ultimately, this thesis suggests that established theorems within Surveillance Studies, such as the surveillant assemblage or theories of rhizomatic control, are not exhausted and prove useful tools for the analysis of the globalisation of surveillance. This thesis recognises that surveillance is not the same everywhere and just as surveillance is comprised of a multitude of heterogeneous processes, so is its globalisation. Therefore, the findings of this thesis call for their validation through explicitly non-Western analyses of the distinct ways surveillance is undergoing processes of globalisation and glocalisation on a global scale.

Keywords: assemblage, globalisation, glocalisation, network externalities, NSA, spaces of flows, surveillance.

Acknowledgements

First and foremost, I would like to express my deepest gratitude to my supervisor, Jutta Weber. Her sharp advice and insights into the matter were a constant push and help, and this thesis would not have been if it wasn't for her. She allowed me to write my thesis exactly the way I wanted to write it.
Furthermore, I would like to thank the entire body of the Erasmus Mundus Global Studies programme: Stehpan Kaschner and Konstanze Loeke of Universität Leipzig for all their patience, support and help and diligence. You guys are the unsung heroes of this programme. Thanks to Alecia Erasmus from University of Stellenbosch. Thanks to Markus, Poldi and Magi from Universität Wien who guided me through the final months of my studies.
A special thanks to Gilad Ben-Nun who has taught me more in a single conversation than I could have learned from a thousand books.
A number of people have accommodated and supported me during my nomadic months of writing: Many many thanks to the eternal Markus Metzger – where would I be without you? Thank you Tiantian Gao, you really helped me a lot. Thank you, Schoppi. And of course, thank you Nwabisa.
A special shout out to Richard Bachmann and Steffen Schimko whose insights and proofreading were of greatest help.
My deepest gratitude to my family who has been with me through the good and the less fortunate days of the past months and years. Their support and help got me where I am today.
Finally, thank you, Nwabisa, for bearing with me through the past months, from near and afar. Ndiyabulela ngokuba undithemba kwaye ndibulela umonde ondinika wona, nako konke okunye. Ngoku masi groove-e.

This thesis is dedicated to my late mother Karin Petit (1952-2007). Loved, cherished and thoroughly missed.

List of Abbreviations

9/11	Terror attacks carried out in the U.S. on September 11th 2001
AT&T	American Telephone and Telegraph Company
BfV	Bundesamt für Verfassungsschutz (GER), Germany's Federal Office for the Protection of the Constitution
BND	Bundesnachrichtendienst (GER), Germany's Federal Intelligence Service
CIA	Central Intelligence Agency (US)
DNS	Domain Name System
DPI	Deep Packet Inspection
FBI	Federal Bureau of Investigation (US)
FRA	Försvarets radioanstalt (SWE), Sweden's National Defence Radio Establishment
GCHQ	Government Communications Headquarters (UK)
HUMINT	Human Intelligence
IBP	Internet Backbone Providers
INTERPOL	International Criminal Police Organization
IP	Internet Protocol
ISP	Internet Service Providers
IT	Information technology
IXP	Internet Exchange Point
NSA	National Security Agency (US)
RFC	Request for Comments documents
SIGINT	Signals Intelligence
TCP	Transmission Control Protocol
UK	United Kingdom of Great Britain and Northern Ireland
UN	United Nations
U.S.	United States

List of Figures

Table of Contents

This, then, is the reasoning of the partisans of mystery:—"You are incapable of judging, because you are ignorant; and you shall remain ignorant, that you may be incapable of judging."

Jeremy Bentham (1843)

Chapter 1: Introduction

Topic and research question

Being deployed to Germany in the service of bulk and targeted surveillance apparently has its benefits both professionally and culturally. According to an unnamed NSA employee and apparent wine connoisseur who gleefully reports from his field work in Germany '[t]he middle Rhein area [...] is quite scenic and offers many opportunities to sample aspects of German life, especially gastronomic pleasures [...] You don't have to go far to find a really good white wine, for some very good Rieslings may well be just down the street' (NSA 2003). It is tempting to dismiss such an account as everyday banality in the hidden world of spying and surveillance. And yet, the peculiar circumstances that call such an account into existence merit scrutiny. Beyond doubt, if it was not for state secrecy, this seemingly banal account would probably never have been produced – nor would the respective NSA employee possibly be stationed in Germany. But state secrecy exists and so it was produced and the internal classified NSA document – like millions of others – only made its way to the public due to the acts of a whistleblower and the work of journalists around the world. In summer 2013 journalists began publishing leaked NSA and partnering agencies' documents obtained by whistleblower and soon-to-be-exiled activist Edward Snowden, at the time an analyst at the surveillance sub-contractor Booz Allen Hamilton. Sparking outrage and a greater awareness of everyday surveillance around the world (Penney 2016), observers remain sceptical whether they brought about any factual change in terms of surveillance policies or practices (Bigo 2016): While there have been efforts to strengthen privacy standards brought forward by actors of civil society, courts and watchdogs, there remains ample room for improvement of privacy regulation on behalf of governments across the globe (Brown 2015). Furthermore, with regard to the protection of foreign nationals, recent changes enacted in U.S. surveillance policies are described as *cosmetic* at best (Severson 2015) while the legality of global surveillance from a global human rights perspective remains doubtful (Georgieva 2015). Nonetheless, the *Snowden leaks* proved a disruptive discursive moment that provided ample insights into global surveillance, and global it appeared – be it in terms of reach, collaboration between different agencies or in terms of populations put under bulk surveillance.

The NSA employee's account of the pleasure of being stationed in Germany as quoted above seems banal only at first glance. Such accounts form one of a myriad of mosaic pieces that build the complex world of global surveillance. Emanating from the *Snowden leaks* are the most basic observations that surveillance is somehow conducted on all geographical scales,

against entire populations and appears, in many ways, omnipresent. Collaborating agencies and private enterprises seem to be simultaneously creating and exploiting *the global as a space* and arena of surveillance. And yet, in order to explain the presence of NSA employees in Germany, analyses are needed that go beyond the examination of certain agencies' practices, the detailed study of individual surveillance technologies and the effect these have on the individual subject – despite the unquestioned importance of such analyses. Instead, an analysis of surveillance across different spatial scales necessarily needs to take a step back and broaden its focus to a degree where general assumptions about the intersection of surveillance and the global are rendered possible. The past years have seen an emergent push within the discipline of Surveillance Studies to establish such a broad focus on surveillance and scrutinise its reconfiguration on a global scale. Outside the field of Surveillance Studies, *globalisation* is a theoretical instrument conveniently deployed, for instance, in the study of global economic integration, the emergence of global phenomena and the specific spatial and temporal configurations that emerge from globalisation processes – and the peculiar role of the nation-state and state territoriality in the context of such phenomena. However, *globalisation* remains a theoretical tool often neglected in the study of surveillance.

While their analytic value remains undoubted, recent studies of the changing environment of surveillance therefore often leave out a reference to the global as a spatial scale and processes of globalisation that profoundly reconfigure this scalar unit. For instance, Haggerty and Ericson's (2000) influential conception of the *surveillant assemblage* makes no mention of spatial scales; Bauman and Lyon's (2013) conversation on *liquid surveillance* equally leaves out spatial references to the global, as do network- and protocol-focused analyses of control within the Internet as pursued by Alexander Galloway (2004) and Laura DeNardis (2012); even benchmarks like Foucault's study of the *panopticon* and the role of surveillance in the disciplining of subjects (1995) allows for an addition of a spatial perspective.

Such a spatial perspective on (global) surveillance seems essential. Klauser asserts the importance of the study of the different spatialities produced by surveillance as space itself forms the 'locus, tool and object of surveillance' (2013, p. 291). Spatiality of surveillance appears to be inscribed with prevailing paradoxes central to contemporary surveillance and is therefore all the more worth a close scrutiny. As Klauser explains with regard to urban surveillance:

> surveillance (in its spatialities) has to be studied simultaneously with regard to fluidity and fixity, flows and presences, circulations and enclosures, external separation and internal organisation, because it is the articulation and reconciliation of precisely these contrapuntal

> pairs of logics that condition the functioning and implications of [urban] surveillance today (ibid.).

This notion will be taken up with the study of the globalisation of surveillance which, as any kind of globalisation, has to be understood as a multidimensional and at times paradoxical phenomenon that produced distinct emerging spatial reconfigurations of state power and global phenomena. Whilst Klauser seeks to study the spatialities of urban surveillance, this thesis seeks to scrutinise surveillance at a global stage with a focus on the globalisation of surveillance which serves to address the aforementioned neglect of scale and of globalisation processes within Surveillance Studies.

And yet, globalisation is not always excluded from analysis of the intertwinement of surveillance and the exercise of power. Hardt and Negri's influential *Empire* serves as an example where the 'source of imperial normativity is born of a new machine, a new economic-industrial-communicative machine [...], a *globalized* biopolitical machine' (Hardt & Negri 2000, p. 40, emphasis mine). Hardt and Negri here seem to be on the right track asserting how surveillance is part of processes of social sorting in the shape of a regime of homogenisation and heterogenisation and of inclusion and exclusion that operates on a global scale. What they refer to as *empire* – namely a new form of sovereignty under globalisation comprised of a complex interweaving of supra-national phenomena and organisms – necessarily relies heavily on the powers of societal domination which include surveillance and social sorting. Globalisation therefore is part of the trajectory to establish the emerging type of sovereignty on a *global* scale. Despite a somewhat polemic language, their analysis rightly asserts that

> Empire is emerging today as the center that supports the globalization of productive networks and casts its widely inclusive net to try to envelop all power relations within its world order—and yet at the same time it deploys a powerful police function against the new barbarians and the rebellious slaves who threaten its order (ibid. p. 20).

In contrast to other analyses, Hardt and Negri take the global and processes of globalisation into their focus. Globalisation and forms of societal domination such as surveillance seem inseparably involved in the establishment of new regimes of sovereignty and their implementation across heterogeneous populations on a global scale. But how exactly are surveillance and globalisation intertwined? Surveillance is not just a tool in the grand trajectory of globalisation and forceful global integration. Rather, it seems that the latter is transforming the former: Surveillance is increasingly undergoing processes of globalisation and more analyses are needed that take this process into focus. This thesis therefore endeavours to add a spatial macro-oriented focus to the diverse analyses of the changing

environment of surveillance by insisting on the preponderance of globalisation processes within the world of surveillance.

And yet, Murakami Wood (2013, p. 317) rightly stresses that the globalisation of surveillance is not an unarguable fact and a given. While surveillance appears increasingly ubiquitous, one should not infer that it is an evenly spread practice in a globalised world. Instead, surveillance on a global scale is a multidimensional phenomenon and the assertion of a globalisation of surveillance needs intense scrutiny in order to understand how the global and surveillance are interwoven. Inspired by Murakami Wood's approach to bring 'surveillance studies[sic], assemblage theory and political economic work on globalization and neoliberalization in and around geography into a closer conversation' (ibid.), this thesis endeavours to do exactly that: To scrutinise the way surveillance and the global intersect by looking at the way surveillance infrastructures may be undergoing globalisation processes.

While there are numerous ways this theme may be tackled, this thesis takes a decidedly U.S.-centred approach. There are several reasons for this explicit focus on the West: Firstly, the *Snowden leaks* present both the most comprehensive intelligence leak in history and they provide insights predominantly focussed on the infrastructures and practices of the NSA and partnering agencies. Unfortunately there are no comparable leaks to those of the summer of 2013 that provide insights into the workings of intelligence agencies not part of the global NSA surveillance network. Secondly, the NSA is understood to be the most powerful and best equipped agency when it comes to both bulk and targeted surveillance (Bauman et al. 2014). The reasons for and particularities of this preponderance will largely be laid out throughout this thesis. The U.S. arguably plays a central role in all dimensions of globalization, be it in military-, economic, social or environmental realms (Nye 2002), despite prevailing differences between these dimensions. More than any other dimension, militaristic globalisation is understood to be a foremost American trajectory. Consequently, the notion of the globalisation of surveillance necessitates a recognition of the partially hegemonic position the U.S. holds in global (surveillance) networks and across global phenomena and rightly infers that this equally holds true for the globalisation of surveillance.

With these thoughts in mind, this thesis poses the following questions:

> *In how far do NSA digital surveillance infrastructures evince an ongoing globalisation of surveillance?*
>
> *Emanating from these infrastructures, what are the distinct ways in which globalising surveillance is being spatialised?*

In order to adequately answer these research questions, the following clarifications concerning surveillance (a), globalisation (b) and infrastructure (c) seem necessary.

a) Throughout this thesis I will use the term *surveillance* with primarily *digital surveillance* in mind. Why? On the one hand for reasons of practicability and convenience and on the other hand because it appears that the infrastructures of digital surveillance can hardly be separated from other forms of surveillance. Surveillance is a multidimensional phenomenon whose different dimensions are closely interwoven on a technological, infrastructural and policy-oriented level. However, I will adhere to the conventional differentiation between human intelligence (HUMINT) and signals intelligence (SIGINT) and provide the broad yet straightforward definition (inspired by DeNardis 2015, p. 73) that *surveillance* as used here refers to the *observation or monitoring of digital communications or activities of individuals, groups of societies, if not entire populations, based on SIGINT derived from these activities or communications.* This definition comprises the surveillance of content and information surrounding content, such as metadata, and supports the broad claim that '[s]urveillance can occur at almost any point in a communication network' (ibid.).

Two aspects merit particular mention in this context: Firstly, this thesis understands that contemporary forms of surveillance are not only conducted by states but are carried out by a multiplicity of human and non-human actors that comprise individuals, particular technologies that can create their own forms and dynamics of surveillance, and the outsourcing of surveillance to corporate entities and private actors. *Outsourcing* here implies that private actors or corporations may not necessarily be government sub-contractors but are either legally obliged to cooperate in forms of surveillance or may be collaborating unwittingly in such forms of surveillance (Verde Garrido 2015, p. 157).

Secondly, a crucial dimension of contemporary forms of surveillance comprises what has been termed *contemporary biopolitics of information and communications* (ibid. p. 160). The slim format of this thesis regrettably does not allow for a broader scrutiny of biopolitical aspects of surveillance and biopolitics will therefore largely be excluded from this thesis. Nonetheless, *surveillance* as understood here entails an intertwinement of the Foucauldian concepts of governementality and biopolitics with contemporary forms of surveillance. Biopolitics for Foucault represents a 'technology of security [...] or regulatory technology' that is concerned 'with the population as a political problem' (Foucault, quoted ibid.). In this sense, biopower is concerned with the production and reproduction of life itself (Hardt & Negri 2000, p. 24). The biopolitics of information and communications in this context 'represent a novel intrusion [...] into biosociological processes of acquisition and production

of information and its circulation and distribution by the power of states and corporations' (Verde Garrido 2015, p. 160) which allows states, corporate entities and other powerful actors of global capitalism to deploy a security apparatus of both disciplinary and biopolitical technologies of power in the domination of populations. As such, the notion of biopolitical surveillance stresses the fact that both new forms of surveillance and the rescaling of surveillance will produce new forms of 'inclusion and exclusion enacted through new technologies of population control' (Bauman et al. 2014, p. 136).

b) There is no universally accepted definition of *globalisation* as the notion of globalisation itself proves one of the most contested concepts social sciences, geography and economics have produced over the past decades. Therefore, in order to avoid both yet another contestable definition of globalisation and the unnecessary muddying of theoretical waters, this thesis invokes an inherently intuitive understanding of globalisation that will only be amended where necessary throughout this thesis. The concept of *synthetic generalisation* relies on the observation that 'diverse attributes of a topic revolve around a central theme which unifies the attributes, lending coherence to an otherwise disparate set of phenomena' (John Gerring, quoted in Keiber 2014, p. 25). Central themes of globalisation invoked here are a generally increasing compression of time and space due to the advent of modern communication technologies and modern forms transportation; the global diffusion of neoliberal policies and ideologies; a recalibration of power in the context of contested processes of waning and reinforcement of national sovereignty and state-territoriality; the advent of global phenomena whose key characteristic is a fluidity that is inherently not place-based; and – most generally – contested processes of global integration on political, economic, social and militaristic levels across the globe. In addition to these general traits of globalisation, a spatial focus of analysis understands globalisation as a 'highly contradictory reconfiguration of densely interwoven, superimposed spatial scales, including those on which the territorial state is organized' in the context of which 'state territorial power is not being eroded, but rearticulated and reterritorialized in relation to both sub- and supra-state scales' (Brenner 1998, p. 3).

c) Lastly, I borrow my understanding of *infrastructure* from Susan Leigh Star and Geoffrey Bowker's essay *How to Infrastructure* (2006) where, to begin with, infrastructure is thought of as 'that upon which something else rides, or works, a platform of sorts' (ibid. p. 230). Consequently, we can grasp infrastructure as something that runs or is built underneath a scrutinised object or practice, something the object of study is dependent on. As such, infrastructure is of relational quality, understood to be contingent on working conditions within which it is made use of. It is of vital importance to understand this relational and

contingent aspect of infrastructure. For instance, the Internet, a central infrastructure for the focus of this thesis, is many things at once and here it is both a global communication network and at the same time the essential media exploited by digital surveillance. It is both infrastructure of communication and surveillance, and in both cases its essential quality is related to the conditions of its usage. In both cases its composition and use is highly contingent. The Internet could have emerged in a different way and could be used in different ways from the ways it is now. Also, it did not per se have to become a powerful infrastructure of surveillance.

And yet, *relationality* and *contingency* do not suffice to describe all relevant characteristics of *infrastructure*. Hence, further inherent characteristics of infrastructure identified by Star and Bowker are firstly its embeddedness into other structures, social arrangements as well as technologies, and secondly a certain transparency in the sense that infrastructure invisibly supports that which makes use of it and does not have to be reinvented for every use. Thirdly, infrastructure reaches beyond a single site or practice and routinely is linked to the conventions of certain practices. Fourthly, infrastructure embodies standards and is built on an installed base in the sense that infrastructure 'does not grow *de novo*; it wrestles with the inertia of the installed base and inherits strengths and limitations from that base' (ibid. p. 231, emphasis in original). And, finally, infrastructure becomes visible upon breakdown.

These characteristics can best be explained with a look at the infrastructures scrutinised in this thesis, namely surveillance infrastructures. Simply put, the infrastructures of surveillance are those through which surveillance is carried out, that form the *underneath* of surveillance. Digital surveillance is embedded in a multitude of other structures, such as institutional arrangements, modes of capitalism, the digital economy and the emergence of big data, consumer and mass communication culture and of course specific technologies – technologies put under surveillance (such as certain digital communication technologies assembled in communication networks) and technologies deployed in the name of surveillance. Secondly, the infrastructures used for surveillance are largely transparent, invisibly supporting the exercise of surveillance. In the case of surveillance, state secrecy must be understood as an integral part of surveillance infrastructures which pushes the invisibility of surveillance infrastructures to an extreme. Yet, those with access to surveillance infrastructures do not have to reinvent these infrastructures. This connects to the next observation that surveillance infrastructures cannot be pinned down to a single unit through which surveillance is carried out as they are embedded in a community of practices and established ways of use. In addition to that, surveillance has not sprung out of the earth with the advent of information

technologies, but prevalent surveillance infrastructures have largely been built upon pre-existing infrastructures and practices. All the while surveillance infrastructures embody surveillance standards (of procedure, in terms of policies and technologies) – and may become visible once the infrastructures break down. Here, I say *may*, for in the world of surveillance invisibility of infrastructures must be understood as both the modus operandi and the very core of the entire infrastructural arrangement, actively pursued by the actors making use of the infrastructure. The hypothesis nonetheless holds true if one understands *leaks* like that by Edward Snowden as moments where the infrastructure of state secrecy breaks down, making visible to a certain degree the infrastructures of surveillance.

Infrastructure generally tends to exhibit heterogeneity and flexibility as a direct consequence from its contingency. It is for this reason that Star and Bowker (ibid. p. 234) stress the importance of standardisation and classification in the development of infrastructure: Standards are like the shared language of different units or practices, necessary on all layers of infrastructure. As such, standards often are a key site where socio-political conflicts are mediated (Galloway 2014, DeNardis 2009, 2014). The issue of standards, like so many of the phenomena scrutinised here, seems complicated by the prevalence of state secrecy. On the one hand, Internet standards such as protocols are predominantly openly accessible – prevailing standards within the world of surveillance on the other hand remain almost universally unknown.

Such circumstances point to the reason why I stick to Star and Bowker's understanding of infrastructure. As they explain,

> analysing infrastructure means problematizing this relationship between background and foreground. A given infrastructure may have become transparent, but a number of significant political, ethical and social choices have without doubt been folded into its development - and this background needs to be understood if we are to produce thoughtful analyses of the nature of infrastructural work (Star and Bowker 2006, p. 233).

This thesis endeavours to do exactly that: To problematise the relationship between the background (surveillance) and the foreground (digital communication) and show how surveillance infrastructures evince an ongoing globalisation of surveillance which in turn developed out of significant political, ethical and social choices.

The title of this thesis, *A Geography of Globalising Surveillance*, ultimately takes into consideration what Gregory (2011) conceptualised as particular geographies produced by what is termed *everywhere war*. The intertwinement of global terrorism and a shift in modern warfare towards targeting human individuals and groups of individuals as opposed to other

states marks a form of violence that can break out basically everywhere, hence the term *everywhere war*. Most crucially, 'within this warscape military and paramilitary violence could descend at any moment without warning' while 'within it precarious local orders [...] constantly forming and re-forming' (ibid. p. 239). The instalment of the everywhere war is as much a geographical, geopolitical, biopolitical and geo-economical trajectory as it is a matter of active political and spatial imagination (ibid.). As such, the everywhere war seems increasingly globalised and localised in geographical terms.

The same seems to hold true for surveillance. Surveillance cannot be equated with modern warfare – though intractably interwoven with it – as surveillance comprises its own bio- and socio-political trajectories and serves many more purposes than just modern warfare. Nonetheless, a tentative thesis of this thesis which will be elaborated below is the assertion of what could be framed as *everywhere surveillance*: The convergence of many a technology and actor engaged in surveillance on a global scale entails that surveillance can basically occur everywhere. However, as with everywhere war, the notion of *everywhere surveillance* acknowledges the heterogeneous character of the scrutinised phenomenon in all its ruptures, discontinuities and breaking points: Surveillance can potentially occur anywhere which does not entail that it necessarily does so. And while Gregory analyses how 'deadly liaison between modern war and modern geography has been conducted in resolutely territorial terms' (ibid. p. 239), the same can be asserted of global surveillance: Modern geography and infrastructural arrangements bring territorial units to the fore despite the perceived non-territoriality or placelessness often ascribed to surveillance. As will be seen, surveillance, while conducted on a global scale, unfolds upon local infrastructures and sub-sate spatial units. As such, the notion of a geography of *everywhere surveillance* presents the theoretical nexus where the here deployed analytical tools of globalisation and glocalisation converge.

Disposition

This thesis is structured as follows: The first two main chapters will present the theoretical framework this thesis is footed on. Understanding the globalisation of surveillance in its key technological and geo-political aspects requires an interdisciplinary approach taking into consideration numerous concepts of globalisation, surveillance, and networks. Consequently, the theoretical framework will firstly present relevant concepts of the multitude of processes subsumed under *globalisation*, namely global assemblages and processes of de- and reterritorialisation. Here I will visit perspectives presented by Collier and Ong and Gilles Deleuze. Afterwards, glocalisation of state-power according to Saskia Sassen's analysis of world cities and Neil Brenner's view on urban glocalisation in Western Europe will serve as a

foil through which new spatial configurations emerging from globalisation can be scrutinised. Lastly, the study of spaces of global flows in networked societies, as presented by Manuel Castells, will form an essential background to our understanding of global surveillance.

I then turn to different aspects of the study of surveillance – namely the intertwinement of security and surveillance, the surveillant assemblage as proposed by Haggerty and Ericson in the context of Deleuze's societies of (rhizomatic) control and ultimately a focus on the concept of surveillance hegemony which brings the nation-state back into focus as a unit of analysis.

The second theoretical chapter directs our attention to networks. Networks play a significant role through this thesis, for a number of reasons: The different communication network types laid out in the beginning of this chapter not only lay the foundation for our understanding of the organising logic of the Internet, but also serve as a foil through which the distinct ways power and surveillance are networked can be analysed. Afterwards, a look at protocols and protocological control will explain the working logic of the Internet, the key communication infrastructure in this thesis. The chapter will conclude with a turn from digital and communication networks to the economics of networks more generally – independent of the scrutinised kind of network – and how economics can influence the infrastructures of communication and surveillance.

In *Chapter 4: Mapping NSA digital surveillance* I delve into a qualitative analysis of the *Snowden leaks* that is guided by the research questions posed by this thesis. I firstly conceptualise NSA digital surveillance as the penetration of different layers of the Internet (the physical and protocological layer and the layer of global flows of data) and look at how exactly the penetration of different layers is achieved in infrastructural terms. The other main focus of this chapter will be on the institutional arrangements behind global digital surveillance that evince an ongoing internationalisation of surveillance efforts. This qualitative analysis is primarily based on journalistic publications of the *Snowden leaks* and a number of leaked NSA documents – all taken from the *Snowden Surveillance Archive* (https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi) where the leaked documents and their journalistic coverage are catalogued. This analysis is further corroborated with the help of recent academic research based on the insights granted by these leaks. Due to the slim format of this thesis and the vast amount of documents leaked, I cannot discuss all the leaked documents, or the coverage they have produced. My analysis of the insights into NSA infrastructures is therefore continually guided by my research questions.

The penultimate main chapter of this thesis will evaluate the findings emanating from the qualitative analysis of the *Snowden leaks* with the help of the concepts laid out in the preceding theoretical chapters. It will be demonstrated in how far these theoretical concepts are helpful in the analysis of the globalisation of surveillance – and where they fall short. In reaction to the latter, two further subchapters will be added: The first will concentrate on the transfer of policies and technologies under the neoliberalisation of governance and the crucial role individual agency plays in this context in the shape of a narrow elite of *travelling technocrats*. The other subchapter, dubbed *Shadow Globalisation*, will meditate over the far-reaching implications of *state secrecy* for surveillance infrastructures and the nature of the scrutinised kind of globalisation, the possibility of knowledge and the hindrance secrecy poses to academic analysis.

In this spirit, the concluding chapter will summarise the key findings of this thesis and reflect upon their implications for future research on this subject. The final thought will be dedicated to the importance of whistleblowers whose actions first and foremost seem indispensible to analyses like this thesis.

Limitations to the findings of this thesis

There are a number of limitations to the findings emanating from this thesis. To begin with, this thesis concentrates mainly on U.S. surveillance infrastructures, casting aside their foreign counterparts. While the American surveillance apparatus doubtlessly presents the most powerful and elaborate of its kind, a scrutiny of other apparatuses surely would have produced a more differentiated geography of globalised surveillance. However, due to the lack of information on and insight into these apparatuses, such a broad focus eludes the scope and feasibility of this thesis. Secondly, the reliance on journalistic sources entails further margins of error. While the journalists reporting on the *Snowden leaks* and other leaked insights into the American security apparatuses certainly possess some kind of expertise, it cannot be ruled out that their journalistic perspective on the leaked material entails errors and lack of vista. Thirdly and closely connected to this, the leaked files consulted here describe most elaborate surveillance infrastructures by making use of highly technological *insider* language. Many of the unknown terms and phrases encountered during my research could not be clarified despite extensive research. Fourthly, both the files used in this essay and the broader topic are veiled by state secrecy which has to be considered as a key hindrance impeding academic scrutiny in this field. Lastly, on the one hand, leaked *Snowden files* made their way into the public only in June 2013. Three years seems a rather short amount of time in academia and it can be concurred that a lot of crucial unpublished research on the content

and the implications of these files is still underway. On the other hand, in the volatile world of information technology and surveillance three years seems inconceivably long. Firstly, it is assumed here that surveillance programmes analysed here have been further enhanced over the past years, and secondly some of the leaked files date back over ten years – a circumstance which seems to make some of the findings of this thesis outdated.

And yet, the understanding of this thesis concurs with the position that epistemology occurs through the look in the rear guard (Canguilhem 2006; Sprenger 2015, p. 31). The fact that the academic race against time seems inherently lost does not derogate the epistemological value of scientific insight, for else any analysis of the presence would be rendered obsolete. Instead, a genealogy of the present serves to confront the present with its own contingence (Foucault, paraphrased by Sprenger 2015, p. 31), thus confronting it with the possibility that things could have been different from what they are. As such, an analysis of the globalisation of surveillance infrastructures is as much a scrutiny of these infrastructures' geography, composition and evolution, as it is a testimony of the historical moment we live in. Ultimately, a close look at recent developments within the scrutinized matter serve as a foreshadowing of what is likely to only intensify in the near future, for there is no indication to be found that any of these developments will be put to a halt in the near future.

Chapter 2: Globalisation and Surveillance

This chapter will first concentrate on processes of globalisation of interest for the purpose of this thesis and then turn to the key concepts in the study of surveillance.

Processes of globalisation

Any study of globalisation is confronted with both the subsumption of manifold different phenomena under one term and salient scholarly disaccord over the actual existence, the different dimensions, consequences and ramifications of globalisation (Collier & Ong 2005, p. 3 ff.). This thesis decidedly *avoids* presenting a general definition and conceptualisation of globalisation. Instead, I presuppose an intuitive understanding of globalisation and will revisit a number of handpicked analytical instruments convincingly invoked in the study of it. These instruments will be deployed in the analysis of the globalisation of surveillance in the hope that descriptive inference – 'using observations from the world to learn about other unobserved facts' (King et al. 1994, p. 8) – will allow us to see previously unexplored aspects of the globalisation of surveillance. Ultimately, this thesis will provide its own contribution to the broad and heterogeneous canon in the study of globalisation processes.

Global assemblages and the dialectics of de- and reterritorialisation

The first theoretical tool deployed here is the *(global) assemblage*. To begin with, Collier and Ong observe that global phenomena have the capacity to de-contextualise and re-contextualise while related but not bound to specific social and cultural processes. *Global* in this context entails the ability of phenomena

> to assimilate themselves to new environments, to code heterogeneous contexts and objects in terms that are amenable to control and valuation (Collier & Ong 2005, p. 11).

In the scope of time and space, such phenomena seem to possess neither beginning nor end, nor a specific locality which such forms can be exclusively pinned down to. And yet, the quoted excerpt continues as follows:

> At the same time, the conditions of possibility of this movement are complex. Global forms are limited or delimited by specific technical infrastructures, administrative apparatuses, or value regimes, not by the vagaries of a social or cultural field (ibid.).

Furthermore, the globality of such phenomena derives from their capacity of adaption and assimilation, their rejection of rigid and immutable *external* organising logics – and from their capacity to incorporate encountered objects, hindrances and environments. But how can one grasp the rejection of specific spatial fixity and simultaneous capabilities of incorporation where to-be-incorporated matter seems material or graspable in some ways? In other words, the final sentence of the excerpt quoted above seems to suggest some kind of temporal and spatial fixity of global forms and the processes through which these forms are mediated. It appears that global forms can only be grasped through the assumption of multiple logics rather than material denominations. They exist on the one hand in terms of an ideational space, on the other hand in terms of the *actual* global which 'indicate[s] the real world conditions that result from the application of global forms' (Murakami Wood 2013, p. 320).

This notion seems well included in the term *assemblage* which in the words of Deleuze and Guattari, 'is precisely this increase in the dimensions of a multiplicity that necessarily changes in nature as it expands its connections' Deleuze & Guattari 2005, p. 8). As such, the assemblage seems inherently temporal and contingent and yet capable of incorporation, assimilation and adaption.

This juxtaposition highlights tensions inherent to the concept of the *global assemblage*: On the one hand, *global* implies placelessness, a fluidity of matter that functions on mobility, movement and circulation. On the other hand, *assemblage* 'implies heterogeneous, contingent, unstable, partial, and situated' (Collier & Ong, 2005, p. 12). This thesis understands that the way these two aspects can be reconciled is if assemblages are considered

as ways of reterritorialisation of global forms (ibid. p. 4). De- and reterritorialisation are dialectic processes producing new dimensions of spatial and temporal fixity, and new organising logics. Deleuze and Guattari (2005, p. 10) explain how these two processes are interlinked:

> Each of these becomings[of de- or reterritorialised forms] brings about the deterritorialization of one term and the reterritorialization of the other; the two becomings interlink and form relays in a circulation of intensities pushing the deterritorialization ever further.

It appears that the dialectics of de- and reterritorialisation can best be explained by providing an example close to the topic of this thesis: Middell argues that the interplay of these processes can be read from the ongoing reconfiguration of state territoriality in the context of globalisation. Territoriality is widely understood as a key basis of modern state-building, seeking to make congruent diverse political, social, economic and identity realms within a fixed spatial unit (Middell, undated). This organising principle seems partly eroded by the emergence of border-transcending phenomena such as an increased mobility of people and goods, global flows of information and capital, and internationalised division of labour under the umbrella of increased global economic integration. This increase in mobility doubtlessly led to a deterritorialisation of the exercise of political power which in turn was met with a reterritorialisation of control of goods – and surveillance seems to be part of this trajectory. Therefore, it seems that the dialectics of de- and reterritorialisation are simultaneously at work as 'various actors compete for forms of control over global flows, and [that] there are specific arenas and moments when the battle for a new regime of spatial configurations becomes more intense and globally synchronised' (ibid. p. 4). Reterritorialisation occurs when spatial configurations are somehow eroded or undergo significant changes.

Collier and Ong suggest that the aforementioned inherent tension within the concept of *global assemblage* is solved if assemblage is understood as a form of reterritorialisation of global forms. While of most elusive and ephemeral kind, the term assemblage nonetheless captures the spatial and temporal configurations global forms entail. Again, assemblages have to be understood as multiplicities of logics, denominations and, ultimately, *enunciations*, as Deleuze and Guattari describe. They further explain (2005, p. 22 f.):

> An assemblage, in its multiplicity, necessarily acts on semiotic flows, material flows, and social flows simultaneously [...]. There is no longer a tripartite division between a field of reality (the world) and a field of representation (the book) and a field of subjectivity (the author). Rather, an assemblage establishes connections between certain multiplicities drawn from each of these orders, so that a book has no sequel nor the world as its object nor one or several authors as its subject.

The importance of this concept to the focus of this thesis will be elaborated upon further in the conceptualisation of the (global) surveillance assemblage. Yet, one last aspect seems noteworthy with regard to the establishment of connections between the multiplicities of an assemblage: Incorporation, variation, establishment of connections, are all processes that entail an increase in variety, width, depth and reach. Through these processes the assemblage grows yet bigger, more ramified. This presents an aspect arguably underexplored in relation to the dialectics of de- and reterritorialisation: How these processes can lead to the exploration of previously uninhabited connections. In essence this notion will build a reoccurring theme throughout this essay, and it is captured most aptly by Deleuze and Guattari declaring (ibid. p. 11):

> Write, form a rhizome, increase your territory by deterritorialization, extend the line of flight to the point where it becomes an abstract machine covering the entire plane of consistency.

The networked society

In *The Rise of the Network Society*, Manuel Castells introduces a number of observations of critical importance to this thesis. Castells sets out to analyse globalisation in what he perceives as a new form of economy that bears the following distinctive traits: Equipped with a new technological paradigm, it is *informational, global and networked.* Firstly, it is informational as productivity and competitiveness of entities or agents of this economy largely depend on their capacity to 'generate, process, and apply efficiently knowledge-based information' (Castells 2010, p. 77). Secondly, it is global in the sense that the components of production, such as materials, labour in times of division of labour, capital and management, technology and information, as well as patterns of consumption and circulation are organised on global scales. Thirdly, it is networked in the sense that competition and production in this globalised economy is largely mediated through global business networks. Networks in general comprise the interconnection of nodes and form open, expendable structures that in turn are interconnected through switches and prove a powerful instrument in the exercise of power. The new political economy is organised around and through global networks of capital, management, information and global commodity chains. As such, networks 'constitute the new social morphology of our societies, and the diffusion of networking logic substantially modifies the operation and outcomes in processes of production, experience, power, and culture' (ibid. p. 500 ff., quotation p. 500). Castells predicted that the growth of networks and consequently their importance would occur based on an expansive logic that supersedes expansionist forces of industrial capitalism. As such, future competition for power and the exercise thereof will evolve largely around the access to networks.

This new form of economy took its present shape in the last quarter of the twentieth century and is marked by a new technological paradigm, namely technological revolutions evolving around information and its respective technologies of information-processing. While information and knowledge have always constituted central domains of political power, what presents a historic discontinuity in the case of the informational, global and networked economy is that its key technologies 'act upon all domains of human activity [...] establishing endless connections between different domains, as well as between elements and agents of such activities' (ibid. p. 77-78, quotation p. 78). Castells' depiction of the consequences of the advent of the informational networked society largely concurs with other general analyses of globalisation, stressing the emergence of a *globally interconnected* economy, globally played out competition and highly diversified patterns of production. This global economy is equally intertwined with processes of *regionalisation*, as some means of production and employment are inherently static and bound to local structures enhanced by the regionalisation strategies of local or national governments. Thus, what has emerged is a partially regionalised global economy whose organising logic is not opposed to the industrial capitalist logic it has superseded, but subsumed under the shift to information-processing and a 'gigantic leap forward in the reach and scope of the circulation sphere' (ibid. pp. 99-111, quotation p. 100).
Beyond doubt, information and its processing technologies build the arteries of global communication infrastructures and production patterns. While Castells' analysis was written well before the advent of *social-networking* as a basic form of human interaction, his analysis of the importance of networking logic holds true both for this type of interaction as for the structuring of communication networks in general. Therefore, the conception of networks as the new social morphology forms a foil through which this thesis undertakes its analysis. Ultimately, information processing equally lies at the heart of contemporary surveillance technologies.

Spaces of flows

Castells argues that space and time are being transformed under the effects of the new technological paradigm and of new social formations emerging in the context of the new economy (Castells 2010, p. 407 f.). Global economic integration and complementary regionalisation processes are starkly crystallised in global cities that function as command centres where global networks ensure and largely drive innovation, coordination and management of the global economy. On the one hand, the complexity of a globally integrated economy clearly resists oversimplifications that pinpoint to a very limited number of global cities as such command centres, given the heterogeneous segmentation of the global economy

and the importance of regional centres in emerging markets. Therefore Castells understands the global city as a process of connecting nodes of the global network 'with different intensity and at a different scale depending upon the relative importance of the activities located in each area *vis-a-vis* the global network' (ibid. p. 411, emphasis in original). On the other hand, all nodes of this global network in general and global cities in particular are endowed with a key function of the new economy: The switching, control and management of global flows – be they of information, capital, knowledge, symbols, technology, interaction, management, or of other sorts. These flows bring together and integrate regions and simultaneously exclude others from the global economic order. Therefore, they simultaneously elude and govern territorial contiguity.

In essence, the networked society comprises a new organising logic which Castells calls *space of flows*. Understanding this organising logic necessitates analytic clarity with regard to what *space* itself constitutes. Space, Castells argues, is made of socially embedded material practices and material products and constitutes a material product itself (ibid. p. 441). Space is made by people, inhibited by people and consequently derives its meanings and relevance from people. In relationship to time, space can be understood as the 'material support for time-sharing social practices' (ibid. emphasis removed). I would suggest that Castells' wording here is slightly misleading. Firstly, *material* must also comprise *non-material* products of the informational economy. While it is true that even virtual spaces have some kind of material reality – e.g. in the shape of Internet infrastructure, cables, routers, databases, and so forth – the exercise of spatial practices does not necessarily have to coincide with the governance of this material reality. To give one of many examples, the participation in political activity on social media can be understood as the participation and framing of practices and products within a confined space and yet the graspable material reality of this space eludes the participants in the spatial practice.

Secondly, it is doubtful whether space is exclusively *made by people*. I would suggest that technologies such as protocols or databases can entail their own kinds of dynamics which can elude the notion of exclusively human agency (see Weber 2015) and these technologies can equally constitute space in terms of infrastructural arrangements. Castells here seems to neglect a perspective on non-human actors that could serve to enhance the complexity of the multitude of actors in the *networked society*.

As mentioned previously, the informational economy is structured around all kinds of flows. These flows, Castells argues, are what dominate political, economic and symbolic life and are the new medium through which social practices are articulated. Combining this observation

with the aforementioned understanding of space leads Castells to the following definition (ibid. p. 442, emphasis in original):

> *The space of flows is the material organization of time-sharing social practices that work through flows*. By flows I understand purposeful, repetitive, programmable sequences of exchange and interaction between physically disjointed positions held by social actors in the economic, political, and symbolic structures of society.

Space of flows consequently constitutes the material form of support for social practices and economic functions in the informational society. As such, spaces of flows are made up by a number of different layers. Firstly, circuits of electronic exchanges. This is the technological infrastructure of flows and consists of mainly electronic devices enabling communication and transport technologies based on information-processing. As the networked society finds its spatial articulation in the exchange of global flows, communication inherently is essential as exchanges occur through communication. The second layer consists of the hubs and nodes through which the flows are circuited. Beyond doubt, the *first* layer is not placeless, and the hubs and nodes is where its infrastructure mainly crystallises. Hubs and nodes form the aforementioned control centres where flows are switched and exchanged (ibid. pp. 442-444). While global cities doubtlessly present key hubs and nodes, Castells here introduces an aspect that will be of seminal importance to the study of globalising surveillance infrastructures: It is not only global or regionally important cities that function as hubs and nodes. This stems from the fact that the

> functions to be fulfilled by each network define the characteristics of places that become their privileged nodes. In some cases, the most unlikely sites become central nodes because of historical specificity that ends up centering a given network around a particular locality (ibid. p. 444).

Most crucially, *it is the concerned network itself that defines the functions of its hubs and nodes and therefore erects its internal hierarchies*. The study of globalising surveillance will show that surveillance networks comprise their own geography of hubs and nodes that at times – for instance in the case of remotely located interception sites – does not necessarily coincide with the global geography of the informational economy.

The third layer is formed by managerial elites endowed with directional functions within the spaces of flows. As with the second layer, the strength of Castells' conception lies in the fact that it can be applied to spatial realities that at first glance do not necessarily coincide with this conceptualisation. While global surveillance infrastructures may not be equated with the networked society, this infrastructure seems largely dominated by technocrat-managerial elite, as is the case with the spaces of flows in the networked society. Again, this notion could be

enhanced with a perspective on non-human actors that can introduce their own kinds of dynamics into the realm of spaces of flows in the networked society. I suggest that this notion can be included in the notion of *elitism*: Just as the ordinary populace is generally understood to be barred from access to the managerial elite, technologies such as databases often entail their own kind of elitism as they are operated in secret or under corporate confidentiality. What function does the domination by elites fulfil? In both cases it seems that '[a]rticulation of the elites, segmentation and disorganization of the masses seem to be the twin mechanisms of social domination in our societies' (ibid. p. 446). This, lastly, leads to the observation that the space of flows, despite its preponderance as the dominating spatial configuration in the informational economy does not permeate every sphere of human life. People remain interwoven with places where they live and work and thus largely perceive their way of life as place-based.

Global cities and glocalised power

A useful instrument of analysis often deployed in the study of globalisation is the scale of *the urban*, and, on a more global scale, the *emergence of global cities.* Such a *spatial turn* brings to the fore the distinct ways processes of globalisation have produced new spatial configurations while such configurations simultaneously drive the dynamics of globalisation processes. *Global cities* as a tool of analysis as proposed by Saskia Sassen focuses on emerging strategic territories in the global informational economy (Sassen 2005; unless otherwise noted, the following aspects stem from this source). Global cities – as Castells demonstrated – can be understood as the command centres in networks of global flows which elude conventional forms of territoriality and even state sovereignty. As such, global cities are a spatial unit where global phenomenon and processes are reterritorialised, as the management of global flows has an inherently material dimension. Global commodity chains and internationally operating corporations, despite their geographic dispersion, usually entail a strong degree of centralisation of management and further core functions and headquarters of corporations thus largely produce new sites of employment and capital concentration which in turn are subject to new agglomeration dynamics. Emerging networks of global cities increasingly are of transnational dispersion as global integration intensifies.

Arguably there are caveats to Sassen's account of the emergence of global cities. For one, her conception of the nation-state has been described as static and failing to portray the prominent role nation-states play in the establishment of global cities within their territories (Brenner 1998, p. 11). Most crucially however, the focus on the globalisation of surveillance brought forward here will produce a markedly different understanding of the geography of command-

centres that oversee global flows. While global cities retain an important role in the context of globalising surveillance, there are also spatial aspects to it that are markedly *un-urban* and paradoxically bring peripheral places to the fore as key spaces in the interception as well as command of global flows.

Nonetheless, the strength of Sassen's conception of global cities lies in its ability to analyse what she refers to as the '*combination* of geographic dispersal of economic activities with simultaneous system integration' (Sassen 2012, p. 34; emphasis in original) under a analytically fixed unit such as the global city. To emphasise the combination of de- and reterritorialisation, Sassen explains (ibid.):

> The territorial dispersal of economic activity at the national and world scale implied by globalization has created new forms of territorial centralization. One critical and often overlooked fact is that this territorial dispersal is happening under conditions of ongoing concentration in ownership and control.

While phenomena such as global flows elude territorial fixtures, global cities are spaces where the material consequences – in the form of managing functions – and realities of such global flows crystallise and are intractably interwoven with the *local*, *regional* or *urban* or on other sub-national scales. This *interweaving* of global and sub-national scales is largely driven by and within the given spatial parameters and specific power relations behind those parameters, and by the broader ramifications of economic integration.

But how can one grasp the complex interplay of global phenomena and placed-based units through which these phenomena unfold which leads to the emergence of new spatial configurations? It is suggested here that Neil Brenner's conceptualisation of *glocalisation* is a helpful analytical tool for the scrutiny of emerging spatialisation configurations. In order to understand this conceptualisation, a few theoretical remarks seem necessary. To begin with, state spatiality appears as the key spatial arena within which glocalisation processes unfold. It can be understood as

> socially produced, conflictual and dynamically evolving matrix of sociospatial interaction. The spaces of state power are not simply 'filled,' as if they were pregiven territorial containers. Instead, state spatiality is actively produced and transformed through socio-political[sic] struggles in diverse institutional sites and at a range of geographical scales (Brenner 2004, p. 450).

Here again one encounters an understanding of space as a process rather than a fixed container. As such, *space* forms a multidimensional matrix of social action and constitutes a presupposition, medium and product of capitalism (Brenner 1997). The spaces in question are predominantly defined by the multitude of interaction unfolding within its boundaries – and the interaction with other spatial units. In relation to our focus of interest – namely the

intersection of non-fixed fluid global phenomena and territorially fixed – or place-based – units, the nation-state comes back into focus, a notion that largely resists conventional understandings of globalisation that assert the waning of state power. The spatiality of state power 'is at once a presupposition, a medium and a product of the conflictual interplay between *inherited* geographical parcelizations of state space and *emergent* political strategies intended to instrumentalize, restructure or transform the latter' (Brenner 2004, sp. 454, emphasis in original). Here it will come to no surprise that once again the general arena within which such processes unfold is globalisation.

Brenner understands that glo*b*alisation has led to new configurations of urbanisation and state territorial organisation in the shape of 'contradictory, contested strategies of reterritorialization through which the place-based and territorial preconditions for accelerated global capital circulation are being constructed on multiple spatial scales' (Brenner 1998, p. 3). As such, global cities are only but one of many dimensions of capitalism's changing global geography. Resisting conventional narratives of waning state power, Brenner argues that reterritorialisation is largely driven by the state providing both territorial organisation and infrastructure. Most crucially, Brenner argues that territoriality forms a central component of global flows even if such phenomena elude territorial boundaries: Territoriality provides the spatial frame for units below both the global and national scale, such as the regional or the local, that play pivotal roles in processes of globalisation. The importance of these sub-national scales derives from the fact that

> territorial states appear to be orienting themselves primarily towards the provision of *immobile* factors of production – i.e. those externalities associated with capital's moments of territorial fixity within spatial infrastructures organized on the sub-national scales of cities and regions (ibid. p. 15).

Beyond the provision of labour which is always materially situated at fixed localities, these sub-national units provide spatial arrangements such as conference centres, public-private partnerships, science parks, enterprise zones, export processing zones, locally oriented military spending and venture capital provision (ibid.). It is through the provision of such infrastructure that regional and local spatial configurations retain importance. To foreshadow a crucial observation made in this thesis, sub-national spatial units also eagerly provide immobile factors in global surveillance infrastructures, such as fusion centres, interception sites and key institutional arrangements.

In essence, spatial configurations such as global cities epitomise the notion of *glocalisation* as a dynamic of de- and reterritorialisation: Glocalisation is a *trajectory* of the spatial reconfiguration of territorial power in the shape of 'increasingly dense superimposition and

interpenetration of global political-economic forces and local-regional responses within the parameters of a single, re-scaled framework of state territorial organization' (ibid. p. 16). This interpenetration of global phenomena and regional responses entails a state-led delegation of core state functions upward or downward to supra-national or to regional/local spatial units. As such, glocalisation appears as a state-led agenda 'to position strategic local spaces competitively within global or supranational circuits of capital accumulation' (Brenner 2004, p. 473)

Glocalisation captures the phenomenon of global phenomena – eluding state territoriality – intersecting with spatial units bound to state territoriality. Glocalisation processes however may not be understood as mere reactions to globalisation, as glocalisation itself, Brenner suggests (1998, p. 16 f., emphasis in original)

> is at once the *outcome* of crisis-induced socioeconomic restructuring on urban-regional scales and a *medium* of state-led reindustrialization through a profound redefinition of each state's relationship to its major cities and regions.

This thesis will endeavour to take *glocalisation* slightly out of their context as it proves a helpful tool in the analysis of globalising surveillance.

On surveillance

This theoretical chapter so far has taken crucial aspects of globalisation into focus that will come into use when I scrutinise the globalisation of surveillance. The following sub-chapters in contrast will turn to an analysis of the changing environment and the organising logic of contemporary forms of surveillance which appears equally necessary for the study of the globalisation of surveillance.

Commercialised global (in-) security

This thesis understands that surveillance has undergone tremendous changes over the past decades, most of which are as much connected to the technological developments of surveillance infrastructures as they seem intractably interwoven with terrorism and global (in-)security, the networked society and the commercialisation of surveillance. As will be seen, these changes entail that surveillance has begun to 'morph from its erstwhile character as a centralized and hierarchical 'apparatus' of the state or of capitalistic corporations and started to take on a different character as a decentralized and rhizomic[sic] 'assemblage'' (Lyon 2004, p. 138, quotation marks in original). To begin with, numerous analyses observe that the attacks of 9/11, the advent of global terrorism and the concerted efforts of nation-states to curb it have had profound effects on surveillance (Price 2014, Bigo 2010, Keiber 2015, Lyon 2004, Monahan 2011, Fuchs 2013 p. 1334, Haggerty & Gazso, Monahan 2012, Gates 2012).

However, this thesis equally resists the apparent temptation to state that the aforementioned phenomena were initiated by 9/11 and its consequences (Monahan 2011, p. 84). Instead, ample evidence points to the fact that the described phenomena had been established long before the advent of global terrorism: While some forms of surveillance, such as the tapping of phones or the interception of mail have a very long history (Lepore 2013), surveillance operations such as the ECHELON programme, revealed long before the *Snowden leaks*, inform the notion that the bulk surveillance of entire populations in the name of security – or just because some states have the technological capacities to do so – has been an established practice before 9/11 (Verde Garrido 2015, p. 154). The same, of course, holds true for international collaboration in intelligence matters, economic spying and the targeted surveillance of foreign state officials and ordinary citizens. In consequence, the public outrage following the *Snowden leaks* seems equally somewhat surprising given the fact that many of the revealed surveillance practices had been known before, which points to a general disregard to established research in the field of surveillance in particular (Lyon 2015, p. 142) and the broader implications of previously revealed infrastructures, such as the ECHOLON programme, in particular.

However, 9/11 and the emergence of counter-terrorism can be understood to be of seismic effect on the discursive and consequently legal enactment of counter-terrorism and the increasing securitisation of the global. For instance, counter-terrorist legislation such as the U.S. Patriot Act would not have been possible if it was not for the attacks of 9/11 as catastrophes and terror attacks are generally understood to open time-windows for policy enactment that would not be possible if it was not for such events. The Patriot Act therefore served both to anchor already existing surveillance practices into federal law and to promote further intensification of such practices. Surveillance did not emerge in response to terrorism, but the 'political climate after 9/11 simply encouraged politicians, state agents, and others to embrace surveillance programs, in a public way' (Monahan 2012, p. 285).

Furthermore, the *War on Terror* provided ample incentives for a general shift from the prevention of threats to the yet incipient practice of their premediation as the prevalent answer to the perceived threat of global terrorism (de Goede 2008): The alleged mission of counter-terrorism has seen a shift from the pre-emption or prevention of factual threats to societies to the imagining and consequent pre-emption of *potential* terror attacks and global security risks. As such, the premediation of threats is not so much a project based on the future but on the deployment of future threat scenarios in the service of the enactment of policies and practices in the present (ibid. p. 159).

Phenomena such as the premediation of threats based on algorithmic analyses of communication data are arguably closely connected to the emergence of big data in the networked society and inform the notion that surveillance has become increasingly commercialised and privatised (Landau 2013, p. 61). These twin processes can be observed in two predominant forms: Firstly, the emergence of big data in the networked society produces new forms of surveillance, both quantitatively and qualitatively and equally reinforced exiting practices (Lyon 2014). *Big data* refers to the 'the capacity to search, aggregate and cross-reference large data sets' (Boyd & Crawford, quoted ibid. p. 2) that form the digital backbone of the networked society. The *Snowden leaks* provide ample evidence of how capacities and data sets are increasingly made use of in the context of both bulk- and targeted surveillance. Nonetheless, I here emphasise the contingency of the exploitation of big data for surveillance purposes. It seems that big data entails the *potential* use for surveillance but big data technologies do not inherently necessitate prevailing forms of surveillance that make use of these technologies. Again, the exploitation of big data is closely interwoven with the premediation of threats under prevalent counter-terrorist regimes as

> Big Data practices are skewing surveillance even more towards a reliance on technological ''solutions,'' and [that] this both privileges organizations, large and small, whether public or private, reinforces the shift in emphasis towards control rather than discipline and relies increasingly on predictive analytics to anticipate and pre-empt (ibid p. 10, quotation marks in original).

These conditions have created what Lyon (ibid. p. 1) frames as at least *ambiguous complicity* of Internet companies: Whether they are wittingly cooperating with Intelligence agencies or their databases and cloud services are exploited without their knowledge or consent, Internet companies seem intimately involved in the surveillance and mining of big data to the degree that observers speak of a *convergence of surveillance tracks* – corporate surveillance of metadata for commercial purposes and state-led surveillance of metadata for alleged security purposes (Price 2014, p. 45).

Secondly, the outsourcing of surveillance practices to private entities such as sub-contractors evinces the ongoing privatisation of core state responsibilities in the context of risk prevention – a phenomenon that doubtlessly extends beyond surveillance (see Klein 2007). Such corporate-state security relationships increase NSA dependency on 'private corporate services for the outsourced collection of data' and 'corporate owned data farms where the storage and analysis of the data occurs' (Price 2014, p. 46).

These processes underlie the notion of an ongoing commercialisation of global (in-)security. Beyond doubt, the emergence of global terrorism and global insecurity point to issues that run

deeper to the core of modernism and global political, economic and societal arrangements than can be explored here. The notion of global insecurity is possibly best captured in Beck's notion of the *risk society*: In contemporary societies, capitalist production increasingly goes hand in hand with the broad societal production of risks and thus the distribution of wealth across society is intractably interwoven with the distribution of conflicts and problems connected to techno-scientifically produced risks across society (Beck 1986, p. 25). Global terrorism as a challenge to global security can be seen as one of these produced risks which are distributed across societies on a global scale – as is their mediation (Lyon 2004, p. 137). For Beck, the notion of a *world risk society* describes the way modernity has brought about risks nation-states increasingly are either unwilling or unable to mediate themselves. Such risks consequently span across all societal strata and are simultaneously globalised and individualised in the sense that individual subjects have to bear the costs of globally produced risks (Beck 1986, p. 29 ff., Lyon 2004, p. 137). In this context, global surveillance can be seen as one of the ways by which global risks are mediated: Presented with a global uninsurable risk produced by modernity, the conflicts of distribution and mediation of this risk unfold on a global scale and within the lives of individuals alike, and the deployment of surveillance in this context comes at its own perils as

> the pace of surveillance growth, enabled by commercial pressure, technological innovation and cultural commitments to 'techniques-as-solutions', far outstrips the capacity of analysis and policy to understand and cope with it. Such surveillance both addresses risks and produces others (Lyon 2004, p. 137; quotation marks in original).

Emanating from this short overview are the multidimensional changes the environment of (global) surveillance is undergoing. But how can one grasp these developments and their particular relation to the global on a theoretical level? It is argued here that despite their prevalent use, the concepts of rhizomatic control and the surveillant assemblage remain powerful concepts in the analysis of the globalisation of surveillance, as does the concept of surveillance hegemony. It is to these different concepts that I turn to now.

The societies of rhizomatic control

Deleuze draws together three different concepts or metaphors useful for our analysis that need further attention: the society of control, the rhizome and the assemblage. Just as in Castells' *networked society*, the advent of information technologies presents a caesura in the periodisation proposed by Gilles Deleuze's view on the emergence of the societies of control. The advent of these technologies marks the shift from what Foucault analysed as the *disciplinary societies* to the societies of control. The 'environments of enclosure' of the disciplinary society – such as the prisons, families, schools, factories, etc. – have erupted into

a state of permanent crisis (Murakami Wood 2013, p. 319). Enter computers and information technologies: '[R]ecent disciplinary societies were equipped with thermodynamic machines [...] control societies operate with a third generation of machines, with information technology and computers' (Deleuze, quoted in Galloway 2001, p. 81). And just as Manuel Castells does, Deleuze relates information technologies to a restructuring of capitalism, only that the capitalism analysed by Deleuze brings about new modes of production, societal control and subjectivation. Under a capitalist system that has moved from production to the provision of services as its essential *modus operandi*, the intertwining of digitalisation and new forms of productions produce new forms of control (Deleuze 1990, p. 5 f.). The *bodies* or the subjects of this kind of control, Deleuze writes, become *dividuals*, a neologism evoking 'the dissolving of individual identity into distributed networks of information' (Galloway 2004, p. 12). This dividual finds itself in perpetuated modes of control, dubbed *modules* or *limitless postponements.* The subject of control is not foremost a to-be-disciplined body, but a subject absorbed in flows of data, samples and informational capitalist modes of production.

Galloway (2012, p. 522) rightly points to the fact that the French *contrôle* means both the 'the power to influence people and things, but [it] also refers to the actual administration of control via particular monitoring apparatuses'. Control seems clearly contrasted to the concept of punitive measures in pre-disciplinary societies and the disciplining enclosures of the Foucauldian societies, as control produces new subjectivities: 'Man is no longer man enclosed, but man in debt' (Deleuze 1990, p. 6). To be in debt implies having acquired certain goods (material, educational, virtual) and capabilities – which possibly help the subject advance in society – in exchange for financial means, which makes control as a form of domination all the more intricate. Another example Deleuze provides elsewhere is the image of the *freeway*, or the networks of freeways that make up the arteries of human movement on land: By constructing networks of freeways subjects are not enclosed but see their possibilities in movement multiplied and broadened; yet, what is equally multiplied are the means of control (Deleuze, quoted by Galloway 2012, p. 522). This understanding of control will become clearer in connection with its rhizomatic functioning elaborated below, which entails an increase in multiplicities as well as in *potentialities* of control. However, what is emanating from the *freeway example* already is that societies of control are societies where 'mobility is fostered inside certain strictures of motion, where openings appear rather than disappear, where subjects (or for that matter objects) are liberated so long as they adhere to a variety of prescribed comportments' (ibid.). In order to avoid techno-deterministic interpretations of control it seems noteworthy to underline once more the contingency of what

was coined *the historic moment we live in* (see chapter *Limitations to the findings of this thesis*): Deleuze seems to suggest that every society has its own kinds of technologies, but there need not be a causal relationship between the advent of information technologies and the shift from discipline to control: The here described technologies are merely the technologies the society of control has at hand, the technologies corresponding to the dispositif of control inscribed into the society of control. The emphasis on contingency firstly acknowledges that *things could have been different* in the sense that the described technologies could (have been) used for other purposes than societal control, and that consequently the advent of these technologies did not causally presuppose existing forms of control.

But how does control function in the society of control? How is it structured? The *postscript* redacted in its essayistic style only alludes to the ways control is structured: Presented as 'ultrarapid' and 'free-floating', as 'modulations' and 'independent variables' through which the individual subject passes, the forms of control are primarily translated into 'codes' and 'passwords' – and, most famously, the societies of control describe a shift from 'one animal to the other, from the mole to the serpent' whose 'coils [...] are even more complex than the burrows of a molehill' (Deleuze 1990). Luckily, this figurative interpretation of control can be enhanced by a study of the rhizome and assemblages. Rhizomes are structures found in plants where 'an immediate, indefinite multiplicity of secondary roots grafts onto it and undergoes a flourishing development. This time, natural reality is what aborts the principal root, but the root's unity subsists, as past or yet to come, as possible' (Deleuze & Guattari 2005, p. 5). As alluded to before, the rhizome grows via expansion and increase in multiplicities: Growing roots in any possible direction and interconnecting the different roots. When the rhizome breaks at any given point, it recommences its processes of expansion right then and there, and the possible connections are manifold and unlimited in number. As Deleuze and Guattari (ibid. p. 9) put it:

> Every rhizome contains lines of segmentarity according to which it is stratified, territorialized, organized, signified, attributed, etc., as well as lines of deterritorialization down which it constantly flees. There is a rupture in the rhizome whenever segmentary lines explode into a line of flight, but the line of flight is part of the rhizome. These lines always tie back to one another.

What one can see from the interplay of territorialisation and de- and reterritorialisation is a levelling of hierarchies (Haggerty & Ericson 2000, p. 614) to the degree where the rhizome can at any given moment merge with its different roots. In essence, the rhizome cannot be reduced to units for there are no clearly distinguishable units that *as a whole* form the rhizome. The rhizome consist of dimensions multiplying as it expands, and as such only

consists of a middle and the off-shooting roots that can form new rhizomes on their own or connect back to the middle at any given moment (2005, p. 21). This logic explains the quoted notion[1] of expansion through deterritorialisation until the rhizome forms an abstract machine covering the whole plane of consistency: The middle of the rhizome can deterritorialise at any given moment into myriads of roots expanding into all directions and drawing new interconnections and finally reterritorialise into middle structures consisting of joint roots. This form of expansion can be operated indefinitely until the rhizome penetrates the entire field within which it expands.

In a nutshell, the rhizome serves as a metaphor of how control mechanisms work and expand in societies of control. Just as the rhizome can grow into a ubiquity of roots and interconnections, so can the forms of control expand and merge into new forms or reinforce pre-existing forms of control. And just as removing a string of roots does not affect the rhizome, so does removing one control mechanism in the society of ubiquitous control not affect the overall working logic of the society – i.e. control.

The principles behind rhizomatic organisation and expansion are of importance for this thesis for two reasons: Firstly, they present a suitable metaphor for the organising logic of distributed communication networks (Galloway 2004) which will play a prominent role through this thesis. Secondly, this thesis argues that global surveillance infrastructures can be seen through the foil of rhizomatic organisation and expansion, where, as with the rhizome, '[w]e can no longer even speak of distinct machines, only of types of interpenetrating multiplicities that at any given moment form a single machinic assemblage' (Deleuze & Guattari 2005, p. 36). It is this notion of the surveillant assemblage that I turn to now.

The surveillance assemblage

At this point it seems worthy to relate the *assemblage* to the context of surveillance, as brought forward by Haggerty and Ericson's concept of the *surveillant assemblage*. Haggerty and Ericson observe that in contrast to historic forms of surveillance, modern forms of surveillance increasingly monitor population groups that had not been monitored previously. This monitoring occurs under the partially concerted operation of a multitude of surveillance systems 'abstracting human bodies from their territorial settings and separating them into a series of discrete flows. These flows are then reassembled into distinct 'data doubles' which can be scrutinized and targeted for intervention' (Haggerty & Ericson 2000, p. 606, quotation marks in original). Such a multiplicity in surveillance systems is best understood in the shape

[1] See chapter *Global assemblages and the dialectics of de- and reterritorialisation*.

of the surveillant assemblage. Assemblages, the authors explain in reference to Deleuze and Guattari, are multiplicities of diverse and heterogeneous units solely united in their *working together*. As such, they

> comprise discrete flows of an essentially limitless range of other phenomena such as people, signs, chemicals, knowledge and institutions. To dig beneath the surface stability of any entity is to encounter a host of different phenomena and processes working in concert [...] any particular assemblage is itself composed of different discrete assemblages which are themselves multiple (ibid. p. 608).

This again is the previously encountered multiplicity in dimensions of assemblages, the propensity to enlarge one's territory by means of de- and reterritorialisation. However, Haggerty and Ericson specify an aspect unmentioned thus far: Most crucially, the surveillance assemblage exists as a *potentiality*: The possibility that surveillance systems, technological devices and the manifold possible connections between these different interfaces *can* be interlinked under a common purpose. It is precisely this possible connection of a multitude of systems and devices that makes the surveillance assemblage thus powerful: It cannot be undermined by prohibiting or fighting a particular technology or manifestation of surveillance, or by abolishing particular practices of surveillant institutions (ibid. p. 609). This augmentation in potentiality increases the factual possibilities of monitoring targets as surveillance practices span across state and non-state actors and infrastructures. In terms of specific targets and specific forms of surveillance, the assemblages entails that *if you cannot get a target one way, you may very well get it another way.* For the surveillant assemblage represents the 'desire to bring systems together, to combine practices and technologies and integrate them into a larger whole' (ibid. 610) which is likely to have one of its heterogeneous units successfully direct its focus on any given target.

As with Manuel Castells' *networked society*, spaces and flows play a central role in the functioning of the *surveillant assemblage*. The surveillant assemblage captures and recreates flows of information and communication data, essentially a process of 'introducing breaks and divisions into otherwise free-flowing phenomena. To do so requires the creation of both spaces of comparison where flows can be rendered alike and centres of appropriation where these flows can be captured' (ibid. p. 608). The assemblage manages to deconstruct human communication into flows of data and reassemble these flows according to prevailing modes of governance and surveillance. With regard to factual surveillance infrastructures, the aforementioned *spaces of comparison* are centres or key nodes in global surveillance networks, such as fusion centres in the U.S., where intercepted data is analysed, processed and stored, while *centres of appropriation* can be equated with both interception sites and the

sites where surveillance operations are conceptualised, coordinated, implemented and possibly carried out from afar.

Once again, the metaphor of the rhizome offers helpful contributions: Just as the rhizome has no clear beginning nor end and operates based on multiplication, 'variation, expansion, conquest, capture, offshoots', it remains 'an acentered, nonhierarchical, nonsignifying system without a General and without an organizing memory or central automaton' (Deleuze & Guattari 2005, p. 21). The rhizome expands through deterritorialisation and interconnections between its branches. Similarly, Haggerty and Ericson explain, no single technology has brought about the potential surveillant assemblage, but 'its expansion has been aided by subtle variations and intensifications in technological capabilities, and connections with other monitoring and computing devices' (Haggerty & Ericson 2000, p. 615). Very much like the rhizome, the surveillant assemblage expands its capabilities and its reach through countless offshoots that interconnect and form their own (sub-)assemblages. Most crucially, assemblages are not governed by a single organising logic, or a *General* in the words of Deleuze and Guattari, and thus the assemblage is not directed asymmetrically according to the will of the powerful. The assemblage, as is the case with the rhizome, is strictly non-hierarchical and without a centre. Haggerty and Ericson point to this fact as they stress the emergence of counter-surveillance technologies and the fact that powerful groups of society can equally be subject to monitoring techniques and practices, while maintaining that turning the surveillant assemblage against powerful groups remains largely a potentiality (ibid. p. 617 f.).

It is exactly this kind of expansion through interconnections between potential multiplicities that makes the surveillant assemblage a crucial analytical tool in the study of the globalisation of surveillance. To foreshadow a key finding of this thesis, the globalisation of surveillance is largely driven by the *working together* of manifold technologies and constant processes of de- and reterritorialisation of surveillance infrastructures and practices, evinced by the NSA global surveillance apparatus. As such, the emergent global surveillant assemblage consists of heterogeneous units that in turn form their own assemblages while nonetheless subsumed under prevailing surveillance regimes. Digitalisation and information technologies have allowed for a shift in surveillance practices and infrastructures whose constant processes of de- and reterritorialisation have expanded the reach of the global surveillant assemblage.

In essence, the surveillant assemblage allows for a potential penetration of human life that knows few boundaries and whose reach

> can involve something as direct as tagging the human body so that its movements through space can be recorded, to the more refined reconstruction of a person's habits, preferences, and lifestyle from the trails of information which have become the detritus of contemporary life. The surveillant assemblage is a visualizing device that brings into the visual register a host of heretofore opaque flows of auditory, scent, chemical, visual, ultraviolet and informational stimuli (Ibid. p. 611).

However, the concept of the *surveillant assemblage* has drawn justified criticism. How does the *working together* of heterogeneous units work if there are no directing institutions behind the assemblage? The simultaneous suggestion that the assemblage is without central automation and yet simultaneously a concerted operation seems problematic as this entails an 'ascription of agency to the theoretical concept itself' (Barbara Prainsack and Victor Toom, quoted in van der Velden 2015, p. 184). Beyond the obvious conceptual deficiency that comes with such an approach – the assemblage is not a machine or a set of existing operations, but only a theoretical tool, a visualisation, that seeks to grasp the multiplicity of ways surveillance infrastructures can be synchronised – such an ascription of agency also brushes aside questions about the specific actors behind specific surveillance technologies and practices (ibid.).

In his defence, Haggerty saw this inherent weakness to the *surveillant assemblage*, conceding later that centralisation is a de facto way by which the assemblage can be deployed: The different subsystems and sub-assemblages can occasionally be integrated 'when powerful agenc*ies* work to combine and align these dispersed [surveillance] systems, often to serve purposes that were not part of the original rationale for the development of each particular subsystem' (Haggerty & Gazso, 2005, p. 174, emphasis added). The emphasis added here points to the fact that according to Haggerty and Gazso centralisation within the assemblage does not occur under the umbrella of a single entity operating the totality of technologies subsumed under the assemblage, but rather entails the cooperation of specific entities to 'combine, integrate and deploy the diverse systems that they and other organizations have established' (ibid.). It is in the spirit of this concession that I combine the *surveillant assemblage* with the now following conceptualisation of *surveillance hegemony* which brings the state as an actor back into focus and will ultimately serve as a justification for the later undertaken scrutiny of global NSA surveillance infrastructures.

Surveillance hegemony

This thesis concurs with Jason Keiber's (2015) critique that the focus on assemblages and the minutiae of hidden and diffuse means of surveillance can lead to a neglect of state-centred hierarchies within surveillance infrastructures. States still matter in the context of surveillance. With *surveillance hegemony*, he provides a useful tool of analysis. In trying to

grasp global U.S. surveillance infrastructures, Keiber starts with the observation that *hegemony* in general implies an exercise of power that derives its legitimacy from more than just material preponderance, but rather from a stability that rests upon and is reflected within a set of rules, institutions and ideas in the shape of social norms and dominant ideologies. Hegemony as such remains hierarchical, but

> [c]ompliance and participation within the order is ultimately ensured by a range of power capabilities available to the hegemon—military power, financial capital, market access, technology and so forth. Direct coercion is always an option in the enforcement of order, but less direct 'carrots and sticks' are also mechanisms to maintain hegemonic control (John Ikenberry, quoted ibid.).

The exercise of hegemony therefore occurs in manifold ways. Institutions through which it is exercised can be international or supranational and operate in a number of economic, political and diplomatic realms. Dominant ideologies can be grasped in the shape of powerful narratives and depictions about and of the world that resonate throughout the international hemisphere in which hegemony is exercised. Crucially, even if the dominant ideology is not fully accepted, adherence to it is manifested in the actions of the states subjected to hegemony. This voluntary adherence derives from the key characteristic of hegemonic rule: Direct coercion is just but one rarely made use of instrument as the subjects of hegemony follow the lead of the hegemon, for it is *equally beneficial* to them based on the way the entire order is arranged. The hegemonic system is therefore replete with incentives to the subjects of this hegemony that reward their adherence and softly penalise their opposition.

One of the key domains of hegemonic rule is the exercise of infrastructural power. Infrastructural power, based on sociologist Michael Mann, comprises the 'capacity of the state to actually penetrate civil society and implement its actions across its territories' (Mann 2008, p. 355). *Capacity* in this case entails both the potential as well as the deployed resources of the state, *through which* power can be exercised (ibid. p. 357). Infrastructural power is a way of *caging of social relations* into coherent entities that can be governed, such as closed societies or nation-states. *Hegemonic rule* consequently entails the capacity of the hegemon to *project its infrastructures* into other states (Keiber 2014, p. 45). This projection of infrastructures in turn presents one of the key channels for the hegemon through which its hegemonic power is exercised. Once the infrastructures of the hegemon have successfully been projected into other states, hegemonic rule seems somewhat softened as the need for direct coercion is further reduced. This projection serves multiple purposes as it not only instils hegemonic rule, but also facilitates and reproduces its exercise.

What then is *surveillance hegemony*? Keiber argues that surveillance hegemony deserves to be scrutinized independently of conventional conceptions of hegemony for two reasons: Firstly, surveillance increasingly plays an integral role in the *raison d'être* of contemporary states and embodies a realm where the state retains its tight grip on political and infrastructural power. Secondly and more crucially, surveillance hegemony other than conventional hegemony does not merely base its footing on post-war (neo-)liberal discourses that have helped install the U.S. as key hegemon in the contemporary world order, but its legitimacy hinges upon security discourses: 'in order for the West's anti-terrorism discourse and its related security practices to spread, there needs to be a discursive fit between the agenda of the US[the hegemon] and the norms held by the security and intelligence elites of other states' (Keiber 2015, p. 171). As such, surveillance hegemony, while clearly intertwined with other conceptions of hegemony, deserves its own use here as an instrument of analysis for the particular traits it evinces: Firstly, surveillance hegemony is based on the increasing securitization of Western societies framed as collective efforts to tame terrorist threats. Undoubtedly, such a discursive legitimization seems somewhat surprising given the fact that terrorism remains a minor threat to Western societies whose reactions to this threat can be interpreted as overwrought (ibid. p. 172; see Mueller & Stewart 2012; Harbisher 2015). Nonetheless, it seems that the counter-terrorism narrative constitutes what largely weaves together a surveillance environment in which the states with the widest capacities to counter terrorists have a preponderant position: Most saliently, terrorism is framed as a constant, predominant threat *to* everybody emanating *from everybody* in the sense of individuals, rather than collective entities such as other states: 'The broader counter-terrorism norm is that states should cooperate in counterterrorism, and effective counter-terrorism entails cooperative international surveillance of individuals' (Keiber 2015, p. 175).

Secondly, surveillance hegemony entails the existence of a surveillant hegemon managing to project its surveillance infrastructure into other states. In the case of surveillance, this projection to a considerable degree entails the transfer of technologies of surveillance and the use thereof. The hegemon possesses technologies and the capacity to master these technologies that eludes other states. These technologies are transferred to the subjected states by ways of transfer and training of personnel to use these technologies properly. This not only facilitates interoperability of surveillance infrastructures, but further enhances dependence on the hegemon and reproduces both its hegemonic position and literally the way it *perceives* the world. *Training* is a key term here as it stands for the internalisation of values just as much as the desired exercise of certain capabilities:

> Training produces a common working knowledge and vocabulary, facilitates interoperability, and lays the foundation for future cooperation. The state providing the training reproduces its own practices in the trainees. The result is multiple states working with the same optics (Keiber 2014, p. 148).

Thirdly, surveillance hegemony plays out largely without direct coercion by the hegemon, but rather through the projection of infrastructures and the erection of an order which directly and predominantly indirectly compels other states to adhere. This is embodied, Keiber argues, by the fact that relationships between the hegemon and its subject states are largely depicted as partnerships that involve the *capacity-building of intelligence partners* and the *sharing of responsibilities* in joint counter-terrorism efforts (ibid. pp. 59-69). As such, the surveillance hegemon is understood to come to the help of other (possibly *weaker*) states rather than imposing its security regime on such states (Keiber 2015, p. 173).

Fourthly, surveillance hegemony must be fitted in an institutional framework replete with legal treaties conducive to the exercise of surveillance hegemony. Amongst other frameworks, the UN in the shape of Security Council Resolutions 1267 and 1373 which compel states to share counter-terrorism information with each other and to keep lists of sanctioned individuals, prove a fertile ground for the counter-terrorism trajectory (Keiber 2014, pp. 72-75). Other representative institutional arrangements in this context are INTERPOL or The Global Counterterrorism Forum (Ibid. p. 77 ff.; for a detailed study of INTERPOL's surveillance network see Gardeazabal & Sandler 2015).

Fifthly, the infrastructural relationships amongst concerned states and with the hegemon, all under the umbrella of surveillance hegemony, tend to take the following shapes (as long as it is a successful relationship out of the perspective of the hegemon): The infrastructures of the states or security apparatuses can become *shared* where both states contribute to surveillance practices at hand. The 'extent of sharing can vary. On one end of the spectrum there may be a merging of state resources and personnel. On the other end, the host state may simply give permission for the projecting state to conduct surveillance.' Or the infrastructures can become *synaptic* when the surveillance infrastructures of these states merge to a certain degree. This can entail either the growing closer of surveillance infrastructures in proximity or a move towards interoperability. Sixthly, this relationship of infrastructures can amount to the hegemon installing its infrastructures on the subject state's surveillance sites and directly tapping into these infrastructures, with or without the consent of the concerned state (Keiber 2014, p. 45).

Finally, as with many kinds of hegemony, surveillance hegemony is not a one-sided arrangement and the hegemon itself, despite its expenses in resources in order to uphold its

hegemonic position, benefits from the overall order. In surveillance matters, the putting-in-place of technologies into different states and the training of personnel and the maintenance of these technologies might come at a certain material cost, but at the same time the hegemon is granted access to new kinds of intelligence and can further tighten its grip on global surveillance infrastructures.

This thesis refers to the NSA as the surveillant hegemon. On the one hand, the NSA by far outmuscles other security agencies in terms of funding, the number of employees and of surveillance operations run on a global scale (Bauman et al. 2014, p. 126 f.). Furthermore, the NSA seems to be the driving force in the context of all the partnerships it maintains with other agencies (see below). The *Snowden leaks* have produced a complex picture of globally maintained partnerships and collaborations that demonstrate how the NSA is actively solidifying its position within global surveillance. On the other hand, American surveillance hegemony seems largely historically grown, be it terms of America's tight grip on the physical infrastructures of the Internet (see below), its capacity to coerce U.S. companies – often global market leaders – into ambiguous partnerships (see below) or in terms of general US post-war military hegemony. NSA surveillance capacities seem unmatched and the here scrutinised globalisation of surveillance is intractably interwoven with NSA efforts to further solidify its hegemonic position on a global scale.

Chapter 3: On networks

This chapter presents a nexus between theoretical framework and the empirical chapters that follow, as it contains both theoretical conceptions, such as the organising logics of networks and the economics at play within networks, and more empirical observations, such as the structural analysis of the Internet and protocols. Therefore, this chapter builds another footing for the descriptive inference of the globalisation of surveillance undertaken below.

Three communication network types: centralized, decentralized and distributed networks

Paul Baran's *On Distributed Communication Networks* (1964) is arguably seen as one of the founding articles of modern communication networks in general, and the Internet in particular. Baran's search for novel types of communication networks originated in the geo-political context of the Cold War. As nuclear testing had proven that high altitude nuclear blasts would disrupt long distance short wave (high frequency) transmission, and given the fact that communication networks at the time were mostly built upon the transmission of such

waves, Baran and others sought to find a new type of network structure that could withstand a nuclear blast. In network terms, what was needed was a network robust enough to withstand the enemy destruction of many nodes and allow for intercommunication between the remaining (physical) nodes (Baran 2002, p. 265 f.). The answer Baran found to this predicament lay in distributed networks and the technology of packet-switching. Baran famously differentiated between three different types of communication networks, namely the centralised, decentralised and distributed network, each with markedly different architectures (Figure 1) (ibid. p. 266 f.; 1964, p. 1).[2]

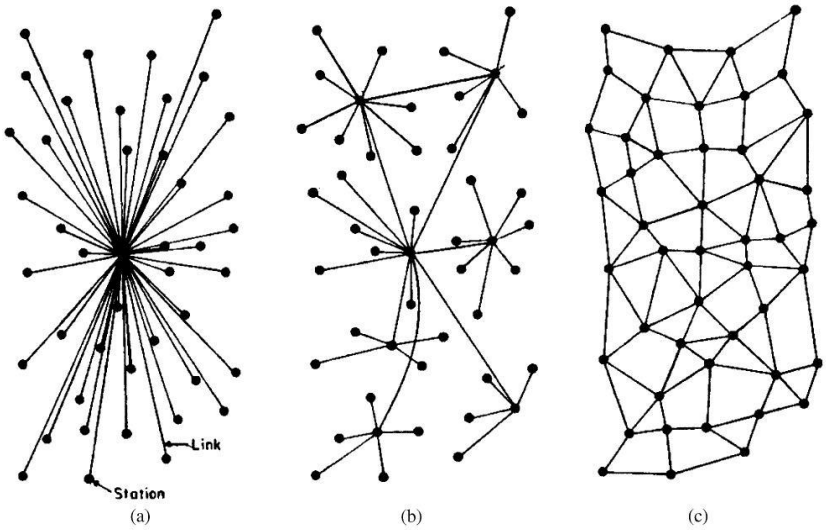


Figure 1: Three network types 1

The *centralised* network (a) is comprised of one central node (hub) that is connected to *n* possible stations (hubs) via direct links between the central hub and each node. This network type exhibits a strong hierarchy as any connection between two nodes has to be set up as a connection from node n_1 to the central hub and from the central hub to n_2 (or vice versa), which Baran refers to as *simple switching* (Baran 2002, p. 266 f.). The nodes, subordinate by nature, are therefore dependent on the central hub and are not connected individually, and all activity travels from centre to periphery (or vice versa) (Galloway 2004, p. 30). On the one hand, this set-up entails maximised central control, as each connection passes through the central node. On the other hand, maximised vulnerability inheres in this type of network as the entire communication is taken down in case the central node is destructed. In contrast, the

[2] I am aware of Alexander Galloway's (2011, p. 90) critique that the reproduction of this type of mapping of communication infrastructures entails 'a massive repetition of the same and nothing more' as such mapping routinely relies on the 'hub-and-spoke aesthetic' where '[n]odes are connected by links. [...] the legibility of the map remains suspiciously one-sided, even ideologically motivated.' However, it is hoped that the mapping of US digital and geo-political surveillance infrastructure undertaken in this thesis does justice to Galloway's implicit demand to pay more attention to the usually cast aside 'facts on the ground' (ibid.).

decentralised network consists of several centralised clusters within which most traffic occurs while the rest of traffic travels through longer links connecting the different clusters (Baran 2002, p. 267). This multiplication of centralised networks entails a more flattened hierarchy where there is no single hub that exercises control over all other hubs and links. At the same time this network type exhibits a greater robustness than centralised networks as the destruction of one or several (but not all) central hubs or links does not necessarily compromise all communication. Looking at the overall flows of traffic it remains nonetheless with stark vulnerabilities.

The *distributed* network is the most robust and intricate network. It has no central hubs and each node is an autonomous agent functioning as 'intelligent end-point systems that are self-deterministic, allowing each end-point system to communicate with any host it chooses' (Hall 2000, p. 6). The robustness of the distributed network stems from the infinitely higher number of possible connections between two nodes as traffic can be routed around the failing parts of the network (Baran 2002, p. 269). The essential question with regard to the *connectivity* of the network proposed by Baran was: How does the switching of one connection to another work at each node? The answer to this lay in *packet-switching*.[3]

Packet-switching is a 'data transmission technique whereby user information is segmented and routed in discrete data envelopes called packets, each with its own appended control information for routing, sequencing and error checking' (Data Communications Glossary, quoted by Baran 2002, p. 265). In essence, each packet is able to find its own way while its route is not predetermined, but determined at each new node it reaches. Should a node be damaged or failing completely, the packet just travels to another node. Future routing is always determined at the present node. Once all packets of the same user information have arrived at their final destination, they reassemble and create the original message (Sprenger 2015, p. 86; Galloway 2005, p. 20). The routing protocol proposed by Baran (2002, p. 270) merely consists of a 'to' and 'from' address field and 'handover counter' field that informs the network of the length of the path taken by each packet, thus growing with every link travelled. Lastly, two requirements build in this technology are that firstly in-transit storage time of each packet at the nodes should be minimised, and that secondly the shortest possible path throughout the network should be found within the changing network landscape (Baran 1996, p. 6).

[3] While Baran is contributed with the general principles behind packet-switching, British scientist Donald Davies, who worked on very similar technologies but who was unaware of Baran's research, coined the term *packet-switching*. See Galloway 2005, p.20; Baran 2002, p. 273.

Baran's trailblazing research was of seminal importance to emerging contemporary communication networks. The Internet has to be understood, on the one hand, as a computational network allowing for global flows of data and all kinds of traffic, regulated by protocols as the organizing mechanisms in the digital sphere. This computational network is a global distributed network that comprises many different computational networks, the World Wide Web being one of the most important of these networks. As a matter of fact, the Internet has to be understood as a *network of networks*:

> An Internet communication system consists of interconnected packet networks supporting communication among host computers using the Internet protocols . . . The networks are interconnected using packet-switching computers called 'gateways' (Robert Braden, quoted in Galloway 2004, p. 38. Quotation marks in original).

At the heart of these different packet networks, computers functioning as hosts generally execute 'application programs on behalf of user(s), employing network and/or Internet communication services in support of this function' (Braden, quoted ibid.). Equally close to Baran's distributed network is the functionality of headers on the Internet. Similar to what Baran referred to as data envelopes that carry from-and-to-descriptions, headers contain data concerning network address of source and destination, while the rest of each packet comprises the *payload area* which in turn contains the actual sent data (Fuchs 2013, p. 1333). This metadata contained in the header has to be accessible for every node the data packet trespasses, which in turn usually does not save the metadata for longer than the duration of the successful travel of the concerned data packet to the next node.

Baran's distributed network on the one hand stands for a greater robustness, but it is crucial to understand that the distribution of autonomous nodes in a non-hierarchical way does not imply that control has been removed. On the contrary, as the subsequent chapters will show, distributed networks 'produce an entirely new system of organization and control that, while perhaps incompatible with pyramidal systems of power, is nevertheless just as effective' (Galloway 2006 p. 318).

Protocols

In general, *protocol* as used here refers to the technology of organisation and control in distributed computer networks. As the distributed network is comprised of autonomous nodes, absent of one (or more) hubs that make governing decisions, there needs to be some kind of organisational function so that packets sent through the network eventually make it to their final destination where they are reassembled into the original message. Otherwise, distributed networks would become ungovernable to the extent of disfunctionality and stable communication would be rendered impossible. Therefore, protocols as a set of generally

applicable rules ‘govern[ing] the set of possible behavior patterns’ (Galloway 2001, p. 83) within the network seem indispensable. In principle, protocols operate at the level of coding:

> they encode packets of information so that they may be transported, they code documents so that they may be effectively parsed, and they code communication so local devices may effectively communicate with foreign devices (ibid.).

Returning to the example of Baran’s distributed network, protocols, for instance, are responsible for the way messages are divided into packets, how these packets are categorised or what kind of header they carry, how they are sent through the network, how they are dealt with at the nodes, for a shared language at the nodes, what happens to the packets when a link is disrupted and the packet returns to the sending node, and how packages are reassembled and reconstructed once all packets of one message have arrived at the final destination. In order for all these tasks to be overseen and performed accordingly, networks consist of nested protocols, as no single protocol can oversee all these tasks operating simultaneously under the conjoint goal of directing and ensuring the flow of information (ibid. p. 84; Thacker & Galloway 2014, p. 297, 303.)

Protocols thus are the core functioning principle for distributed networks and their importance cannot be overstated. There are a number of crucial characteristics inherent to protocols: Firstly, their formality. Protocols divide and encapsulate information into packets and remain relatively indifferent to the content of these packets (Galloway 2005, p. 22; 2001, p. 83. Sprenger 2015, p. 34 f.). They primarily ensure the preservation of content (Thacker & Galloway 2014, p. 297; Galloway 2006, p. 319) as data is parsed but not read and it is mainly the header of each packet that is accessed. Secondly, protocols allow for interoperability among different technologies (DeNardis 2012, p. 723). Thirdly and closely related to their pivotal role in distributed networks, protocols ‘also exist in historically and culturally specific contexts’, despite their technological formality (DeNardis 2015, p. 72). This undoubtedly makes protocols one of the key arenas in which political rights and social norms are constantly negotiated in the digital sphere. Such power struggles often (but not exclusively) evolve around encryption, security, privacy and alternative communication infrastructures, and are often framed in dichotomies such as *liberty vs. security* or *privacy vs. surveillance* in public discourse. Given that protocols are largely designed by private companies and standard-setting institutions outside the legislature, questions are regularly raised concerning public interest, Internet governance and the legitimacy of private entities to function as standard-setting institutions (DeNardis 2009, 2012, p. 723; 2013, 2014). Accordingly, societal conflicts increasingly materialise across different levels of Internet governance (DeNardis &

Hackl 2016). Lastly, protocols are key entry points for entities engaging in network surveillance. This derives from their pivotal importance to and central functionality within networks such as the Internet, which entails a considerable amount of control. While control in the context of computer networks might be of necessity for network maintenance and the stability of flows, it also entails the existence – but not the necessity – of surveillance (Sprenger 2015, p. 24).

Internet protocols

Internet protocols, usually contained in the Request for Comments (RFC) documents, the publicly accessible core rules and policies of the Internet managed by the Networking Division of the University of Southern California's Information Sciences Institute, form an essential part of the Internet's infrastructure (Galloway 2006, p. 82). In application of the general protocological principles laid out in the previous chapter, the Internet as a distributed network consists of several nested protocol layers with different functions (Figure 2). *Nested* in this context signifies that the transport layer is encapsulated within the internet layer, while the application layer is encapsulated within the transport layer, and so forth (Galloway 2004, p. 39. For another convincing conception see Hall 2000, p. 7 ff.). The different layers work together in the following way (Galloway 2004, pp. 40-49; Thacker & Galloway 2004, p. 297 ff.): The application layer is responsible for the content of the used technology (i.e. an emailing programme or a web browser), preserving the content of the data during the network transaction. The transport layer is higher up the hierarchy than the application layer and responsible for the correct transit of data through the network (while not responsible for the actual act of transporting the data). It ensures that data is sent from one node to the other and that individual packets make it to their final destination. The internet layer is still larger than the two previous layers and is preoccupied with the actual movement of data through the network and remains largely indifferent to content. The final layer describes the actual hardware equipment through which data moves, e.g. fibre-optic cables.

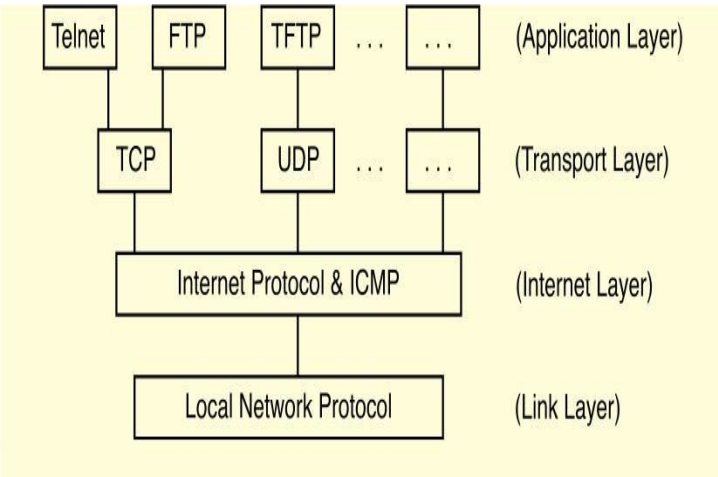


Figure 2: Protocological Internet layers

This division of labour allows the Internet to work efficiently and function properly. There are two sets of protocols which deserve special mention at this point. On the one hand, Transmission Control Protocol (TCP) and Internet Protocol (IP) are the main protocols responsible for the transport of data to and via the autonomous nodes (Galloway 2001, p. 83 f.). TCP/IP is a *family* of protocols and not two individual protocols, and this collection of protocols ensures that a connection from node n_1 via n_n to n_2 is established. In this case TCP is 'responsible for the "handshake" that happens between two computers at the moment a connection is established', while IP fragments data into packages and routes them from one node to another and eventually reassembles them (Galloway 2004, p. 42-45; quotation p. 42, quotation marks in original). TCP/IP use an 'anarchic and highly distributed model, with every device being an equal peer to every other device on the global Internet' (Hall 2000, p. 407), thus degrading any kind of notion of hierarchy.

The other protocol worth mentioning here, the Domain Name System (DNS) forces hierarchies upon the entire system. DNS, in a nutshell, is a decentralized database that translates names (used by humans) into numbers (used by computers), e.g. a website's name (*www.thesisonGlobalisingsurveillance.com*) into an IP address (*110.235.345.682*) (Galloway 2004, p. 47. Examples mine). DNS is highly hierarchical insofar as a handful of *root-servers* exercise control over the entire DNS database and merely delegate control and access to lower branches of the hierarchy (Galloway 2001, p. 84). As with Baran's centralized network, DNS is vulnerable to external control, manipulation and surveillance, something that governments and private actors routinely resort to by means of port-scanning, filtering, rerouting and blocking (DeNardis 2012, p. 728 ff.; 2013, p. 42).

In essence there are two very different sets of protocols at work here, the deterritorialising TCP/IP family and the reterritorialising DNS (Galloway 2001, p. 8; see also: C't - Magazin für Computertechnik 2014). The here undertaken look at the different Internet protocols allows us to understand two points of critical importance to the analysis of digital surveillance. On the one hand, even on the protocological level the Internet has to be understood as a complex and at times paradoxical set of technologies that epitomise the way infrastructures do not grow *de novo* (Leigh Star & Bowker 2006) and usually develop out of preexisting infrastructures. At the same time, infrastructure only becomes visible upon breakdown while usually remaining invisible to the average user. The working together of protocols as obverse as TCP/IP and DNS evinces the technological complexity of the Internet. On the other hand, it seems that the more intricate a system, the more intricate the ways control can be exerted within this system. The emergence of the Internet has coincided with

the emergence of distributed and yet highly effective forms of control. It is to this notion that I turn to now.

Protocological control

As alluded to above, the formality of protocols and the anarchic type of routing within distributed networks does not put an end to control, but rather allows for new forms of it. What seems unusual but is deeply inscribed into protocols is that this type of control is based on 'openness, inclusion, universalism, and flexibility [...] [,] control borne from high degrees of technical organization' (Galloway 2004, p. 142).

Part of this new type of control originates in the previously mentioned tension of radically distributive and highly hierarchy-oriented principles behind core protocols, the tension between TCP/IP and DNS. While the former relies on universally applicable standards, such standards have to be universalised somewhere, and generally accessible, which materialises in a bureaucratic, centralised institution such as DNS. While the former in its highly distributive nature has to rely on standardisation, the latter ensures the universality of standards. This logic entails the moment of protocological control: Only if there is a shared protocol, networked communication is possible. Any kind of communication in a network using a certain protocol has to oblige to the standardisation implemented by the protocol. While this enables radical openness on the one hand, given the formality of protocols, it also entails rigid control mechanisms (Sprenger 2015, p. 22). Such control cannot be equated with surveillance, for control is necessary if both stability of flows and orderliness of communication are to be ensured. For instance, control is part of every switching process occurring at every node. If it was not for this type of control, packets would be free-floating eternally, and communication would be rendered a matter of randomness. Control is exercised when TCP/IP reads and evaluates header information at the nodes. This type of control has to be understood as a form of network maintenance. Traffic works orderly as long as it is operated within the parameters set by protocols. Once again, distributive routing of packets is only possible due to its universalised standardisation, namely the composition of headers. This standardisation ensures the radical openness of the network on the one hand as it ensures that what is of only concern is the orderliness of the header, but the format invites multiple vulnerabilities which in turn enable not only control, but also surveillance. Deep Packet Inspection (DPI) is a case in point: DPI comprises a set of technologies that penetrate the packets while in transit at the nodes on a deeper protocological level than the transport layer, thus effectively accessing the payload of the transiting packets which in turn grants access to the content comprised in the packet. Again, while DPI can be used for network maintenance purposes, such as the

detection of malware, viruses and other network security related issues, it can also be used for all kinds of surveillance (DeNardis 2012, p. 725). Fundamentally, a look at the organising logic of the distributed network reveals the ubiquity of possible control and/or surveillance sites, as nodes are *virtually everywhere* and form an integral part of the networks' very infrastructure. If every node is a site of control, and control potentially allows for surveillance without necessitating it, the possibilities to exploit the network for surveillance purposes seemingly abound.

This notion can be connected, once more, to Deleuze's *postscript* where computers are the key medium through which control is established (Deleuze 1990, p. 6). The distributed network serves as an example of a structure eluding centralised command and control, but rather operates through myriads of control sites and mechanisms (Galloway 2004, p. 5). As such, the distributed network appears as the playing field of the society of control and protocol as the materialised moment of individuation and control (Thacker & Galloway 2014, p. 293; 303). In a nutshell, distributed networks and protocols do not represent an emancipation of control. Rather, they stand for a form of control that in itself is more distributed than other forms of control. This transformation of control has taken aim at flows of information, intercepted at nodes in the shape of individuated data packets and has taken control to the micro-level of human interaction (Sprenger 2015).

On network economics: externalities, monopolies, merging of networks

This chapter serves to revise economic principles at work in networks. I argue that bringing the 'economic construct of network externalities' (DiMaggio & Cohen 2003, p. 3) into the here undertaken analysis allows for fruitful ways of understanding processes of globalisation within global surveillance infrastructures. The here elaborated principles are laid out in a generalised way, for it is understood that network economics come to play in all kinds of networks and not just communication networks. Therefore, in general terms, these principles are equally understood to be at work within the broader realm of the NSA and partnering agencies' surveillance network, the Internet as well as the information technology industries that largely comprise the backbone of communication infrastructures in terms of soft- and hardware.

In their standard work *Information Rules*, Shapiro and Varian bring forward a general argument that can be used against any *discourse of newness* that seeks to present information technology and its respective industry as something new and unprecedented: While some of the products of information technology are indeed novel, the economic principles at work are not. The only decisive shift that has occurred is a general coming to the fore of network

economics in the informational age while previous industries were rather driven by economies of scale – economic principles that largely guided material choices in industrial production (Shapiro & Varian 1999, p. 173). What are these principles? In essence, these principles are *network effects* and *network economics*, *high fixed costs and low marginal costs*, *switching costs* and (*technological) lock-ins*. Network effects and externalities are two similar phenomena of crucial importance. The term *network externality* describes the fact that *the value of a network depends on the number of members connected to it, and increases with this number.* In close connection to this, *network effects* occur as *the value of a product within a network increases with the number of users or consumers of the product* (ibid. p. 174). This has to be understood as a mechanism of positive feedback: Positive results tend to produce more positive results in economic terms, and as a consequence the entities producing positive results grow, the stronger become stronger. While a negative feedback makes the weaker get stronger and the stronger get weaker, pushing towards equilibrium, positive feedback in the shape of network externalities can lead to extreme market dominance and, ultimately, monopoly structures (ibid. p. 175 f.).[4] The prevalence of monopolies in certain markets is closely connected to these feedback mechanisms: If there are a very limited number of firms competing in a certain market, the potentials of externalities are greatly enhanced and usually not all competitors survive the race. These market situations are called *tippy* as the entire market can tip in favour of one firm or the other. In its extreme, this can lead to a 'winner-take-all market in which a single firm or technology vanquishes all others' (Shapiro & Varian 1999, p. 177). IT markets therefore are particularly inclined to such feedback mechanisms as some of the products introduced to the market are indeed novel and some firms can remain with a tight grip on their products or technologies. It is important to understand that such feedback mechanisms can go both ways: If success and positive results are successfully harnessed, growth and further positive results seems to be intertwined, forming a virtuous cycle. However, in times of crisis they can form a 'vicious cycle of collapse' (ibid. p. 176).

Network externalities get further enhanced through high fixed costs and low marginal costs, switching costs and (technological) lock-ins. High fixed costs and low marginal costs describe cases where it is highly expensive to produce a product, but the reproduction (or copying) of that product is very low. IT markets abound with examples where the reproduction of a good is virtually close to zero (Cooper & Madden 2008). However, high fixed costs and low costs

[4] For more on this crucial point see Anderson 2001, p. 359 f.; 2008, pp. 216-231; 2014; Anderson & Moore 2009, p. 2719; Lelarge & Bolot 2008. In opposition to such positions, Liebowitz & Margolis (1994) argue that while network effects are indeed a pervasive feature in economies, network externalities are largely overrated.

seem to gradually move IT markets from monopolies to oligopolies, with a limited number of players with the muscle in terms of capital and positive feedback to stay in the race (Economides, 2007, p. 246). *Switching costs* are the financial burden of transitioning from one technology to the other if the technologies are mutually exclusive or not compatible. The transition of LPs to CDs is a widely known example. Switching costs therefore tend to burden both consumer and producer as consumers might refrain from making the switch if costs are too high. Lastly, *lock-ins* are situations where consumers do not have much of a choice and have to remain with a certain product or company which often enjoys a monopoly position within that market as switching to another product is either too costly or because there is no alternative around (Anderson 2001, p. 359).

A simple example for network externalities is the telephone: If nobody else uses this technology, it is rather a worthless object, its material value aside. If another person buys this technology and I can have a conversation, its value has increased. The more owners of a telephone, of the more use it is. Equally, the firm producing the telephone makes more profit the bigger the network of telephone users grows.

Furthermore and most crucially, in cases of network externalities, networks usually grow at the expense of smaller networks, especially if there is low degree of traffic between these networks, a process which is called interlining (ibid. p. 182; see also Economides 2007, p. 241). However, as Shapiro and Varian point out, players need to find allies when they want to make their network grow, unless in a situation of extreme monopoly. Finding allies usually entails concessions of some sorts, agreements, overcoming barriers, and arrival at common standards. Standards, in turn, have their own benefits, as summarised here:

> [S]tandards enhance compatibility, or interoperability, generating greater value for users by making the network larger. […] These standards fuel beneficial network externalities in two ways. First, and most directly, the standard makes it possible to share information with a larger network (without the need to convert the data from one format to another). Second, and indirectly, the enhanced ability to share data attracts still more consumers using this format, further expanding the available network externalities (Shapiro & Varian 1999, p. 229).

Why is the study of network externalities relevant to this thesis? Because in line with observations made by Ross Anderson, it seems that network economics are not only at work in the industries underlying surveillance infrastructures, but rather they are 'present and growing in the national-intelligence nexus itself' (Anderson, 2014, p. 2). As such, network externalities and monopolies are firstly exploited when certain infrastructures are used as a medium of surveillance. For instance, network externalities are largely responsible for the fact that the internet's backbone is carried by a limited number of companies, some of whom willingly facilitate surveillance. But most intriguingly, they are also at work within

surveillance infrastructures themselves which leads to the tentative hypothesis that network externalities are one of the key aspects behind the globalisation of surveillance. While Anderson observes these externalities to take effect on the technological and economical level of surveillance infrastructures, this thesis goes yet further in maintaining that they are also largely at work on an institutional level as externalities push foreign agencies to join the U.S. surveillance institutional network.

Ultimately, network externalities throughout this thesis are understood as a driving force across multiple dimensions of globalisation, not just globalisation, invoking processes of ambiguous integration and de- and reterritorialisation of (monopolised) power. It is for this reason that a close scrutiny of network externalities *within* global surveillance seems necessary in order to understand the nature of the globalisation of surveillance.

Chapter 4: Mapping NSA digital surveillance

With the previously undertaken theoretical consideration in mind, I now delve into providing a glimpse into NSA global surveillance infrastructures. The choice of examples provided here is guided by the research questions posed at the beginning of this thesis. Furthermore, the limitations to the findings of this thesis, laid out in the beginning, largely apply.

The *Snowden leaks*: A glimpse into the secret world of U.S. communications surveillance

The *Snowden leaks* provided a wealth of insights into surveillance infrastructures. As such, the *leaks* form part of a history of NSA leaks while undoubtedly constituting the biggest intelligence leak to date. Furthermore, the revealed programmes have to be understood as a continuation and advancement of programmes previously disclosed. For instance, the NSA ECHELON programme, revealed shortly before 9/11, was designed to 'capture all satellite, microwave, cellular and fiber-optic communications', and 'processe[s] this information through massive computers which search for key words or phrases, thereby drawing out particular individuals and messages for special attention' (Haggerty & Gazso 2005, p. 182; see also Murakami Wood & Wright 2015, p. 133). And yet, the insights into the different programmes provided by the leaks remain staggering. To provide but a few: The NSA PRISM programme provides access to the servers of U.S. Internet giants like *Google*, *Facebook*, *Apple Inc.* and others, while BOUNDLESS INFORMANT categorizes and maps data intercepted from computer and telephone networks (Greenwald & MacAskill 2013a, 2013b); WELLSPRING collects images from emails for facial recognition (Propublica 2014; unless noted otherwise, all following programmes are taken from this source; see also Landau 2013,

2014); DISHFIRE collects more than 200 million text messages globally; QUANTUMTHEORY injects spyware onto targeted computers; SMURF programmes grant access to Smartphone data, cameras, microphones and power management; BULLRUN (NSA and GCHQ) aims at undermining cryptography standards and tools; the joint GCHQ and NSA project MUSCULAR allows for the breaking into data centres of Internet giants (Gellman & Soltani 2013); EGOTISTICALGOAT/GIRAFFE tracks TOR users; lastly, TURMOIL is a network of surveillance sensors planted globally and in outer space to collect data from cables and satellites and collect micro-wave communications.

Such technological elaborateness is apparently matched by ambition. Surveillance and spying activities, besides the bulk collection of communications data including metadata and content, have been extended to the interception of the communication of entire countries (Devereaux et al. 2014); the involvement in targeted killing operations (Miller et al. 2013); economic spying; surveillance of UN conferences; hacking news outlets' central servers; breaking into university networks globally, including American universities; the targeted spying on American minorities and, lastly the NSA's involvement in interrogations occurring at Guantánamo Bay (Currier 2016; see Lee & Williams 2016).

What emerges from the *Snowden leaks* is a global infrastructure of surveillance, the legality of which seems based on loose footing (Austin 2015), that extends beyond surveillance exercised by state actors alone and is not limited to the surveillance of foreign states and its leaders, but has broadened its scope to the general public of domestic and foreign societies. Most relevant to the interest of this thesis, the *Snowden leaks* shed light on ways surveillance has been globalised. These ways can best be understood by a close scrutiny of the programmes functioning as the media through which surveillance is exercised, and by studying the way the different layers of Internet communication have been penetrated. As Keiber convincingly argues, '[w]ithout knowing more about the NSA programs, it is hard to know to what extent the U.S. is strong arming states into partnerships' (Keiber 2015, p. 175), and thus to what extend the globalisation of surveillance has been driven forward.

Excursus: The geography of the Internet, a network of networks

While the chapters on networkshave already provided insight into the theoretical functionality of the Internet as well as its key technological aspects, this chapter briefly turns to the geographical architecture of the Internet, which provides the background against which the mapping of U.S. surveillance infrastructures will occur.

The Internet has to be understood, on the one hand, as a computational network – or more accurately as 'a loosely coupled collection of independently managed networks. However, at

its core there are a few very large networks, each of which strives to be as efficient as possible both internally and in its connections to other networks' (Hall et al. 2011, p. 9). This allows for global flows of data and all kinds of traffic, regulated by protocols as the organizing mechanisms in the digital sphere. However, the Internet equally comprises a *spatial* and *material* dimension. This is the realm of hardware, servers, fibre optic cables, underwater cables, etc., operated by Internet service providers, telecommunication companies, private and semi-private actors. Of particular interest here are those components that form the material and geographical architecture of the Internet. Most broadly, the Internet is also 'fundamentally tied [to] physical places and the people [,] who create, regulate, distribute, and consume its data' (Zook 2009, p. 556). The material reality forms its own kind of network that exhibits particularities in stark contrast to the distributed network logic of the Internet.

The physical network of the Internet is essentially divided into different segments owned by different service providers competing and collaborating in a global capitalist market (Yong et al. 2006, p. 776). These service providers are hierarchically organized into different tiers. The first tier comprises the Internet Backbone Providers (IBPs) who mainly provide the long-haul fibre optic cables which constitute the material infrastructure of the internet (Tranos & Gillespie 2011). The IBPs are globally interconnected and therefore generally do not have to purchase IP transit to reach certain routes as mutual peering agreements allow different IBPs to make use of each other's infrastructure. Mutual agreements and pricing contracts usually are based on common interests, such as wide reaching geographical network coverage, as well as improved network utilization and capacity (Yong et al. 2006, p. 785). In the past the bulk of internet traffic was routed through the infrastructures provided by these global players.

The second tier is formed by the Internet Service Providers (ISPs) which essentially provide network access to individuals and institutions. Tier 3 is largely comprised of contend delivery networks and contend providers (such as *Facebook*) that traditionally had to buy transit from providers of the other two tiers. Tier 2 providers usually possess both peering and transit connections and are, again, interconnected. The recent years have seen an explosion of peering agreements between ISPs and between tier 2 and tier 3. This has led to a general shift in traffic routing within the Internet as the second and third tier now carry the bulk of Internet traffic while tier 1 still has a strong grip on the material infrastructure of the Internet and allocates access to certain networks based on transit agreements which tier 2 or tier 3 providers have to pay for (Krogfoss et al. 2012, p. 164 f.). Over the past decade, the complex geography of the Internet has been further enhanced by the rise of capital intensive multi-national contend providers' ability to uphold hundreds of peering agreements, effectively

allowing them to partially avoid the services of IBPs. As a consequence, the geography of the Internet has to be understood as highly diffuse, complex and also largely unregulated (ibid. p. 169 f.; Malecki 2002, p. 400). This can be interpreted in light of Leigh Star and Bowker's understanding of infrastructure which emphasises that infrastructures are never built de-novo but rather develop out of preexisting infrastructural arrangements. As such, the global infrastructure of the Internet is largely built upon preexisting market structures within communication industries and, geographically, exhibits externalities towards urban areas which traditionally are better connected within commnunication networks than peripheral areas:

> A city that gained a high connectivity early on is more likely to become a hub than a city that gained little connectivity early on, *ceteris paribus*. This can be understood from preferential attachment: new cities entering an infrastructure network will prefer to create links with nodes that are already well connected, in order to profit from transfer opportunities (Vinciguerra et al. 2010, p. 1971, emphasis in original).

Several aspects of this complex geography are of importance with regard to this thesis: Firstly, this geography does not at all correspond to the organizing logic of the Internet as a distributed network, and the way the Internet is spatialised seems to coincide with the emergence of global cities as central hubs in a globalising world economy (Kallus et al. 2011, p. 1063 ff.; Malecki 2002; see also Vinciguerra et al. 2010, p. 1970 ff). Cities mostly are where ISPs are headquartered and where their infrastructures amalgamate; they function as Internet Exchange Points (IXPs). Metropolitan areas play a pivotal role as metropolitan access exchange (MAE) points of IBPs and function as central nodes and switching points. This reflects the 'essentially urban character of the Internet' which, after all, is a predominantly private infrastructure that coincides with consumer demands (Tranos & Gillespie 2011, p. 36).[5]

Secondly, this entails a particular urban-centred global geography of the Internet which cannot be scrutinized here but which evinces broader societal shifts that correspond to the previously visited aspects of the first layer of spaces of flows. A most brief look at this geography reveals the pivotal role global cities such as New York, Los Angeles, Chicago, Dallas, Washington D.C. and San Francisco play in the U.S. and Amsterdam, London and Frankfurt play in Europe. Concerning the function as hubs for undersea cables, Los Angeles, Miami and New York have to be understood as the central landfall nodes (Lindemann 2013).

[5] See Lee 2014 for numerous maps reflecting the way the urban character of the Internet emerged historically.

However, this geography diverges slightly from a *general geography of global cities in a globalized economy*, as with their central role as IXPs Frankfurt and Amsterdam have a far greater significance for the European Internet *backbone* geography than Paris or Brussels, for instance. This points to the notion that in the context of spaces of flows, it seems more important *what flows through* a city than what is contained *within* the city (Tranous & Gillespie 2011, pp. 38-41). While the network typology proposed by Baran (Figure 1) clearly falls short to grasp the complex global geography of the Internet's infrastructure in its entirety, the notion of the Internet backbone consisting of central hubs and spokes and peripheries nonetheless seems reminiscent of the decentralised network structure.

Lastly, with regard to the surveillance of Internet traffic, the complex geography of the Internet leads to the hypothesis that this complexity will be matched by complex U.S. surveillance infrastructures tapping into these different material realities, thus effectively tightening its grip on the spatialities of the global flows of the Internet.

Different layers of U.S. surveillance

In trying to map NSA surveillance infrastructures, I choose a conceptualisation of the Internet as an infrastructure that comprises different layers, namely the physical and the protocological layers, and the layer comprised of global flows. The latter epitomises what Haggerty and Ericson (2000, p. 606, quotation marks mine) see as the basic operation of the *surveillant assemblage*, namely the abstraction of 'human bodies from their territorial settings [and] separat[ion] [...] into a series of discrete flows' to be 'reassembled into distinct "data doubles"'. It is important to understand these layers as nested: As with the different protocological layers of the Internet, one layer is embedded in the next layer. Penetrating the physical layer of the Internet grants the NSA and partnering agencies access to the protocological layers, the exploitation of which is key in the mapping of global data flows. This conceptualisation doubtlessly presents a simplification which serves to make the infrastructure of NSA surveillance graspable. And yet, it is closely oriented at the way the NSA conceptualises its mission to penetrate the different layers the Internet is comprised of (see below Figure 4).

Penetrating physical layers

The NSA and its partner agencies have managed to deeply penetrate the physical layers of the Internet and global communication infrastructures more generally. Doubtlessly, tapping into physical layers has a long history and the recent exposures have to be seen in the light of such. In recent history, the tapping of fibre-optic cables at an AT&T facility in San Francisco made global headlines as the NSA had successfully implanted devices duplicating domestic

and global Internet traffic flowing through AT&T cables. Most importantly, the interception of data took place under AT&T's cooperation as the company had provided facilities ('Room 641A') at which interception devices were installed as well as senior technical personnel overseeing the process (Electronic Frontier Foundation 2006). As Mark Klein, the AT&T whistleblower who revealed this process put it (quoted by Fichtner 2014, p. 67):

> So they took 16 high-speed peering links which go to places like Qwest [Communications] and Palo Alto Internet Exchange [PAIX] and places like that [...] so that they can get the data flow from these circuits to go to the secret room. So this data flow meant that they were getting not only AT&T customers' data flow; they were getting everybody else's data flow, whoever else might happen to be communicating into the AT&T network from other networks.

The NSA docked its interception device in close proximity to a key IXP in North America, thus gaining access to a key node of the Internet's backbone layer. This seems in line with a pattern of NSA 'interception stations in strategic locations' (Murakami Wood 2012, p. 338) in the USA and abroad that routinely involves a number of parties such as other government agencies or commercial enterprises, i.e. IBPs and ISPs. Such interception cooperation serves to successfully exploit the particularities of the Internet backbone infrastructure which is closely linked to the economics of Internet and communication providers (Anderson 2014, p. 2). The aforementioned network externalities have led to monopoly structures that find their material reality in the shape of a decentralised Internet backbone geography that consist of central hubs and connecting links. This geography provides ample opportunities for a network of interception sites located at central hubs, with IXPs constituting key targets for interception schemes (schematically depicted in Figure 3).

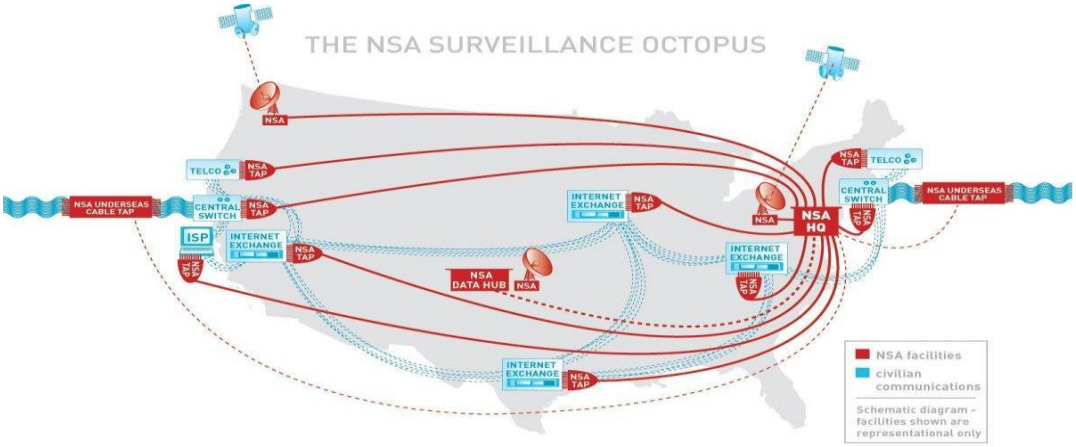


Figure 3: NSA interception sites at IXPs

I argue that the exploitation of the monopolistic infrastructures of the Internet backbone provide the NSA with *both horizontal and vertical access* to global flows of data on the

physical layer of the Internet. *Horizontal* in the sense that the interception sites are just as spread across land and sea – forming their own geography – as are IXPs as the Internet backbone's central hubs. *Vertical* in the sense that interception sites located at IXPs provide the NSA with ability to penetrate global flows of communication most deeply, providing access to metadata and content of communication data.

The *Snowden leaks* have further provided ample proof for the way the penetration of the physical layers of the Internet occurs on a *global* scale. A first example for this process constitutes NSA programme RAMPART-A which 'depends on the participation of a growing network of intelligence agencies', of so-called *third-party partners*, that grant the NSA access to their fibre-optic cables. As the article disclosing RAMPART-A (Gallagher 2014, quotation marks in original) explains:

> The NSA documents state that under RAMPART-A, foreign partners "provide access to cables and host U.S. equipment." This allows the agency to covertly tap into "congestion points around the world" where it says it can intercept the content of phone calls, faxes, e-mails, internet[sic] chats, data from virtual private networks, and calls made using Voice over IP software like Skype.

Part of the motivation for states participating in the NSA penetration of the physical layer of the Internet lies in the access to NSA surveillance infrastructure: 'governments that participate in RAMPART-A get something in return: access to the NSA's sophisticated surveillance equipment, so they too can spy on the mass of data that flows in and out of their territory' (ibid.). However, a number of RAMPART-A operations are also run without the explicit knowledge of the concerned *third-party partner*. Yet, some of the *third-party partners* willingly and aggressively cooperate. For instance, it has been reported that the German BND, itself an intelligence agency meant to collect *foreign* intelligence, tapped into one of the largest Internet hubs in Europe, the Frankfurt DE-CIX, while the BND's Swedish counterpart assisted NSA interception of cables connecting Baltic countries and Russia (Bauman et al. 2014, p. 122; Rensfeldt 2013). Emanating from the practice of intercepting Internet traffic at key nodes is the fact that the geography of such nodes and cables connecting them 'gives political advantages to some countries and may reconfigure power politics at the world scale' (Bauman et al. 2014, p. 124) and furthermore evinces the complex geography of globalising surveillance.

NSA UPSTREAM and GCHQ TEMPORA are understood to be the programmes undertaking the largest undersea interception activities for the respective agencies. UPSTREAM is a collection of programmes that intercept more than 160 billion records (metadata and content) per month (King 2015, p. 13). There are two key strategic interception sites that make the

interception of undersea cables most promising: The regeneration points 'where their[the cables'] signals are amplified and pushed forward on their long, circuitous journeys' and cables are laid out individually, rather than bundled, which makes tapping more easy. Secondly, there are sites where cables make landfall (Khazan 2013). Both interception methods again rely on previously encountered *splinter* technologies that allow for the interception and duplication of data flows without inhibiting the flow of information. As has been reported, analysts using UPSTREAM are schooled to correlate data acquired by UPSTREAM with data stemming from the PRISM system, thus allowing the NSA to bring together two entirely different technologies.

Another programme revealed by the *Snowden leaks* is the GCHQ-run TEMPORA. Data intercepted with this programme is generously shared with the NSA and further partnering agencies. Non-British agencies largely rely on TEMPORA operating under a very 'light oversight regime' as one allegedly leaked GCHQ file states (MacAskill et at. 2014). GCHQ is believed to have placed more than 200 sensors intercepting Internet traffic and retaining metadata for a predefined period of time at key locations. Interception, once again, occurs in the shape of splitter devices that duplicate the data flowing through fibre-optic cables (Bauman et al. 2014, p. 122 f. See also van der Velden 2015, p. 190). The programme presents itself as the biggest programme of its kind, and indeed, if accurate, its numbers point to unprecedented interception capacities (King 2015, p. 7):

> Indeed, the vast number of private communications being intercepted requires a special kind of processing, known as 'Massive Volume Reduction' to make sense of the collected private communications. In 2009, internal GCHQ documents stated 'this massive site uses over 1000 machines to process and make available to analysts more than 40 billion piece of content a day.'

Yet, the unprecedented amount of data intercepted with TEMPORA entails that not all of the data can be retained for a longer period of time. A big chunk of content is therefore disposed of after a certain period of time defined by the value of the gathered intelligence. Furthermore, the data processing centres are spread across the UK and overseas, usually in close proximity to interception sites (ibid.).

What emerges from the closer look at the interception of undersea cables is, once again, a highly diverse geography of interception sites that partially coincides with the importance of global cities in the context of processes glocalisation, but in some circumstances starkly differs from established city-centred accounts of glocalisation. Given the importance of programmes such as TEMPORA to global surveillance networks, key interception sites can form pivotal nodes in such networks even if their material reality consists of operations of

limited size. For instance, the interception of undersea cables has largely been facilitated by splinter technology which served to both enhance the effectiveness of such operations and at the same time reduce their size (see Khazan 2013). Furthermore, the NSA seems to hold a hegemonic position in the access to the physical infrastructure of the Internet. Entailed in this hegemony is the fact that struggles over surveillance and digital civil liberties primarily unfold on the protocological level of the Internet and not on the physical one where NSA preponderance is largely unquestioned.

Penetrating protocological layers

The *Snowden leaks* provide us with a wealth of insights into the ways the NSA manages to penetrate the protocological layer of the Internet. It would be impossible to reproduce a detailed account of the different ways and different programmes serving protocological exploitation the NSA has come up with given the mass of published information on these programmes. Instead, I demonstrate the principle forms of protocological control and exploitation the different surveillance programmes routinely rely on.

The first crucial aspect of the penetration of the protocological Internet layers is that based on the organising logic of the distributed network and the functionality of protocological control: Protocological intrusion into the network of the Internet is possible almost everywhere (see chapter *Protocological control*). In the distributed network data packets are routed between nodes until they reach their final destination where data packets are reassembled into the original message. As explained previously, the route of the data packet travelling through the network is determined at the nodes from where it can be sent to any other functioning node in the network. For instance, if data packet p_1 travels from node n_1 to n_x via nodes n_2, n_3, n_4 the individual route is determined anew at each node $n_{1\text{-}4}$. The '*1-4*' serves as a temporal marker and does not entail that p_1 necessarily needs to travel from n_1 to n_4 in the given order. At each node the future route of p_1 is (re-)determined. The decisive point here is that for the future route of the packet being decided upon, transmission of each packet is shortly interrupted at each node, for the fraction of a millisecond. This moment of interruption suffices for numerous technologies to access the packet and read header and content, Deep Packet Inspection (DPI) being the most prevalent of these technologies (Sprenger 2015, p. 48 f.).

DeNardis (2012 p. 725) frames DPI as a *hidden lever of Internet control*: On the one hand, DPI can be used for network maintenance purposes. On the other hand, DPI technologies can be exploited for a number of purposes ranging from advertising to copyright enforcement, censorship and surveillance. As the name suggests, DPI allows for the inspection of data packets passing through nodes, and the inspection goes beyond the mere header of the packet

as the payload – the part of the packet that contains the actual content – and other layers of the packet can be read and analysed. Beyond network maintenance, DPI can also ensure the steadiness of volume intensive flows. For instance, DPI allows for the prioritisation of packets at the nodes. Thus, if certain applications require a steady flow of many small data packets, such as video or voice-over-IP, DPI allows for the prioritisation of these many small packets so that a steady flow is ensured as these data intensive technologies require a steady and rapid flow and are sensitive to any interruption or slowdown (Sprenger 2015, pp. 48-50).

On the protocological level, the previously encountered TCP/IP protocols are key to DPI: This family of protocols ensures the transmission of data packets as it maps the different transmission dimensions of the Open-Systems Interconnection (OSI) network – the data transmission network of the Internet – into the different layers previously encountered: the nested application-, transport-, Internet- and link layers (see Fuchs 2013, p. 1331. Fuchs' conception consists of five instead of four TCP/IP layers, while I continue to refer to Galloway 2004 for the conception of four layers). There, TCP/IP operates and oversees the transmission of data across the different protocological layers. The TCP/IP data packet in principle consists of three layers: Firstly, the *IP header*, defined at the Internet (network) TCP/IP layer, contains the destination IP in total length. Secondly, the *TCP/IP header*, defined on the transport layers, contains the destination port and sequence number. By reading these two layers, TCP/IP determines how and to where to route the data packet. The third layer is the aforementioned *payload* which contains application data (content such as email text, images, voice and video content) and the application header containing information such as the application programme version, addresses of email senders and receivers, etc. (ibid. p. 1334). In a nutshell, DPI is 'the collection, observation, analysis, and/or storage of data related to an application that is found in Internet packets above OSI layer 3 [here the Internet (network) layer]' (Cooper, quoted ibid. p. 1333). DPI allows the respective network operator to scan the data packet in real time and possibly discriminate among packets according to their payload (ibid.) which stands in stark contrast to the anarchically distributive logic of the distributive network.

Sprenger argues that DPI can be understood as the most important protocological instrument of the NSA surveillance arsenal (2015, p. 49). DPI has found such widespread use that hardware suppliers now routinely sell equipment with in-built DPI technology forming an integral part of the Internet infrastructure – and the key tool in protocological control and surveillance, be it at the nodes of IXPs or within NSA operated data processing centres where

duplicated flows of data are routed to (Sprenger 2015, pp. 49-52, see also Fuchs 2013, p. 3144 f. on the security-industrial complex that provides DPI technology to ever-increasing profits).
In its characteristic not to differentiate between sensitive and non-sensitive content (Fuchs 2013, p. 1342), DPI is central to NSA surveillance infrastructures, but there are other similar technologies that further enhance NSA capabilities of penetrating the protocological layer of the Internet: *Stochastic Packet Inspection* allows for the statistical analysis of Internet traffic based on size and number of data packets, making it possible to determine the type of content wrapped in the data packet. This technology can further be made use for the *deliberate deactivation of ports and nodes* in the network when the route of travelling packets is to be influenced to the degree where data packets can be rerouted to specific nodes (Sprenger 2015, p. 49 f). The most notorious NSA protocological exploitation emanating from the *Snowden leaks* however seems to be what the NSA dubbed *Deep Packet Injection*: As packets' journeys are shortly interrupted at network nodes data is inserted into the whole packet or just the header or payload. This technique is markedly different from DPI for it does not serve the surveillance of content, but the active insertion of data in order to either obtain information or install malicious software (van der Velden 2015, p. 186). One example of this is NSA programme TURBINE: Based on *Der Spiegel* reporting, van der Velden (ibid.) explains that with TURBINE the NSA

> uses software to fake and insert a website, thereby diverging the URL-request to a server that is owned by the NSA (FoxAcid), located at key internet switching points. This only works when the server of the NSA is faster than the server that hosts the website that was originally requested, therefore these machines are also referred to as 'Race Servers'. If the intervention succeeds and the person loads data from the fake server, malware can be installed on his or her computer.

Programmes like TURBINE doubtlessly can be deployed in numerous contexts, not just surveillance, such as electronic warfare, economic spying, etc. Further insertion technologies deployed by the NSA include the *insertion of vulnerabilities*; *further malware injection programmes* that, for instance, intrude into networks by exploiting system admin access points; and *repurposing of web objects* and automated uses of injected malware as *platforms for further malware* (ibid. p. 188; see also Gallagher & Greenwald 2014a). What all these programmes have in common, I argue, is an underlying coalescence of Internet infrastructures with surveillance infrastructures: Through the former, the latter can exist. Yet again, the geographical reach of protocological exploitation is global and built upon (but not limited to) the NSA access points to the physical layer of the Internet.
As described in the introduction to this main chapter, I understand the different Internet layers penetrated by NSA surveillance to be *nested*. This entails that surveillance operates through

the different layers and is enabled from one layer down to the next. For example, protocological exploitation is enabled *qua* penetration of the Internet physical infrastructures. A close look at XKEYSCORE, another notorious programme revealed by the *Snowden leaks*, serves to illustrate this nesting of layers. XKEYSCORE, often dubbed the most evasive and broad-sweeping NSA programme, comprises a network of over 700 servers located at more than 150 field sites in the U.S. and countries all over the globe. Most crucially, XKEYSCORE is largely fed with constant flows of data acquired by the tapping of fibre-optic cables that are part of the backbone of the Internet (Marquis-Boire et al. 2015). XKEYSCORE serves the bulk-collection of communication data and other sets of information with the volume of data intercepted so vast that data is processed and analysed locally. In other words, XKEYSCORE sweeps up so much data that retaining the data for longer periods or relating the raw data back to the U.S. would neither make sense from an intelligence perspective nor would it be technologically feasible without overloading NSA infrastructures. Through XKEYSCORE analysts can intercept Internet traffic in real-time and filter it based on all kinds of selectors, such as email addresses, physical addresses provided on websites, telephone numbers, names, IP addresses as well as metadata (Greenwald 2013b). Once again, such filtering mechanisms are necessary, for else analysts would be overwhelmed with the sheer quantities of intercepted data. NSA files allegedly leaked by whistleblower Snowden detail how XKEYSCORE 'extracts and tags metadata and content from the raw data so that analysts can easily search it' which 'is done by using dictionaries of rules called *appIDs*, *fingerprints* and *microplugins* that are written in a custom programming language (Lee et al. 2015, emphasis mine). Whenever new traffic flows into XKEYSCORE, it is run against these parameters. As Lee et al. (ibid.) explain:

> AppIDs are used to identify the protocol of traffic being intercepted, while fingerprints detect a specific type of content. Each intercepted stream of traffic gets assigned up to one appID and any number of fingerprints. You can think of appIDs as categories and fingerprints as tags.
> [...]
> To tie it all together, when an Arabic speaker logs into a Yahoo email address, XKEYSCORE will store "mail/yahoo/login" as the associated appID. This stream of traffic will match the "mail/arabic" fingerprint (denoting language settings), as well as the "mail/yahoo/ymbm" fingerprint (which detects Yahoo browser cookies)."

On the one hand, this technology largely reduced the amount of work to be done by analysts. The interface of XKEYSCORE, conveniently accessible with standard web browsers such as *Firefox*, resembles conventional search engines and analysts can choose parameters in simple drop-down menus. XKEYSCORE search queries, for instance, can show activities of users based on browsing behaviour, nationality and location (as indicated above). Other examples

include the efficient mining of social media data. One the other hand, XKEYSCORE allows for a number of operations that go beyond mere surveillance, such as the assessment of the exploitability of targets based on their browser fingerprint and operating systems version (Marquis-Boire et al. 2015). Or else '[i]n addition to login credentials and other target intelligence, XKEYSCORE collects router configuration information, which it shares with Tailored Access Operations', a subdivision of the NSA that engages in malware injection operations and electronic warfare (ibid.). All this doubtlessly makes XKEYSCORE one of the most powerful NSA programmes and evinces the interplay of protocological exploitation and the penetration of physical Internet infrastructures.

Mapping global flows: TREASUREMAP

TREASUREMAP is another programme that merits the adjective *powerful*. In an effort to grasp global flows of information, TREASUREMAP intercepts all kinds of data. Leaked NSA documents provide the details: Intercepted with TREASUREMAP are, amongst others, IP- and router addresses, DNS, MAC addresses, numbers of autonomous systems, as well as further metadata and content. Registries include network information and details on network ownership. Operating System (OS) fingerprints include software- and system characteristics unique to any kind of device. Matching DNS to IP reveals user behaviour and network access, as well as geo-location of IPs and of IP accessing patterns (NSA, undated document). Apparently, the TREASUREMAP software can be installed on any kind of device that has access to the Five Eyes networks (ibid.). I suggest that this programme can be seen as a combination of aforementioned programmes and their *operating logic* as TREASUREMAP penetrates the Internet on its different aforementioned layers namely the application-, transport-, Internet- and link layer (see Figure 2) (NSA, undated document). While programmes like XKEYSCORE work mainly through protocological exploitation of Internet infrastructure, and programmes such as UPSTREAM and British TEMPORA exploit the Internet's physical geography, TREASUREMAP does both – and more. Leaked documents include detailed graphics of physical networks and their providers. For instance, the NSA has managed to penetrate the cable infrastructure of German IBPs such as Deutsche Telekom AG, a globally operating tier1 IBP, and even local IBPs such as Netcologne. The latter case is highly interesting as the NSA must have found an access point *within a local network*, and not via aforementioned key interception sites such as IXPs or undersea fibre-optic cables (Müller-Maguhn et al. 2014). Another document details how the NSA in collaboration with GCHQ uses TREASUREMAP to list key staff of IBPs, from senior management to, most importantly, network maintenance engineers, making the latter join the group of alleged

terrorists and political leaders as the most valuable targets of NSA surveillance in terms of SIGINT (ibid.). The surveillance of admins grants the NSA further access to the organising logic and infrastructure of networks of IBPs, which proves a key asset in the surveillance of flows of data. In contrast to the case elaborated above where AT&T consciously cooperated with NSA surveillance efforts, the network providers in this case seemed unaware of the NSA intrusion into their infrastructure. What's more, the intrusion into local networks allows for more than just surveillance, as Internet traffic may be rerouted or cut off on a large scale through network manipulation, while the intrusion could also be exploited for cyber-warfare purposes.

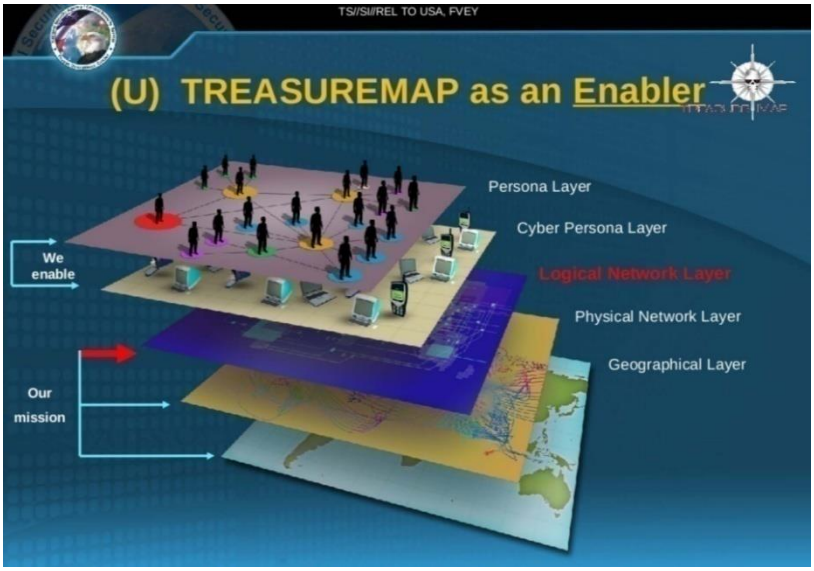


Figure 4: the operating logic of TREASUREMAP

However, the documents suggest that the real purpose of TREASUREMAP lies somewhere else: It allows analysts to 'correlate IP addresses with country, latitude, and longitude', and furthermore grants access not only to the content of global flows, but also to the different parties that have a stake in the concerned flows, stretching all the ways from network providers, to peering ISPs, to hosts of servers, and, ultimately, the devices of individual users and network customers. In other words, TREASUREMAP brings together the physical location of Internet use with its protocological translation and the users of the Internet and their devices (NSA, undated document). In a nutshell, it allows for the correlation of Internet use, Internet users and the infrastructure involved in all its facets. Figure 4 demonstrates the way the NSA conceptualises TREASUREMAP: The programme enables a visualisation of the users of the Internet and the infrastructure they use, and the way they are related to each other. As such, TREASUREMAPS seeks to serve as a *near-real-time interactive map of the Internet*, visualising intercepted global flows of data (ibid.). As put by Müller-Maguhn et al. (2014), TREASUREMAP presents a

> mandate for a massive raid on the digital world. It aims to map the Internet, and not just the large traffic channels, such as telecommunications cables. It also seeks to identify the devices

> across which our data flows [...].One can imagine it as a kind of Google Earth for global data traffic, a bird's eye view of the planet's digital arteries.

TREASUREMAP is the visualisation of global surveillance driven to its extreme. The particularities of the maps called into existence by TREASUREMAP speak to what is being explored, and, as every map, also visualises future points of entry into the realm of global flows, as it will also bring to the fore uncharted territory. At the same time TREASUREMAP serves to visualise the movement and way of life of individual subjects and the way and with whom these subjects communicate. Figure 4 not only illustrates the way surveillance penetrates human life, but it also helps understand why the quoted NSA document states that *the whole is better than the sum of its parts* (NSA, undated document). TREASUREMAP not only enables the surveillance of the individual subject but also equips analysts with the capacity to *see the bigger picture.* To my understanding, TREASUREMAP epitomises NSA's and collaborating agencies' efforts to grasp the Internet in its entirety and also presents the different pillars the globalisation of surveillance is built upon: The penetration of global digital and physical network infrastructures, based on the collaboration of network providers or the exploitation of their infrastructures, the collaboration of several partnering agencies; the drawing together of different interception logics and functionalities, i.e. the nested physical and protocological penetration of global flows of information; and lastly, technological capabilities that elude the agencies' original mandate of *surveillance* for intelligence purposes.

Beyond 'Five Eyes'

The collaboration of different partnering agencies in global surveillance has been a reoccurring theme so far and deserves extra scrutiny. Emanating from the analysis of U.S. surveillance infrastructure so far is a complex global surveillance geography that can only be sustained under the collaboration of a number of foreign agencies and commercial partners worldwide. Categorising the partnerships the NSA maintains can be arduous, for the complexities of such cooperation efforts produce an at times paradox picture of institutional and commercial collaboration. For instance, the NSA can collaborate with a certain country on a number of levels, providing this country with surveillance technologies and enhanced surveillance capabilities and receiving a lot of intelligence and access to communication networks in exchange, and still largely exclude this country from key NSA surveillance strategies, partnerships and capabilities. It appears that the degree of collaboration with foreign partners is as much a matter of historical alignments as of strategic value, geo-political significance, foreign willingness to cooperate and ultimately the feasibility of the

partnership under given technological and socio-political conditions. Based on the logic of surveillance hegemony explored in the theoretical chapter, one can assume that the NSA partnerships are ultimately governed by the interest of the surveillance hegemon and will mostly be guided along this rationale. As the NSA puts it: 'We establish foreign partnerships to satisfy U.S. intelligence requirements', and: 'we can only move our SIGINT relationships forward [,] when U.S. requirements intersect with theirs[the partners']' (Appendix 1: Third Party Relationships). The functionality of such partnership therefore heavily relies on the projection of surveillance infrastructure into the surveillance apparatus of other states or the technological infrastructure of commercial entities. Furthermore, based on the theoretical framework it is assumed that such partnerships are held together by a common broadly applicable narrative, presumably counter-terrorism as a *raison d'être* of surveillance, embedded in an institutional environment replete with incentives to further the cooperation and take the shape of shared or synaptic partnerships. Ultimately, as implied in the term *partnership*, these collaborations are likely to occur under the absence of direct U.S. coercion of *partnering* agencies. This points to the notion that the collaboration between partnering agencies is markedly different from the collaboration of commercial partners that at times have to be legally forced into cooperation. For this reason the collaboration with commercial entities will be scrutinised separately.

Despite their heterogeneity, NSA collaboration with other entities can broadly be put in the following categories (the following typology is inspired by Greenwald 2014a, pp. 118-126): Firstly, there is the aforementioned differentiation between collaborations with commercial entities and with foreign agencies or supranational institutions. The latter, from the perspective of the NSA, can be categorised in the shape of different tiers. The first tier is comprised of the Five-Eyes countries, the historic intelligence cooperation agreements between the U.S., Canada, New Zealand, Australia and the UK that dates back to the early days of the Cold War (Walsh & Miller 2016, p. 349). The second tier comprises *focused cooperation* partners. These partners can include both so-called *coalitions* such as NATO or the EU, as well as individual states and their respective institutions. One allegedly leaked NSA file names Austria, Belgium, Czech Republic, Denmark, Germany, Greece and Hungary as European second tier partners, while a global list would surely include Israel given the NSA's close cooperation with Israeli partnering agencies (Greenwald 2014, pp. 118-126). Another leaked file however suggests that the list of *focused operation* partners may indeed be longer. What is particular to these partnerships is that these partners have some more or less limited cooperation with the NSA but are also targets of NSA spying. The third tier

relationships are what I will call *sporadic cooperation*, as the cooperation with these states is restricted and often limited to individual operations that necessitate access to the geo-political location or intelligence of the respective partner. Likely candidates for this tier are, amongst others, countries such as India, Pakistan, Saudi Arabia, as well as numerous European countries such as Croatia, Portugal and the Netherlands (Greenwald 2014, pp. 118-126). The following chapters will analyse the nature of these different partnerships more thoroughly.

The 'Five Eyes'

The 'Five Eyes' collaboration doubtlessly has to be seen as the most powerful intelligence collaboration in the context of global surveillance infrastructures. Its roots lie in the longstanding and intense cooperation between NSA and GCHQ that can be traced back to 1946 when a series of bilateral agreements laid the foundation for what was to become the *Five Eyes*. Most broadly, the purpose of these agreements, to which Australia, Canada and New Zealand were soon added, lay in the sharing of intelligence and the implementation of joint intelligence operations (King 2015, p. 11 f.). However, the degree of collaboration and intelligence sharing was largely expanded at the outset of the Cold War and has remained very high ever since (Walsh & Miller 2016). As a matter of fact, the countries collaborating under this coalition *routinely grant each other access to the intelligence acquired, the data intercepted and the technologies deployed.* Furthermore, they cooperate in the surveillance of certain targets – for example, partnering country p_1 can approach partnering country p_2 and ask for their assistance in the surveillance of target t_x. Furthermore, partnering countries can ask for assistance of the surveillance of n targets t_n, effectively asking for the assistance in the surveillance of groups of targets or entire populations.[6] While the degree to which partnering country p_1 gets to *systematically operate* the technologies of partnering country p_2 does not seem to be unilateral and appears a matter of individual agreements, I would argue that the possibility to ask another country to direct its technologies on presented targets and generously share the acquired intelligence is a form of *indirectly operating* the technology of a partnering country under the condition of the intense cooperation and intelligence sharing of the *Five Eyes* countries. Documents allegedly leaked by whistleblower Snowden studied for the purpose of this thesis routinely carry headers such as 'TOP SECRET [...] REL[ATE] TO USA AUS CAN GBR NZL' (Appendix 1: Third Party Relationships) or 'REL FV EY[relate to *Five Eyes*]' (NSA undated) which allows for the interference to the apparent ease and

[6] An example for this is the NSA receiving an approach from its Australian counterpart asking for assistance in the surveillance of Australian citizens, allegedly for counter-terrorism purposes (Greenwald 2014, p. 122).

widespread implementation of intelligence sharing the NSA and its partnering agencies engage in. However, Bauman et al. (2014, p. 127) point to the fact that there have also been allegedly leaked files with a classification header declaring 'not for British eyes', an observation which points to the fact that *even within the Five Eyes* there exists distrust and partnering countries engage in surveillance activities that might be opposed to the interests of their partnering agencies.

And yet, cooperation and intelligence sharing remain widespread among the *Five Eyes* countries. As former NSA deputy director John Inglis describes, intelligence is carried out 'in a combined way—essentially [to] make sure that we[the *Five Eyes* countries] leverage one another's capabilities for mutual benefit' (John Inglis, quoted in Greenwald 2014a, p. 118). The example of GCHQ run TEMPORA seems a case in point, where one of the partnering agencies runs one of the broadest surveillance programmes while granting the partnering agencies broad access to the technicalities of and intelligence produced by this programme. However, the *Five Eyes* collaboration doubtlessly is not just about a mutual leveraging of capabilities. Beyond the granting of direct or indirect access to surveillance technologies, the partnering countries routinely engage in information sharing, be it by providing particular information on given targets, or by granting the partnering countries access to databases (Keiber 2015, p. 175 ff.). This enables further cooperation and grants access to possibly new intelligence. Furthermore, relying on partnering countries' infrastructure is also a matter of efficiency, as the collaboration between the partnering agencies has been extended with another crucial function: The minimisation of SIGINT duplication and the division of tasks (King 2015, p. 12). From a NSA perspective, setting up expensive surveillance infrastructure where partnering agencies produce valuable and unfiltered results has to be seen as a waste of resources. It therefore appears that the different *Five Eyes* agencies are engaging in a global division of tasks in surveillance matters, feeding each other's databanks and surveillance operations with intelligence while maintaining a mutual reduction of costs that seems to be to the benefit of all the partnering countries (see King 2015).

Lastly, another integral part of the *Five Eyes* agreements (and beyond) is what on other occasions has been referred to as *jurisdiction shopping* (Palan 2002; Gammeltoft-Hansen 2010). Jurisdiction shopping describes the process when states gain access to the jurisdiction of other states by means of outsourcing, externalisation or relegation of actions and processes prohibited under their own jurisdiction. The TEMPORA case example elaborated above demonstrated the way the partnering agencies making use of TEMPORA gained access to the *light oversight regime* the programme is operated under. Through direct and indirect

operation of programmes run under foreign jurisdiction, the partnering agencies effectively manage to circumvent domestic legal hindrances to surveillance efforts. For instance, while the NSA is legally required not to direct its operations at American citizens unless there is reasonable ground for it (Greenwald & Ball 2013), the vast amount of data the omnivore TEMPORA intercepts is regularly accessed and processed by NSA analysts without prior removal of U.S. citizens' communication data. The use of *surveillance jurisdiction shopping* as an instrument in the expansion of surveillance efforts is promulgated well beyond the *Five Eyes* collaboration and just like other types of jurisdiction shopping seems intractably interwoven with processes of globalisation (see also Bauman et al. 2014, p. 125).

To foreshadow a key finding of this thesis, *surveillance jurisdiction shopping* evinces the way processes of globalisation elude the national boundaries of territorial and jurisdictional sovereignty. For one, the surveillance of entire populations as opposed to state leaders produces legal tensions as bulk collection of communication of individuals not subject to reasonable suspicion under numerous jurisdictions poses an unreasonable state intrusion into the realm of individual privacy. Secondly, tapping into the jurisdiction of partnering countries in order to gain access to data on the domestic citizenry demonstrates how the exercise of state sovereignty can be undermined the by states' own institutions as processes of global integration can supersede core functions of the state (such as the provision of a right to privacy).

As alluded to previously, the *Five Eyes* cannot be grasped as one homogeneous block of surveillance agencies, but the way the different agencies interplay seems highly complex. Within the *Five Eyes*, GCHQ doubtlessly is the closest NSA ally, as the two agencies regularly engage in joint surveillance operations and grant each other generous access to technologies and acquired intelligence. Furthermore, NSA appears to have invested staggering amounts of resources into the British spy apparatus over the years, providing an abundance of incentives to GCHQ to conduct its operations in accordance with an American surveillance agenda (Greenwald 2014a, p. 118 ff.).

This active coalition aside, a number of documents allegedly leaked by whistleblower Snowden provide evidence of the way the NSA has collaborated with the other *Five Eyes* countries. The advanced degree of cooperation between these different countries has led observers to speak of an *Anglo-American guild* of professionals that – as will be seen- increasingly extends to other Western countries (Bauman et al. 2014, p. 127). It has become clear that the extension of NSA capabilities to partnering agencies is a beneficial process to all parties involved respectively, even in cases where partnerships are received ambiguously

by foreign partners. Beyond doubt, what is found here are processes of ambiguous integration that takes place in all spheres of globalisation to which globalising surveillance poses no exception. Here I say *ambiguous* as processes of global integration may not be seen as reciprocally envisaged but are guided by the simple fact that 'power relations structure the game' (ibid.), which – once again – given the preponderance of the U.S. on a global political stage, informs the notion that in key dimensions globalisation remains a U.S.-dominated phenomenon (Nye 2002).

The beyond

Using its infrastructural power, the NSA provides a number of countries with incentives to cooperate in surveillance matters and has established a global network of what is described as *second* and *third tier partnerships*. Again, the network comprised by these partnerships exhibits a complex topography of different degrees of involvement and exchange of technologies for intelligence or access to certain geo-political advantages. Predictably, such partnerships are a matter of mutual trust, reliance and a history of successful cooperation. If that is the case, as one allegedly leaked internal document describes, 'NSA might be willing to share advanced techniques with a proven and reliable partner, in return for that partner's willingness to do something politically risky' (Appendix 1: Third Party Relationships). While the scope of this analysis does not allow for a scrutiny of all the (known) second tier partnerships, most of these collaborations seem to follow a common pattern. The NSA, on the one hand, has a lot to gain from these partnerships:

> Our partners' geography and access to high-priority target communications are a huge plus, as is their expertise on specific targets. With rare exceptions, they know their regional 'hoods better than we do and they exponentially add to our foreign language capability (ibid.).

What is missing in this excerpt, it seems, is the aforementioned aspect of *surveillance jurisdiction shopping* which also largely applies in the case of second- and third tier partnerships. As assumed above, the NSA engages in intelligence collaborations where it is to the benefit of its own interests, i.e. when the collaboration helps to overcome pre-existing hurdles to NSA surveillance efforts. These hurdles can be of geo-political, linguistic, technological and monetary nature, and the NSA ensures that its partner can deliver in the respective realms. The partnering agencies, on the other hand, also have a lot to gain from these collaborations. The NSA routinely invests hundreds of millions of dollars in partnering agencies' technological infrastructure and the training of foreign personnel. Over the decades the NSA has thus set up a network of partnerships that in individual cases are almost as

intense in cooperation as with the *Five Eyes.* Among these, Israel, Sweden and Germany stand out most starkly.

Israel enjoys a surprisingly close relationship with the NSA. Greenwald reports that documents allegedly leaked by whistleblower Snowden details how the NSA routinely shares raw intelligence that includes the data of American citizens – the analysis and processing of which is made difficult for the NSA by the American intelligence oversight regime. Data distributed with the Israeli partnering agencies include 'unevaluated and unminimized transcripts, gists, facsimiles, telex, voice, and Digital Network Intelligence metadata and content' (Greenwald 2014a, p. 124, document allegedly leaked by Edward Snowden). In line with the notion of *surveillance jurisdiction shopping*, much of the sharing of raw intelligence occurs without having undergone processes of minimisation. *Minimisation* is a process where information is destroyed if the interception of this information is prohibited under the American intelligence oversight regime, which is often described as lax (for a contrasting opinion see Margulies 2014). Most surprisingly, despite close cooperation between the NSA and its Israeli counterpart, NSA 'identified Israel as one of the most aggressive surveillance services acting against the United States' as the country regularly spies on the U.S. in order to gain intelligence on its Middle East policies (Greenwald 2014a, p. 125).

Sweden and Germany are part of the NSA's most longstanding partnerships outside the *Five Eyes*, with both countries having received extensive training and equipment in return for special access to geo-political advantages and surveillance environments. In terms of mutual trust, Sweden is understood to be NSA's closest partner in Europe. Sweden's FRA is considered to be an 'extremely competent partner' (Rensfeldt 2013, document allegedly leaked by Edward Snowden) and the joint NSA-FRA efforts have included the tapping of fibre-cables in the Baltic Sea, the operation of XKEYSCORE and other NSA programmes on Swedish technological infrastructure (NSA 2004a), broad-scale sharing of intelligence and the exploitation of various Internet protocols (NSA 2013a). Most astonishingly, leaked documents say that given the depth of collaboration between FRA, NSA and GCHQ, Sweden can be considered an equal partner to the Five Eyes countries (Rensfeldt 2013).

Germany, NSA documents state, constitutes the geo-politically most important *second-tier partnership* the NSA maintains in Europe, hosting a number of central NSA sites. Not only is Germany host to the Frankfurt DE-CIX, but it also is home to various NSA sites that play different crucial roles in the NSA's global surveillance infrastructure. As has been reported (SPIEGEL ONLINE 2014, documents allegedly leaked by Edward Snowden): The NSA European Technical Center in Wiesbaden is a 'primary communications hub' in Europe;

Stuttgart-Vaihingen hosts another NSA centre charged with the analysis of intelligence originating from North Africa; the European Security Center, endowed with the 'collection, processing, analyzing and distribution' of communication streams, as well as the provision of 'crisis support to military operations, is located on Army properties in Griesheim near Darmstadt, codenamed *Dagger Complex* (NSA 2004b). According to leaked files, this site is tasked with a number of responsibilities:

> NSA integrated its Threat Operations Center, responsible for early danger identification, into the site. A total of 26 reconnaissance missions are managed from the Griesheim complex, which has since become the center of the "largest Analysis and Production activity in Europe," with satellite stations in Mons, Belgium, and in Great Britain (SPIEGEL ONLINE 2014, quotation mark in original).

Additionally, NSA has provided technical assistance to the BND on numerous occasions and the partnering agencies run several joint SIGINT operations, most notably in Bad Aibling and Manfall Kaserne, both located in Bavaria (NSA 2005, 2007). Other examples include the importance of the airbase of Ramstein to the American *Drone War* in tribal regions in Pakistan and Afghanistan. While a more detailed look at the German-American surveillance partnership will unfold in the following chapter, the study of *second tier partnerships* sheds light on the complexity of global surveillance infrastructures. While providing the NSA with numerous forms of access to certain goods and receiving considerable shares in training, technology, and, thus, the possibility to participate in global surveillance networks, *second tier partners* remain heavily targeted by NSA spying activities, the NSA wiretapping the phone of Angela Merkel possibly being the most prominent example for this.

The *third tier partnership* is where things get seemingly dark. These countries are predominantly spied on by the *Five Eyes* rather than bringing about sustainable collaboration in intelligence matters (see Hager & Gallagher 2015). And yet, they inform the notion of the robustness and depth of the NSA global surveillance network. Again, network externalities can clearly be seen at work where the value of a network grows with the number of parties it comprises. Therefore, *third tier partners*, despite forming constant targets for the NSA, are left with choices that present no real choices considering the externalities of the NSA surveillance network. As Anderson explains this with regard to India which is

> heavily involved in information sharing with the NSA, [...]. A non-aligned country such as India used to be happy to buy warplanes from Russia; nowadays it still does, but it shares intelligence with the NSA rather then[sic] the FSB. If you have a choice of joining a big spy network like America's or a small one like Russia's [...]. It may be partly an ideological choice, but the economics can often be stronger than the ideology (Anderson 2014, p. 2).

It seems that such choices are *surveillance hegemony* at its best. While the NSA does not appear to invest heavily in the infrastructures of *third tier partners* in terms of technologies and training, its deployment of instruments of power softer than direct coercion prompt countries to participate in the existing order. While the scope of collaboration seems limited in the case of *third tier partnerships*, they still feed into the surveillance hegemonic order the U.S. maintains.

Case example: NSA partnership with German BND/ BfV and the joint use of XKEYSCORE

What are the terms under which *partnerships* between the NSA and partnering agencies unfold? German news outlet ZEIT ONLINE (2015, unless otherwise noted all excerpts concerning the terms of reference between the partnering agencies stem from this source) published the general terms of reference of an agreement between NSA, BND and BfV concerning the joint use of NSA run programme XKEYSCORE that were allegedly leaked by Snowden. This agreement, dated April 2013, aims at

> Provision[ing] the BfV, through the BND, with the NSA-developed XKeyscore computer network exploitation software to improve the BfV's processing analytic capability to encounter extremist threats and, to the maximum extent possible, share all data relevant to NSA's mission.

The wording of this agreement suggests that at the time of drafting, the BND was already able to operate XKEYSCORE. Most astonishingly, the legal basis for this agreement dates back to a 'treaty between the U.S. and the Federal Republic of Germany, entitled Interchange of Patent Rights and Technical Information for Defense Purposes, signed January 4, *1956*' (emphasis mine). The terms of reference state the responsibilities of the different parties involved. The NSA is to provide BND with XKEYSCORE – understanding that the BND will transfer the technology to the BfV – and provide technical assistance in case of software problems. The BND is to help set up XKEYSCORE on BfV computers and train and support BfV in the use of XKEYSCORE. The BfV, lastly, is to pay for the costs of this collaboration, not to use XKEYSCORE against American citizens or entities and in accordance with German law, and, 'share all data relevant to NSA's mission'.

What seems in line with the general overview of *second tier relationship* schemes elaborated above reveals surprising particularities at a closer look at these terms of reference. Firstly, the present collaboration occurs under a law that came into effect almost sixty years before the present agreement was reached. The law doubtlessly was drafted at a time when surveillance occurred under entirely different circumstances and under the use of possibly analogous technologies far less penetrative and powerful compared to programmes such as

XKEYSCORE. From this one can deduce that either there is no law in place that provides a more contemporary legal framework for such collaboration, or that if such a law existed, it was wilfully ignored. This fact seems in line with an underlying discrepancy between legal frameworks and surveillance practices which essentially allows for such practices: The use of laws that seem outdated with regard to the reach and depth of modern technologies, whose wording might have provided clarity under the circumstances in which they were drafted, but whose wording seems vague at best with regard to what modern technologies are capable of, such as the bulk collection of communication data of entire populations or the technological capability to penetrate individual subjects' lives most deeply at very limited costs. While the referenced 1956 law might have provided a sound legal environment sixty years ago, that does not necessitate the suitability of this law under the present circumstances and therefore entails the possibility of under-regulation of intelligence collaborations.

Secondly, in contrast to the BND, the BfV is a domestic security agency tasked with the protection of the German constitution and the inner-German democratic order. As this mandate arguably entails counter-terrorism operations and given the fact that what is framed as *terrorism* is, if not a global than at least an international phenomenon, it makes sense to have some kind international cooperation on this matter. However, the fact that the NSA manages to project its technological infrastructure into an agency tasked with domestic surveillance bears testimony to its infrastructural power and hegemonic position. This relationship is a fairly recent phenomenon, as one allegedly leaked file states that NSA received 'approval in March 2013 to *establish a formal CT relationship with the BfV* and anticipates increasing synergy against the target with BND/BfV/NSA collaboration' (NSA 2013b). And so, by providing the BfV with XKEYSCORE, another file states, 'NSA will enable Germany to provide unique contributions in the form of collection, data summaries, and/or finished intelligence to the high-priority CT mission' (NSA 2013c). It can be assumed that direct operational synergies will be produced in accordance with other NSA and BND sites operating XKEYSCORE. The BfV sees the advantage in the use of XKEYSCORE in its capacity to decode most protocols used in the volatile world of the Internet, which the apparently partially out-dated BfV programmes were struggling with (Netzpolitik.org 2016). BfV employees, questioned by a German parliamentary committee, maintained that the BfV had acquired a slimmed-down version of XKEYSCORE that merely served to analyse previously and lawfully acquired data of individual targets. This slimmed-down version, they assured, could neither serve to share bulk communication data, nor could it be used by the NSA to spy on the BfV itself. All the while, intelligence acquired under the use of

XKEYSCORE seems to be related to BND which in turn communicates the acquired intelligence to NSA (ibid.).

Finally, revisiting the study of network externalities, it seems that the installation of NSA surveillance programmes on partnering agencies' surveillance equipment potentially creates technological lock-ins *within* global surveillance infrastructures which further enhances network externalities (Anderson 2014, p. 3). Supplying surveillance technologies to partnering agencies arguably increases the dependence of these agencies on the capabilities of the NSA – and its willingness to share its know-how. Essentially, the provision of surveillance technologies to partnering agencies is as much a matter of achieving short-term goals – access to SIGINT and possibly new segments of global communication – as it is part of what could be dubbed a *mission creep of surveillance hegemony enhancement*: A project to solidify the cooperation of partnering agencies in the long term by furthering their dependence on NSA infrastructure and capabilities and deepening what is framed as *partnerships* and *cooperation*. This *mission creep* arguably forms a part of the enhancement of NSA global surveillance infrastructures and is thus intractably interwoven with the ongoing globalisation of surveillance that is partially carried by prevailing *partnerships* and *cooperation*.

Merging of law enforcement and intelligence

The collaboration between BfV, BND and NSA, all tasked with supposedly very different mandates, comes to little surprise given how network externalities seem to be at work even within the state security apparatuses, where law enforcement and intelligence increasingly merge. While the previous chapters have scrutinised the way externalities make the global NSA surveillance network grow and more powerful – so that it is still better for other states to (even reluctantly) join this network given its scale and technological capabilities – this chapter analyses externalities within state security apparatuses on a different level.

Historically, Western states used to exhibit a division of labour between law enforcement and intelligence. Collaboration between these separate realms of the executive was at times necessary in the face of threats to state and society whose origin and targets could not be pinpointed to an interior or an exterior. The different realms of the executive therefore cooperated where, in a sense, desperate times call for desperate measures. It can however be assumed that *in practice* law enforcement and intelligence have always exhibited merging tendencies, especially as they both vertically operate under the same highest entity, namely the head of state or the government, and both form part of what is broadly termed the *security apparatus*. Thus it can further be assumed that these tendencies to merge where already

taking place in the U.S. and other Western democracies before 9/11 (Monahan 2011). Yet, this analysis understands that the global *War on Terror* has introduced new dynamics to the merging of law enforcement and intelligence and consequently provided an 'an impetus for a surge in many preexisting, but perhaps dormant, forms of state surveillance' (ibid. p. 84).

The merging of law enforcement and intelligence seems intractably interwoven with the perceived *threat of terrorism*. As alluded to before, this perceived threat has seen a general shift from the prevention of immediate threats to the premediation of possible threats, focusing on individual subjects as possible agents of threats. This focus on sub-state threats has broadened the conception of national security and led to a blurring of boundaries between *foreign* and *domestic* intelligence and to a greater connectivity between the different agencies tasked with the originally separate types of intelligence, as well as between the different respective agencies (Walsh & Miller 2016, p. 357). As a result, law enforcement and intelligence have undergone processes of merging. This merging takes place on a number of levels. Firstly, on a technological level, it seems that

> law-enforcement and intelligence systems will merge into a single surveillance system, since [...] there are strong network effects, there is technical lock-in growing from the fact that everyone's using the same technology platforms and presenting warrants to the same service firms for the same data; and the back-end systems needed to aggregate, index, and analyse the product have high capital costs and very low marginal ones (Anderson 2014, p. 71 f.).

Once again, network effects and externalities in the informational spheres seem to be an underlying logic in surveillance networks. While network effects seem to be at work on a transnational level as seen with the profusion of XKEYSCORE to foreign agencies, it can be assumed that efficient surveillance programmes are equally distributed between different domestic agencies. After all, there is no reason why the FBI should not be operating a programme such as XKEYSCORE if both BND and BfV are operating it in Germany. The exercise of surveillance is therefore influenced by the dynamics of network effects that see different parties use the same technologies. The repeated use of the same technologies constitutes new surveillance practices which in turn form an integral part of surveillance, and feeds into a particular informational economy geared towards the used technologies.

Secondly, this merging of law enforcement and intelligence is reflected in the merging of institutions (ibid.). It appears that under the contemporary counter-terrorism *dispositif* the collaboration between different security agencies is a must and a given. Counter-terrorism units now combine the personnel of different agencies and are subsumed under common mandate to premediate and foil future terrorist attacks (Monahan 2011). The counter-terrorism divisions tend to amalgamate different spheres of the executive to the degree that response

units, intelligence gathering units and law enforcement units can be subsumed under the same body. This analysis supports the notion that once enacted, it will be difficult to disentangle such institutional amalgamation in the future as such mergers tend to decrease governmental accountability and transparent governance (Anderson 2014; Monahan 2011; Regan & Monahan 2014).

Ultimately, perhaps the most revealing way law enforcement and intelligence mergers can be observed lies in the novel spatial configurations these mergers produce: Law enforcement and intelligence agencies now routinely cooperate in fusion centres, a reterritorialisation of political power that is likely to spread in Europe similar to the way it has diffused all over the U.S. in recent years. The U.S. Department of Homeland Security, since its formation in 2002, has overseen the creation of a nationwide network of close to one hundred fusion centres that aim at sharing and analysing information in order to prevent possible terrorist attacks. As Torin Monahan informs us, fusion centres

> prioritize counterterrorism activities, [...] conducting "threat assessments" for events and linking "suspicious activities reports" to other data to create profiles of individuals or groups that might present terrorist risks. In this capacity, fusion centers engage in a form of "intelligence-led policing" that targets individuals who match certain profiles and singles them out for further monitoring or preemptive intervention (Monahan, 2011, p. 84).[7]

These centres are usually located within police and state departments and staffed with employees from different agencies and private companies operating in the respective industries. The staffing with personnel from different agencies is no coincidence of course, but rather lays the foundation for the envisaged merging of the different spheres of the executive. As the Department of Homeland security itself describes, the '[fusion] centers' goals are to blend law enforcement and intelligence information, and coordinate security measures to reduce threats in local communities' (Department of Homeland Security, quoted ibid.).

As such, the surveillance of global flows of information intersects with *the local* in peculiar ways. Firstly, because fusion centres can be understood as an expression of the informational surveillance society, as they largely acquire the to-be-analysed data from the private sector and share analysed information with this sector, I suggest that *fusion centres are a means of*

[7] The accumulation of data and centralisation of political power at fusion centres unfortunately often entails abuses of power, such as racial and political profiling, surveillance of non-terrorist groups and activists, and illegal data mining. As Monahan (Ibid. P. 88 f., quotation marks in original) explains: 'surveillance capabilities of fusion centers enable and invite "mission creep" [...] whereby analysts draw upon the resources at their disposal to exceed the policies and laws that are intended to govern their activities.'

integration into the global informational economy. The discussed processes make fusion centres switching points in the spaces of global flows of information and at the same time intractably interweave the exercise of political power with a global informational economy. The organising logic of fusion centres transforms local places into spaces where informational modes of production – the production, accumulation and processing of (big) data – are utilized *partially* in ways in line with the agenda of political power. Here I say *partially* because fusion centres also help bring to light the paradoxes of globalisation and the rescaling of political power: On the one hand, they are an instrument of integration into globalising surveillance and into the global informational economy and at the same time the exercise of political power at fusion centres is often marked by a lack of clear-cut policies and mandates and does not always occur to the benefit of governance (Monahan 2011).

Lastly, fusion centres are an example of state-led glocalisation of political power. The state is proactively mobilising local resources in order to grasp a globally spread phenomenon using globally spread technologies and create spaces where this phenomenon can actively be pursued and grasped. This at the same time makes the respective local appealing to investments and generates employment in certain sectors given the ongoing privatisation within surveillance infrastructures and practices (see following chapter).

Commercial surveillance partners

In capitalist societies comprised of privatized telecommunication providers, surveillance has always relied on the ambiguous cooperation of commercial entities. These entities are usually in charge of communication infrastructures and thus hold the key to the media of communication – and the exploitation thereof. Setting up a global digital surveillance infrastructure under the general trajectory to *collect it all* therefore necessitates the voluntary or forced cooperation of commercial entities. In the spirit of the hegemonic *partnerships* encountered previously, these collaborations with commercial entities here are dubbed *ambiguous commercial surveillance partnerships*, knowing full-well that these arrangements often are produced by direct or indirect coercion. However, it is argued that the business models and commercial infrastructures of these private entities contribute to the emergence of new kinds of surveillance, and thus, wilfully or not, these entities are partners to state agencies engaging in surveillance.

Thus, a number of previously discussed programmes rely on the collaboration of commercial partners: The interception of fibre-optic cables is often facilitated by telecommunication providers that either help set-up interception devices or readily provide facilities where the NSA can operate its interception missions. Beyond the provision of facilities and

infrastructure, providers are often obliged by law to share customer information and consumer data. The first-ever Snowden revelation broke that American provider Verizon is compelled by law ‘produce to the NSA electronic copies of "all call detail records or 'telephony metadata' created by Verizon for communications between the United States and abroad" or "wholly within the United States, including local telephone calls"’ (Greenwald 2013a, excerpt from NSA documents allegedly leaked by whistleblower Edward Snowden). Similar legal mechanisms oblige German providers to hand over customer information to the BfV, now equipped to mine the data using XKEYSCORE, while BfV employees assure that this occurs only on an individual case-to-case basis (Netzpolitik.org 2016). Given the presence of network externalities within the IT and communication industries, the collaboration of providers grants the NSA access to vast amounts of consumer information.

Furthermore, the *PRISM revelation* shed light on another aspect: The nexus of digital modes of production and surveillance. Under the PRISM programme U.S. agencies access user data of Internet giants such as *Google, Facebook, Apple* Inc. and others. It has been reported that the companies in question were unaware of this programme (Greenwald & MacAskill 2013). While there exist contrasting opinions concerning the truth of this statement,[8] I argue that the *wilfulness, ignorance or forced nature of such cooperation is secondary* to an analysis of the way digital modes of production and surveillance intersect, in the sense that the readiness to cooperate might grant the NSA access to yet greater amounts of data, but the possibility of such forms of surveillance is rooted more deeply in the nature of modes of digital production and capital accumulation in the informational economy. Anderson explains the complexity of the *PRISM* case, highlighting that the companies in question ‘believed they were providing only targeted warranted access to the FBI; it came out only later that an NSA analyst can click on a button [...] and cause a request to flow automatically through the FBI to their systems' (Anderson 2014, p. 4). And yet, such forms of surveillance are only possible in the informational economy: After all, the tapping into user data is preceded by the unbridled accumulation of user data mined for advertising purposes. The gathering of user data and the consequent mining of this data *is* the mode of production for a number of Internet giants, and as such, these companies produce spaces where the data is stored, namely on databanks, clouds, and high-octane servers. In essence, the emergence of big data fuelled new forms of surveillance that ‘draw upon existing practices of voracious data collection and fluid

[8] For instance, Bauman et al. argue that the companies in question are forced to hand-over vast amounts of user data under the given programme (2014 p. 123), while Schmid (2014) argues that PRISM rather has to be understood as a programme serving the surveillance of individual targets.

information exchange, as exemplified by social networking sites such as *Facebook* or private-sector data aggregators' (Monahan 2011, p. 87, italics mine).

Bauman et al. (2014, p. 123) point out that the complicity of Internet companies in surveillance places these companies in an unclear position between public and private actors. And yet, much more seems to be at stake in the context of the convergence of internationalisation, digitisation and privatisation of surveillance:

> This conjunction creates an overarching effect of dispersion that challenges the very idea of a reason of state conducted by a "state" in which the government determines national interests and national security [...] the concept of reason of state is now less and less encapsulated in the formula of a national security performed by intelligence services socialized into secrecy and public responsibility, patriotism, and suspicion of services in other nations. Rather, we see the transformation of a reason of state through the emergence of a digitized reason of state performed by a heterogeneous complex of professionals, of sensitive information hybridizing private and public actors (ibid. p. 126, quotation marks in original).

The partnerships and collaborations between the NSA and foreign intelligence agencies doubtlessly serves the externalisation of surveillance and the simultaneous process of jurisdiction shopping. The ambiguous partnerships between the NSA (as well as foreign agencies) and private enterprises however externalises surveillance beyond state-led surveillance efforts and allows it (surveillance) to permeate the fabric of society on previously inaccessible levels. Public/private liaisons not only present drastic changes to the environment of surveillance and the way it is conducted by discernible actors, but given the way private actors operate, complicity is arguably extended to the individual subjects that make use of certain platforms or use the products of certain companies (Bauman & Lyon 2013, p. 66; see also Giroux 2015, p. 111). This externalisation of surveillance in the shape of the participation of consumers informs the notion of the consumer *synopticon* as a new form of surveillance occurring in decentralised digitalised networks where every individual is surveillant and under surveillance alike (Bauman & Lyon 2013, Frick 2015, p. 78). This circumstance can equally be interpreted in the context of technological lock-ins: Given the advanced degree of cooperation between public and private actors and the standing certain Internet giants enjoy in their respective markets, it becomes increasingly hard if not impossible for individual subjects not to participate in (their own) surveillance.

Once again, the extension of the exercise of surveillance into private realms seems to be a most pervasive form of rhizomatic expansion: Surveillance is undergoing processes of deterritorialisation and reterritorialisation in the shape of the manifold user accounts, electronic gadgets and online interaction associated with individual consumers. The

networked society thus has broadened the plane of consistency to countless potential dimensions whose potentiality of interconnection appears far from exhausted.

Chapter 5: Towards a critical understanding of globalising surveillance

Bringing together the various findings emanating from the previous chapters, this chapter seeks to bring forward a critical understanding of the globalisation of surveillance that partially relies on insights gained elsewhere and partially introduces a new perspective to the study of the globalisation of surveillance.

Network analysis of NSA global spying activities: a (de-)centralized distributed network

The three communication network types proposed by Baran and partly refined by Galloway served as a foil through which the Internet and its exploitation can be analysed. The global NSA surveillance infrastructure is arguably comprised of networks. However, the complexity of these global infrastructures suggests an analysis that eludes the theory of three network types. I argue that *global NSA surveillance infrastructures consist of a complex multiplicity of partially nested and partially interconnected centralised, decentralised and distributed networks which allows for manifold forms of interconnection, surveillance and expansion*. As such, the theory of the surveillant assemblage expanding in rhizomatic ways serves best to understand the complex geography of this interweaving of networks (for a similar understanding of the NSA global surveillance network(s) see Fichtner 2014, p. 70 ff.). Furthermore, I here concur with Berry (2008, p. 368) that network analyses routinely neglect the question of scale which shall be met here by several scalar references.

A *centralised* network structure can be found within the institutional arrangement of the NSA itself. The greater trajectory of NSA surveillance is undoubtedly conceptualised, decided upon, managed, and overseen from its headquarters at Ford Meade, Maryland. While the NSA maintains operation-, interception- and data processing sites on the better part of the globe, the structure of this network doubtlessly has a central hub in the shape of the headquarters. The headquarters are also the site where most of the surveillance programmes are designed, programmed and implemented and where the majority of surveillance operations are directed from. At the same time the headquarters are also the NSA site at which by far the most staff is employed. Equally, in its function as headquarters Fort Meade presumably is allocated the lion share of the NSA budget. Consequently, as with Baran's centralised network, the NSA internal institutional composition displays a strong hierarchy.

Another sphere where the *centralised network* provides a useful tool of analysis is the composition of NSA processing centres (not to be confused with the *fusion centres* where numerous agencies cooperate, see below). The data flows intercepted by the NSA are duplicated using splinters and other duplication devices. The flows of data are usually not interrupted and permitted to flow freely (while being duplicated) – the exception of course is when the NSA decides to take entire networks or even countries off the grid. The *duplicated* flows however become 'part of a new network of unidirectional, centralized data streams which flow from peripherical[sic] nodes (the intersection points) to the central hub (the HQ) but not the other way around' (Fichtner 2014, p. 70). Whereas the Internet backbone has to be understood as a decentralised network, the intercepted and duplicated flows of data streaming through this network are assembled in a centralised manner. Figure 3 shows how this is the case within the U.S. where the NSA regularly intercepts data flows at IXPs.

However, on a global scale the geography of interception sites looks markedly different. The *decentralised* network appears on a number of levels. Firstly, NSA interception sites on a global scale are routinely located at key nodes of the Internet backbone infrastructure which in turn comprises a decentralised network of several hubs and clusters while other geographical areas are more peripheral to the backbone infrastructure. Accordingly, the NSA decentralised network of interception sites consists of hubs and of less significant nodes, sites where the NSA maintains large interception and processing operations, and sites of minor importance. At this point I differ with Fichtner (ibid. p. 70 ff.) who assumes a unilateral one-directional stream of duplicated data flows which transforms the decentralised Internet network into a centralised network of duplicated data flows. I argue that while this assumption may be accurate within the territory of the U.S. and the NSA headquarters undoubtedly function as the most important central hub in the global geography of duplicated data flows, the complex geography of globally dispersed interception sites consists of clusters where flows are analysed and processed, and of more peripheral spheres. This network already relies heavily on the cooperation of partnering agencies whose interception sites and operations present an enhancement to the decentralised network of interception sites which once more brings to the fore how intractably the cooperation with partnering agencies is interwoven with the NSA global surveillance network.

As an example: The aforementioned programme TEMPORA has its main interception site set up in Bude, UK. This GCHQ-run site proves to be one of the key interception operational sites run by GHCQ – and is at the same time a site where one of the largest surveillance operations worldwide is carried out. Yet, given the degree of close cooperation between NSA

and GCHQ which involves the *mutual* sharing of vast amounts of data – the world *mutual* describes an at least bi-directional flow of information, which can be further diversified given the manifold ways partnering agencies interconnect. Bude is a central hub within global surveillance infrastructures, just as much the GCHQ headquarters in Cheltenham, UK, are. And both do not primarily work in the service of Fort Meade. The complex relationship entailed in such partnerships shed light on the complexities of globalisation processes within surveillance infrastructures and will be scrutinised further in the later chapter *Revisiting surveillance hegemony*.

Furthermore, the dispersion of fusion centres in the U.S. equally appears to follow the organising logic of the decentralised network. As has been seen, fusion centres are dispersed all over the US, staffed by employees of a whole array of national-, state- and local agencies and intelligence wise feed into and are fed by a number of different agencies. It is not only the NSA that has a share in this moderately recent phenomenon as intelligence stemming from these centres is widely distributed. This again informs the notion that the merging of different surveillance networks is a process integral to the globalisation of surveillance and brings to the fore newly emerged spatialities this form of globalisation has produced.

It is important to understand that these different networks NSA surveillance feeds off seem to be partly nested and partly interwoven. For instance, an interweaving of networks is apparent where the distributed network of interception sites across the globe remains institutionally centralised in the shape of headquarters that delegate functions and responsibilities. At the same time, intelligence processed at fusion centres that is related to the NSA is either sent directly to the headquarters or circulated within the centralised NSA data storing network. Lastly, the mutual sharing of SIGINT presents a clear example of interweaving networks which in the case of some close partnerships go even beyond that as networks are merged. On the other hand, different networks are nested, for instance within the internal NSA hierarchies: A network of domestic listening posts feeds into the NSA Utah data centre which in turn relays intelligence to Fort Meade (see Appendix 3: Nested NSA networks).

Yet, where can the distributed network structure be observed? As it stands, things are more complicated with the distributed network whose structure is more intricate. Based on the argument brought forward by Galloway (2004) that the distributed network is the network equivalent to Deleuze and Guattari's rhizome, I now turn to the way the global surveillant assemblage serves best to explain how global NSA infrastructures can be conceived as distributed networks – and how the concept of the surveillant assemblage needs some refinement in the light of the here undertaken focus on globalisation.

The rescaled global surveillant assemblage

In this chapter I argue that *the globalisation of surveillance infrastructures is closely linked to the deterritorialisation and rescaling of the global surveillant assemblage which in turn can be linked to globalisation processes more generally and beyond the field of surveillance.* To begin with, the overall picture of global surveillance infrastructures arguably goes beyond the scope of centralised, decentralised and distributed networks. At best, one could argue that the *robustness* of the distributed network can be observed in the robustness of global NSA surveillance infrastructures – given how the complexities of this infrastructure allow the NSA to work around possible failures within the system. Should one programme or operation fail and part of the network be disrupted, it is very likely that either another NSA-run programme or operation, or that of another U.S. agency or possibly that of a foreign partnering agency will have successfully acquired the desired SIGINT or at least can provide some assistance to its acquisition. And as is the case with the distributed network, this network of surveillance infrastructures allows for unprecedented ways of control and surveillance.

Yet, while the network diagrams are a helpful means to understand the working logic of the multiple nested and interwoven layers of NSA surveillance infrastructures, the network typology does not suffice to explain their complex interplay. For this, yet again, the global surveillance assemblage seems a helpful analytical tool. As seen previously, the surveillant assemblage entails an increase in multiplicities by bringing together diverse surveillance systems. A key operation of the surveillant assemblage is the duplication of flows, intercepted at centres of appropriation and evaluated at spaces of comparison (Haggerty & Ericson 2000). Singling out a certain programme or system within the assemblage makes sense only for separate analysis, but the essence of the assemblage lies in the *working together* of a multitude of different systems. That said, what seems most essential here is the described rhizomatic expansion of assemblages through de- and reterritorialisation.

There can be no doubt that the NSA global surveillance apparatus in all its interconnections, branching and layers is what materially comes closest to the surveillant assemblage and the principle of rhizomatic expansion within surveillance. Global NSA infrastructures seem to epitomise what Deleuze and Guattari (2005, p. 8) mean by an ‘increase in the dimensions of a multiplicity that necessarily changes in nature as it expands its connections’. As global NSA infrastructures expand through new technologies, new surveillance systems and new interconnections created with modes of capitalism, the digital economy as well as partnering agencies around the globe – the NSA infrastructures themselves change and simultaneously adapt to and alter prevailing surveillance systems and infrastructures. Just as the plant

growing in rhizomatic fashion changes its overall form and that of the roots penetrating the soil, so does a globalised surveillance apparatus.

The networked society, described by Castells, has allowed for a broad-scale de- and reterritorialisation of surveillance systems (see also Murakami Wood & Coaffee 2006). This de- and reterritorialisation has occurred on a technological level, on an inter-systematic level (in the shape of global flows of data that can be intercepted and duplicated at manifold surveillance spaces), on an institutional level (which allowed for the externalisation of surveillance operations to other agencies, corporations and even individual citizens) and in the field of the political economy of the networked society that produces ever-increasing amounts of data and products and services that make use of this bulk of data. Consequently, the rescaling of the surveillant assemblage occurs on all levels of spatial scale, deeply affecting the global, regional and local (the aspect of glocalisation will be discussed in the following chapter). The infrastructures of the surveillance assemblage stretch from surveillance networks comprised of myriads of interception and processing sites across the globe to the very individual electronic device individual citizens carry in their pockets that may be turned into a surveillance tool. What these myriads of surveillance points have in common, I argue, is their *potential* working together – and that on a spatial predisposition for the global.

Yet, how can one grasp the *global* in the *global rescaled surveillant assemblage*? Murakami Wood (2013, p. 320 ff.) argues that the *global* in global assemblages is too vague a concept and needs strengthening through a look at the political economy of neoliberal scalar production: *Global*, he argues, is itself a product of neoliberal scalar politics and surveillance plays a role in this production on a number of levels. Firstly, the term *global* has an all-encompassing aspiration of a sphere that virtually knows no outside, an aspiration that both surveillance and neoliberalisation share discursively. In terms of surveillance once again this seems epitomised by the NSA motto *Collect it all* (Greenwald 2014a). Secondly, surveillance facilitates forms of government that operate globally:

> [G]lobal markets must be matched by appropriately global forms of government to facilitate the extension of economic freedoms and ensure the functioning of those markets. In order to facilitate this both as material rescaling and reterritoralization of economic activity one of the key forms of government that must operate globally – that is wherever and however government is found – is surveillance (Murakami Wood 2013, p. 321).

This role of surveillance can be seen in the light of the control society which ultimately functions based on the enforcement of power structures through control. Only that this enforcement functions on a global level where surveillance is ‘now detached and free-floating from older nation-state structures’ (ibid.) and does not end with the territorial boundaries of

sovereign nation-states. This notion is closely connected to the third way the global and surveillance are linked: Surveillance constructs the global as a discursive instrument, normalising it as the spatial arena for neoliberal governmentality (ibid.). An example for this, I argue, is the way surveillance discourses have shifted to the prevention of *global* terrorism since 9/11. Surveillance, such discourses suggest, has to operate on the global level as the threat it seeks to prevent does equally operate on that level. Beyond doubt, the way the surveillance can be deployed for other purposes than just the prevention of a threat remains largely unmentioned. What follows from this interpretation sustained here is that *global* describes both a condition and a tool driving globalisation trajectories yet further.

What are the trademarks of neoliberalisation of relevance here? Brenner et al. (2010) describe that neoliberalisation can be understood as a path-dependent process of uneven geographies whose main dimensions are: Regulatory experimentation, inter-jurisdictional policy and the transformation of transnational rule regimes. Murakami Wood (2013, p. 321 ff.) relates this observation to the context of surveillance: Regulatory experimentation is at work where one can observe surveillance institutions literally *testing* their equipment on targets and entire populations. What results can particular technologies achieve? The value of particular technologies for SIGINT operations is often determined more aptly when these technologies are actually tried out, instead of being run through virtual projections. That such processes can foremost be a matter of *experimentation*, Murakami Wood argues (ibid.), can be deducted from the fact that many surveillance technologies are known not to produce the desired result – given, for instances, that the deployment of CCTV is being further intensified despite studies pointing to the fact that these technologies have not produced the results desired under their ostensible purpose (see Norris 2012).

Secondly, Murakami Wood argues that policy transfer in matters of surveillance often consists of 'travelling technocrats' that are part of 'transnational networks of expertise' and contribute largely to the spread of surveillance policies *and* technologies (ibid. p. 322) – an observation that will be scrutinised further in the later chapter on *Transfer of policies and technologies*. Lastly, transnational or global rule regimes consist of standards, agreements and joint practices in the context of specific problems and polities that nation-states increasingly adhere to. I argue that in the world of surveillance *counter-terrorism* can be understood as an arena for the establishment of global rule regimes.

What emerges from this excursus to neoliberalisation processes is that the rescaling of the surveillant assemblage cannot be explained by notions of technological determinism. Instead,

the globalisation of surveillance is intractably linked to the broad scale operation of creating *the global* in terms of governance, regulation and processes of neoliberalisation.

However, one may not be misled to believe that the globalisation of surveillance infrastructures leads to similar forms of surveillance spread equally around the globe. Rather, surveillance is historically, socially and spatially rooted (Murakami Wood 2009). It may be spread globally, but it is not implemented (and perceived) the same way everywhere. This analysis predominantly concentrates on the role of the NSA in the globalisation of surveillance as the NSA is identified as a driving force behind this globalisation. The role of the NSA within global surveillance highlights Haggerty's concession that centralisation within the surveillant assemblage may be possible. However, this focus on the NSA does not neglect the fact that surveillance 'operates differently at different socio-spatial levels from orbital space right down to the individual body' (ibid. p. 189). This point will be reflected on further in the concluding remarks.

Glocal surveillance

It seems this analysis has arrived at another paradox: The rescaled surveillant assemblage is as much the NSA as it is not. What is meant by this is that the NSA does not *own* nor operate all the infrastructures necessary to uphold a global surveillant assemblage that functions according to the hegemonic position the NSA holds, nor can it exercise direct control over these infrastructures. The intertwined processes of de- and reterritorialisation of surveillance entail that nation-states have relegated some of its capacities to other entities. I argue that the introduction of glocalisation into the study of the globalisation of surveillance can be understood to draw a connection between different theoretical tools deployed in this thesis, namely the less state-centred surveillance assemblage (deterritorialisation) deployed in the context of surveillance hegemony (reterritorialisation) which brings to the fore the complex and at times contradictory role states play in the context of the globalisation of surveillance.

Glocalisation, as described previously, hinges upon an understanding of state spatiality 'as a dynamic, transformative *process* rather than [as] a fixed thing, container or platform' (Brenner 2004, p. 450). As such, state spatiality is the constantly reconfigured, 'actively produced and transformed through socio-political[sic] struggles in diverse institutional sites and at a range of geographical scales' (ibid. p. 451). In this context, glocalisation strategies aim at positioning sub-state spatial units competitively within supranational circuits of capital accumulation (ibid. p. 473). In essence, such projects are about positioning something inherently non-global (spatial units such as cities, regions, the local) within a globalised form. As such, these non-global units become intractably interwoven with globalised forms to the

degree where these units become restructuring sites for both state-power and the global form in question. Lastly, the participation in global forms and spatial reconfiguration of state-power goes hand in hand with an intensification of uneven development within the respective national territory.

I now suggest that this concept can be taken out of context and applied in the context of the globalisation of surveillance in order to scrutinise the different spatial configurations emerging from this globalisation. There are of course caveats when using a concept that is not tailored to the analysis for surveillance for the scrutiny of the globalisation of that phenomenon. However, globalisation 'does not mean homogeneity. There remain a complex and contingent "placedness" and temporality to surveillance' (Murakami Wood 2012, p. 340, quotation marks in original) and *glocalisation* seems most apt at capturing the spatial heterogeneity inherent to globalisation processes.

Under glocalised surveillance, the global flows of capital in the context of glocalisation are the global flows of information, data. The sub-national spatial units of glocalisation are the different surveillance-, interception- and processing-sites. Here one can observe how the spatial configurations produced by processes of globalisation of surveillance diverge from those produced under globalisation more generally. While the latter identified the urban in general and emergent global cities in particular as the crucial spatial units where state-power is spatially reconfigured as different spatialities coalesce within these units and form new configurations of centralisation and periphery, the picture is arguably different in the world of surveillance.

What are key nodes in global surveillance networks? Surely there are global cities that are part of these networks, be it because they are the location of headquarters of intelligence agencies or because that is where IXPs are located, such as London, Frankfurt, Berlin, Paris, San Francisco, New York, Amsterdam, Sydney, to name but a few. However, there also are other locations with markedly less prevalent names, such as Fort Meade, Bude (UK), Bad Aibling, Griesheim, Manfall, Stuttgart-Vaihingen, and many other secret interception and processing sites around the globe. Some of these sites presumably cannot even be ascribed to a particular city or even village, such as the exact landfall locations of undersea communication cables or possible interception sites of land cables. Given that these sites are usually secret (see below chapter *Shadow Globalisation*), I unfortunately have to remain general and cannot produce an exact geography of glocalised surveillance. However, what one can say is that what all these surveillance sites have in common is that they provide some form of territorial fixity to global fluid phenomena with the respective state providing

essential territorial organisation, infrastructures and institutional arrangements. Consequently, what I observe at these sites are 'contradictory, contested strategies of reterritorialization through which the place-based and territorial preconditions for accelerated global capital [here: global flows of data] circulation are being constructed on multiple spatial scales' (Brenner 1998, p. 3). As with glocalisation in other contexts, it seems that nation-states in this case primarily rely on the provision of immobile factors of production (ibid. p. 15). In the context of surveillance and the interception and processing of data flows these include territorial access to the Internet backbone and IXPs, the localities necessary for interception sites (such as land, estate and buildings), physical infrastructures (such as roads, access to transportation), electronic infrastructures (such as electricity and access to communication networks) and access to secondary infrastructures (such as housing) and the provision of goods to the respective surveillance personnel and, most crucially, access to the respective jurisdiction. The trade-off here is obvious as the states providing these immobile factors through their different spatial units possibly gain access to surveillance networks and improve their standing within the realms of global surveillance and in any case aim to 'position strategic local spaces competitively within global or supranational circuits' (Brenner 2004, p. 473) of flows of data and the surveillance thereof.

Brenner (ibid. p. 454) mentions how a-spatial policies encompass socio-spatial effects. Such policies can impact particular locations and social groups within these locations in distinctive ways and also intensify uneven development within a given territory. The impact on local social groups and the local economy arguably is often limited in the context of surveillance, as surveillance operations are often run by a limited number of personnel. However, exception to this are firstly interception and processing sites that require an increased number of personnel – for instance, the *Dagger Complex* comprises hundreds of employees of different divisions –, secondly headquarters and thirdly fusion centres, especially if the latter encompass outsourced surveillance with private actors (such as Snowden's former employer *Booz Allen Hamilton*) employing hundreds of analysts, researchers, and other necessary personnel.

As mentioned before, this thesis cannot produce a precise typology of the different spatial configurations emerging from the globalisation of surveillance. Not only does such an endeavour elude the format of this thesis, but it is secondly gravely inhibited by state secrecy. What can be established nonetheless is that glocalisation proves a useful analytical instrument that grasps the spatial heterogeneity entailed in the globalisation of surveillance. No matter how elusive phenomena are, be they flows of capital or flows of communication data, there

are spatial ramifications closely intertwined with the circuit and domination of these phenomena. These spatialities are scalable and the different spatial units are sites of reconfiguration of power, capitalism and, in our case, the nature of global surveillance. Ultimately, emerging from the distinct ways surveillance is undergoing processes of glocalisation is that 'specific geography gives political advantages to some countries and may reconfigure power politics at the world scale' (Bauman et al. 2014, p. 124). This stems from the fact that some countries can provide access points to communication infrastructures other states cannot. Taking into account the different ways surveillance may be glocalised doubtlessly opens countless alleys for future research that allow for a consideration of the social, political, economic and, above all, spatial rootedness of surveillance.

These observations on glocalising surveillance can be connected to the aforementioned geographical analysis of *everywhere war* and everywhere surveillance respectively. Everywhere war as a concept highlighted the fact how shifts in technologies, geo-political dimensions of insurgency and modern warfare have produced forms of violence that can occur basically everywhere. This doubtlessly entails a sort of *stealth geography* (Gregory 2011, p. 246) where the potentiality of war remains present though largely invisible. To maintain such geography, intricate interlinks of global and local forces and phenomena seem necessary. The same holds true for surveillance which, as has been shown, is simultaneously globalised to the degree that it can occur everywhere which in turn relies on the increasing glocalisation of surveillance. And as with prevailing forms of modern warfare, the stealth geography of global surveillance is largely pursued through the deployment of state secrecy as a technology of domination, societal control and warfare alike (see below). All the while, globalisation and glocalisation remain intensely heterogeneous phenomena and so a geography of global surveillance has to take into account the countless contingencies, discontinuities and ruptures the intertwinement of these phenomena produces.

Revisiting surveillance hegemony

In total, this study sustains the observations made by Jason Keiber (2014, 2015) on surveillance hegemony while linking this outlook to the globalisation of surveillance. Hegemony in general here was described as a hierarchical exercise of power that derives its legitimacy from more than just material preponderance, but rather from a stability that rests upon and is reflected within a set of rules, institutions and ideas in the shape of social norms and dominant ideologies. Compliance in such constellations derives from a set of instruments of which coercion is only one possible option that solidifies the hegemonic status of the hegemon. Most crucially, hegemony largely operates through the projection of infrastructural

arrangements into the infrastructures of the states subjected to the hegemony. In the case of surveillance, counter-terrorism serves as the ideological background for the projection of surveillance infrastructures into the webbing of other states. This projection can lead to the synaptic or shared use of surveillance infrastructures with both uses generally embedded in institutional arrangements replete with incentives for the cooperation on counter-terrorist agendas.

There is no doubt that the NSA in its commanding function of the global surveillance assemblage upholds a hegemonic position in global surveillance. Yet, a close look at the way this hegemony is upheld produces a picture of paradoxical, contested and dynamic relationships between the NSA (and other U.S. intelligence agencies) and its foreign counterparts. These relationships form a multidimensional mosaic of relationships that comprise what I interpret as relationships of partially *contested integration*: Network externalities in the global political economy of surveillance form a compelling argument for the participation in what seemingly constitutes the biggest surveillance network. Firstly, the projection of NSA infrastructures into other states surveillance apparatus relies heavily on NSA technological preponderance, the creating of technological lock-ins and high switching costs if foreign agencies try to rely on other surveillance technologies once NSA ones are established as standards. Secondly, through the profusion of its technologies, the NSA establishes standards within its surveillance networks which further enhance its capability to harvest foreign agencies' intelligence efforts, thus successfully externalising its intelligence operations. Lastly, network externalities entail that networks often grow at the expense of other networks, thus diminishing the other networks' influence and size. This thesis therefore presumes that the globalisation of surveillance with the U.S. at its centres has partially led to a decrease in power and capabilities of the Chinese and Russian intelligence agencies, as these are not part of the NSA surveillance network.

The partnerships maintained by NSA are contested in numerous ways. Firstly, while the NSA's closest partner, GCHQ has all the aspirations to become just as powerful in its capabilities as its American counterpart and observers understand that it might be the most aggressive Western intelligence agency (Greenwald 2014a). What can be observed here seems to constitute what could be understood as a race-to-the-top of different agencies which arguably is unsurprising in the volatile world of surveillance veiled by secrecy. Secondly, contested integration is found where network externalities push states to participate in NSA surveillance activities despite the fact that politically these states might not be closely aligned with the United States (Anderson 2014). Lastly, contested integration prevails where

partnerships seem like double-edged swords: The *Snowden leaks* have provided ample insights into how countries can form close partnerships while still aggressively spying on each other. It seems that *Five Eyes* membership provides a clear-cut demarcation line in this case. The German-American intelligence collaboration serves as but one example of how a partnering country of the NSA can still be subjected to intense NSA spying as only the *Five Eyes* countries seem to be spared of this (Walsh & Miller 2016, p. 349).

In essence, the NSA enjoys a hegemonic position on all different layers of the Internet. This view creates the general impression that *the Internet has always been a predominantly American venture*. The preponderance of the NSA is perhaps most obvious on the physical layer of the Internet where the overall geography of the Internet backbone in conjuncture with network effects in the relevant industries make it literally impossible for other countries to separate their Internet infrastructure from the reach of the NSA (Anderson 2014, p. 4). It is this hegemonic position that arguably justifies the focus of this thesis that mainly analyses NSA infrastructures: There is no doubt that the NSA is not the only powerful force in the world of surveillance and that the globalisation of surveillance is driven by a multitude of forces, many of which are far beyond the control of the NSA. And yet, the U.S. enjoys a hegemonic position within this secret world that is not matched by any other force in terms of funding, capabilities, reach and personnel. The NSA is understood to be among the most capable of agencies to penetrate the protocological layer of the Internet and at the same time constitutes the single most capable force when it comes to the penetration of the Internet backbone and the physical layer of the Internet more broadly. As such, the U.S. is arguably highly capable to uphold its hegemonic position in the future. This can be deducted from the many aspects of U.S. surveillance hegemony: The preponderance of American corporations within IT industries will not falter, neither will the U.S.-centred backbone structure of the Internet. Furthermore, participating in the U.S. surveillance hegemony remains beneficial to the participating states which most likely will not try to opt out of global surveillance networks erected under U.S. dominance. Lastly, it has been observed that while the *Snowden leaks* produced a global discursive *surveillance backlash* and enraged a considerable amount of ordinary citizens and lawmakers alike, the consequences of the *Snowden leaks* were predominantly general or specified concerns, but little action. Most surprisingly, despite broad-scale outrage and concern, 'the world of intelligence remains quasi-untouched by the scandals and has been moving even faster towards more globalised cooperation among western[sic] democracies [...] with the blessing and legitimising authority of new laws on surveillance' (Bigo 2016).

Who transfers policies and technologies?

As has been established, the globalisation of surveillance to a large degree is based on the transfer of policies and technologies. By *based on* I understand that the transfer of policies is a process integral to the globalisation of surveillance in as much as such transfers are both a *medium through which* globalisation processes are intensified *and rendered possible*. Here I emphasise once more that independent of a seemingly hegemonic constellation under which they occur, such transfers largely are mutual processes where both parties involved provide and receive certain goods, may they be of ideational, procedural, technological or legal kind.

The case example of the provision of XKEYSCORE from NSA to BfV through BND serves a fitting example for such processes. The NSA provides a surveillance technology and training in the use of this technology to foreign agencies. At the same time, technologies deployed by state actors present the embodiment of policies. Here, the embodied policy is the interception of flows of information based on chosen selectors. On the other hand, the foreign partner grants the NSA access to its legal jurisdiction and provides SIGINT. The scrutinised case does not provide clear evidence in how far BfV and BND take serious their mandate to share all relevant data to the maximum extent possible with the NSA and if intelligence on German citizens is included in this agreement. Ultimately, what BfV/BND equally provide is a workforce that takes part in the externalisation of surveillance operations. Murakami Wood demonstrates the way these transfers are intractably linked to the neoliberalisation of global governance. He argues that such transfers often lead to a decrease in accountability as it is difficult to trace back how technologies and policies spread among agencies, domestic and foreign, once established and commonly used. More cynically then, such transfer could also be referred to as *policy laundering* (Murakami Wood 2013, p. 322).

And yet, who *transfers* the policies and technologies in question? Here I introduce an interpretation of the globalisation of surveillance that concentrates not so much on the transfer of policies and technologies, but on the people behind these transfers. How can one grasp what has been coined *travelling technocrats*? To Larner and Laurie (2010, p. 219) such individuals are

> embodied actors who knowingly create careers for themselves through and against broader political-economic processes and national imaginaries. Relatedly, experts are increasingly moving between private, public and third sector organisations, and between local, national and international institutions, reshaping these accordingly. Finally, as different forms of expertise begin to travel so too do they mutate [...]'.

A close look at the biographies of such travelling technocrats reveals extraordinary careers of individuals that transcend different sectors and work as politicians, advisors, military

generals, academics, organisers in political organisations, etc. These are individuals that can be linked to trajectories of global expansion and integration and point to the fact that globalisation entails a multitude of contingencies created by the *people on the ground.* The abundance of leaked *Snowden files* that document conferences, meetings and mutual training sessions of different high-ranking officials from different partnering agencies speaks volumes to the notion that there are 'more actors involved in policy transfer than just the policy makers themselves' which 'points to the centrality of multiple and shifting forms of expertise in the reconfiguring of political-economic institutions, ideas and techniques' (ibid. p. 224). The actions of these socially complex actors are not solely based on the respective national intelligence agenda but they are also part of personal and professional individual trajectories as well as the influence of networks of common travelling technocrats whose identities and professional trajectories are often bound up with the policy positions and fixes [...] they espouse' (Peck and Theodore, quoted by Prince 2012, p. 194).

The perspective on travelling technocrats was first raised in connection with the emergence of global rule regimes and regulatory experimentation. These aspects seem to be interrelated as the travelling technocrats, often endowed with broad agendas that leave considerable space for individual interpretation are also among the actors most directly involved in policy experimentation. Likewise, their actions are often informed by and feed into evolving global rule regimes (ibid. p. 191 f.), which in the world of surveillance often are discursively linked to counter-terrorism. Alas, in the world of surveillance little is usually known about the individuals behind the enforcement of surveillance and the spread of its systems across different nations. In spite of that, the relevance of individual agency adds another dimension to the multidimensional world of globalising surveillance by emphasising the *multiplicity of actors* involved in global surveillance.

Lastly, this class of travelling technocrats can doubtlessly be linked to the Castells' interpretation of managerial elite directing the global spaces of flows using elaborate mechanisms of segmentation and disorganisation of the masses as main tools of social domination (see above). As with those elites, the travelling technocrats move along clear-cut demarcations of *ins* and *outs*:

> The more a society is democratic in its institutions, the more the elites have to become clearly distinct from the populace, so avoiding the excessive penetration of political representatives into the inner world of strategic decision-making (Castells 2010, p. 446).

Castells argues that the defining line between the elites and the populace consists of 'cultural codes [are] embedded in the social structure in such a way that the possession of these codes

opens the access to the power structure' (ibid.). While I support this analysis, I argue that in the world of surveillance the demarcation line between the elite and the populace is much easier to distinguish: Either one is endowed with the fitting security clearance or one is not. Secrecy and security clearances are among the most obvious and effective mechanisms baring a general populace from entering the world of surveillance.

Shadow Globalisation

On a final note I now turn to a recurrent theme of this thesis that so far has not been addressed explicitly: The prevalence of *state secrecy*. Bauman et al. (2014, p. 137) argue that part of the contemporary environment of (global) surveillance is an unchecked demand for secrecy on part of intelligence and security agencies which has enormous ramifications for the quality of democratic rule and modern statehood. Democracy, they argue, is theoretically tied to a *demos* with some kind of access to knowledge of certain quality (ibid). The *Snowden leaks* provide ample evidence for secrecy as a wide-spread practice whose use at times goes beyond common sense. The *secretive dimension* (Bigo 2016) of surveillance arguably is nothing new to surveillance (Lepore 2013). And yet it is an essential instrument in the globalisation of surveillance. To demonstrate this point I revise once more what has been established here about globalising surveillance and analyse if secrecy is involved. Firstly, an essential part of the work of the global surveillance assemblage is the duplication of data flows at interception sites with the original flows usually permitted to flow as intended and the duplicated flows steered at NSA (and cooperating agencies') processing sites. These flows are entirely secret which speaks volumes about the nature of the globalisation scrutinised here. Essentially, while Castells and others speak about spaces of flows and the importance of flows to contemporary capitalism, globalisation and the networked society, one has to acknowledge that there exists *a world of secret flows* that one knows only glimpses of. Secondly, this view is corroborated by the fact that the interception sites where the duplication of flows occurs, the nodes of the networks of secret flows, are highly secret themselves: Only with the necessary security clearance one can actually know of these sites. To the general populace, knowledge of such sites is rendered almost impossible. Consequently, the way surveillance becomes increasingly *glocalised* is mostly unknown to the spatial configurations within which this glocalisation takes place: Beyond the involved personnel and the security apparatus, hardly anybody in the region knew of the *Dagger Complex* until it was revealed by the *Snowden leaks*.

Furthermore, the institutional arrangements behind the scrutinised globalisation processes are equally a matter of secrecy. This entails the institutional composition of the NSA and that of

other agencies – and the notorious *black budget* it is financed with. Then of course there are the *partnerships* classified as secret. As a matter of fact it is not just the general populace of the concerned countries that are largely kept unaware of the surveillance collaborations, *but even the lion share of the political apparatus and the different branches of the respective states remains uninformed*. To prove this astounding fact, let us see how the NSA describes in an internal leaked document why the nature of its partnerships is 'usually insulated from short-term political ups and downs':

> For a variety of reasons, our intelligence relationships are rarely disrupted by foreign political perturbations, international or domestic. First, we are helping our partners address critical intelligence shortfalls, just as they are assisting us. Second, in many of our foreign partners' capitals, few senior officials outside of their defence-intelligence apparatuses are witting to any SIGIINT connection to U.S./NSA (Appendix 1: Third Party Relationships).

This quotation doubtlessly corroborates the aforementioned analysis of travelling (surveillance) technocrats who – endowed with the fitting security clearance – largely shape the nature of globalising surveillance while the remainder of the involved political bodies and concerned populations is largely kept unaware. I have therefore arrived at an astounding finding concerning the relationship between secrecy, surveillance and democratic governance: The motto of this thesis is provided by Jeremy Bentham scrutinising the possibility of knowledge and of political transparency when secrecy is employed (Bentham 1843, see Lepore 2013): 'This, then, is the reasoning of the partisans of mystery:—"You are incapable of judging, because you are ignorant; and you shall remain ignorant, that you may be incapable of judging."' *I argue that this argument is valid not only for the general populace but also for the majority of state-officials and lawmakers* in democratic societies where the demand for secrecy and the use thereof remains unchecked. It is not only the ordinary citizen who – if it was not for whistleblowers – is incapable of *knowing* what her state is involved in, but also members across the state's various bodies that are barred from knowing what core bodies of the state know and how they will act. The ramifications of this core-cutting quality of secrecy and surveillance for the state and its populace are manifold and, alas, cannot be scrutinised here. What is clear however is the fact that only a limited number of travelling technocrats and officials know the true extent of the surveillance apparatus and infrastructures which 'creates an overarching effect of dispersion that challenges the very idea of a reason of state conducted by a "state" in which the government determines national interests and national security and asks its own services to operate accordingly' (Bauman et al. 2014, p. 126, quotation marks used in original, original excerpt referring to slightly different context).

Ultimately entailed in this is a distinct quality of the here analysed form of globalisation which I at long last turn to now.

While there are different types of globalisation exhibiting different degrees of visibility, I essentially argue that state secrecy is the distinctive feature of the globalisation of surveillance which makes it stand out from other types of globalisation and I therefore suggest that the more catchy term *shadow globalisation* aptly describes this inherent and distinctive feature. Beyond doubt there are many processes of globalisation that only the trained eye can see: The emergence of tax-havens (Palan 2002), the externalisation of migration-control (Gammeltoft-Hansen 2010) and even the privatisation of warfare and the response to disasters (Klein 2007) stand out as fitting examples of hard-to-spot-out processes of globalisation. And yet, none of these processes are *secret* the way most aspects of globalising surveillance are classified as state secrets. State secrecy permeates almost all dimensions of this globalisation from the people involved (the travelling technocrats and the entire personnel with the respective security clearance), the infrastructures built and deployed, the spaces created and the intelligence produced. All this happens in the shadows and we, the general populace, are systematically barred not only from access but even from knowledge of the scrutinised processes. And yet, the emergence of surveillance studies and the increasing engagement with the globalisation of surveillance proves that this should not lead to discouragement, but rather serve as a powerful incentive for academics to work with the little we have, an endeavour this thesis humbly tried to pursue.

Conclusion

This thesis asked in how far NSA surveillance infrastructures evince an ongoing globalisation of surveillance and in what distinct ways globalising surveillance is being spatialised. The findings of this analysis can be summarised as follows: Firstly, emanating from a look at NSA infrastructures, the globalisation of surveillance has to be understood as a multidimensional phenomenon of partially converging, contested and paradox processes of integration and transfer of surveillance infrastructures, be it in the shape of policies, technologies, practices or personnel, whose trajectory unfolds predominantly *in the dark*, in contrast to other dimensions of globalisation. The globalisation of surveillance can be thought of as rhizomatic increases in dimensions of surveillance (here: in surveillance infrastructures and their interweaving) as the contingent dimensions expand the reach of the rhizome through interconnections and processes of de- and reterritorialisation. The notion of the *surveillant assemblage* therefore has to be amended with a scalar understanding that allows for a penetrative scrutiny of how

the surveillant assemblage operates on a global scale. For this reason, the notion of the rescaled, global surveillant assemblage was put forward here, for this notion adequately describes the manifold ways the complex expansionist trajectory of the surveillant assemblage both increasingly unfolds on a global scale and lies at the heart of the globalisation of surveillance.

Secondly, this globalisation produces new spatial configurations of surveillance across different scalar units to the degree that surveillance is becoming glocalised just as much as it is being globalised. As in other dimensions of globalisation, glocalisation of surveillance describes ambiguous processes where state-sovereignty and the notion of territorial rule is being reconfigured across different spatial units that form the basis of territorial fixities of otherwise fluid and saliently non-territorial forms. Nation-states, through their different spatial units, largely provide non-mobile and place-based factors within these global forms, such as access points to the Internet's physical infrastructures, or transportation and most crucially access to foreign jurisdictions. Most interestingly, this provision of place-based factors can occur wittingly (under the consent of the host state) or unwittingly. The concept of *glocalisation* is borrowed from analyses preoccupied with economic restructuring of urban configurations in Western Europe in times of globalisation, and therefore, while a useful analytical tool, the picture emerging from glocalising surveillance is markedly different from that of conventional glocalisation processes: Glocalising surveillance produces new spatial configurations where inconspicuous spatial units can form essential nodes of global surveillance networks as they are integral to particular surveillance infrastructures that are of pivotal importance to these networks. This circumstance furthermore informs the notion that the globalisation of surveillance is a heterogeneous phenomenon and surveillance and the infrastructures it is operated upon are not the same everywhere.

Thirdly, network externalities are powerful dynamics at work on multiple levels of globalising surveillance infrastructures, be it within IT industries or the physical infrastructure of the Internet, or within the growing NSA global surveillance network that leaves states with even less data-omnivore agendas with the dire choice of complicity vs. exclusion. Externalities that allow a given network to grow at the expense of other networks further informs the general conception of NSA surveillance hegemony that allows the NSA to set standards in terms of surveillance infrastructures and practices and to project its own technologies and infrastructures into the surveillance apparatuses of other states. It appears that network externalities lie at the heart of numerous dimensions of globalisation and surveillance is part of this development.

Fourthly, the globalisation of surveillance is largely built upon ambiguous liaisons between public and private actors. The digital economy doubtlessly forms the heart of the networked society. Within this societal configuration more and more data – and thus more and more power – is assembled in the hands of private corporations whose monopolies transcend industries and markets over land and sea. Not only has this new capitalist configuration rendered possible new forms of surveillance, but it has further allowed for an unprecedented compression of time and space *within* surveillance infrastructures and the externalisation of core state functions to non-elected actors that barely answer to the general populace and do not stand for elections. Surveillance is a multidimensional phenomenon embedded in cultural, social, political and economic frameworks. Therefore, each era has produced its own forms of intertwinement between capitalism and surveillance. Programmes such as PRISM seem to epitomise the contemporary intertwinement between big-data-oriented capitalism and state-sponsored surveillance.

Lastly, the dimension of globalisation scrutinised here remains a matter of secrecy that goes beyond the mere exclusion of the general populace and cuts to the core of modern statehood. This thesis finds that individual agency of a tiny elite of travelling technocrats of intelligence agencies plays a much underestimated role in the globalisation of surveillance which points to the multiplicity of actors involved in the globalisation of surveillance. The *Snowden leaks* provide ample evidence of how senior state officials across the globe proved ignorant of the extent of their respective intelligence agencies' operations and collaborations. The implications of this doubtlessly are manifold and raise justified concerns about accountability and transparency of democratic rule, the nature and stark centralisation of political power in the hands of a tiny elite – a notion that has been described as the 'dangers posed by a rogue national security state, operating in secret and without the knowledge of democratically elected officials' (Greenwald 2014b). It appears that the *partisans of mystery* have perfected their craft to a degree where even their own masters have become incapable of judging.

This last notion points to the fact that what might be emerging from the interweaving of globalising surveillance and state secrecy are new modes of state sovereignty. State secrecy as a technology of governance is at work on multiple levels and not only separates a surveillance-technocratic elite from the ordinary citizenry, but also serves to conceal emerging types of governementality that unfold both on a global scale and almost entirely outside of democratic elections and democratic participation. The surveillance state largely operates through and functions thanks to secrecy operating at a number of levels. While traditional understandings of sovereignty tend to emphasise notions of state-territoriality and

the formation of a *demos* willing to hand over its collective power (and use of violence) to the state, it appears that the surveillance state increasingly derives its sovereignty from the deployment of state secrecy as its key technology that seeks to facilitate the implementation of surveillance across multiple realms of surveillance and legitimise the exclusion of the ordinary citizenry from these crucial spheres of contemporary modes of (global) governance, biopolitics and state-sovereignty.

Unsurprisingly, the scrutiny of a largely secret object such as globalising surveillance raised more questions than it could answer, thus opening numerous alleys for future research. Several observers argue that the *Snowden leaks* and insights into prevailing surveillance programmes and surveillance environments evince the need for new concepts that allow for a refined understanding of surveillance and the globalisation thereof (Bauman et al. 2014; van der Velden 2015; Fuchs 2015; Lyon & Murakami Wood 2015). Here, this suggestion can only partly be sustained. This thesis has shown that on the one hand the possibilities to make use of prominent conceptualisations in surveillance studies are not exhausted yet. The (global) surveillant assemblage, societies of rhizomatic control and the protocological translation of such forms of control on the one hand provided useful tools for the study of surveillance, just as *glocalisation* and the *spaces of global flows in the networked society* did for the study of the globalisation of surveillance. It is therefore doubtful whether analyses on global surveillance are in need for novel *grand concepts* such as the panopticon or the surveillant assemblage to understand the globalisation of surveillance any better. However, this thesis has also shown that the study of globalising surveillance raises many a new issue predestined for future research.

To name but a few possible future research projects, I firstly concur with Fuchs (2013) that surveillance studies so far has shown a neglect of Critical Theory and the way Critical Theory can help understand the complex contemporary interweaving of surveillance, hegemony, media, political economy, ideology, the state – just as the role surveillance plays in contemporary class struggles. Fuchs' word of caution not to introduce new concepts and disciplines but to combine available conceptual with theoretical tools in order to avoid a further inflation of the object of study (ibid. p. 7) needs to be taken into consideration at this point.

Furthermore, this study has shown that there is no global homogeneity in surveillance environments, even as surveillance is globalising. The globalisation of surveillance produces new temporal and spatial configurations that are historically, socially, economically and

politically rooted (Murakami Wood 2009, 2014). As such, surveillance is conceptualised, exercised and perceived differently at different places. Consequently no single study can take this heterogeneity into account and what is needed is a multitude of studies scrutinising surveillance at specific places at specific times in history in order to create a more complete picture of how surveillance is being rescaled globally. I strongly concur with Murakami Wood (2009, 2012) who calls for explicitly non-Western studies of this globalisation – both in focus and in authorship – to add to Western-focused studies like this thesis in order to provide a yet more detailed picture of what surveillance looks like in the Global South, and elsewhere.

In addition to that, future research on the globalisation of surveillance should take into account the possible emergence of counter-movements opposing the globalisation of surveillance. Globalisation most generally has inspired counter-movements globally all across the political spectrum. Are we currently witnessing the emergence of anti-globalisation movements *within* the world of surveillance? I would argue that the TOR project can be understood as an incipient anti-globalisation of surveillance movement. TOR is both a free software client and the network the client connects with and serves the anonymisation of internet traffic by making use of the Onion Routing technology (González 2013, p. 74). Most interestingly, TOR makes use of technologies and organising principles encountered throughout this thesis: Data packets are encrypted into multiple layers and sent through a distributed network of multiple nodes or relays run by volunteers. In this network only the exit node can hand over the message to the requesting server while the list of possible nodes the data packets can transit through is taken from another node of the TOR network, namely the directory server. If a node fails for some reason, the data packet can be sent to any other node within the TOR network (ibid. pp. 74-77). Through encryption and multiple rerouting the origin of the original message is made anonymous. *Appendix 2: TOR hexagons* shows the (unfortunately uneven) global spread of this technology with nodes run by volunteers around the globe. Future research on projects like the TOR project should scrutinise whether we here find an anti-globalisation movement that seeks to counter globalised surveillance while – as anti-globalisation movements tend to do – making use of both the global infrastructures and network externalities the opposed globalisation is comprised of. Anti-globalisation movements often become *global* themselves and TOR seems to be an example of this. But even if not framed as an anti-globalisation movement, the TOR project can be understood to stand for what elsewhere has been termed *resilience in the surveillance context*: ‘the ability of people (individuals and groups) and organisations to adapt to and/or resist surveillance,

recognising that, while some forms of surveillance may be acceptable or tolerable, others pose a serious challenge to our fundamental rights' (Wright et al. 2015). The TOR project evinces the ambiguities often inherent to (global) techno-political movements. On the one hand it is often used in the pursuit of criminal purposes - a predominant realm of the *dark web* -; on the other hand it can be used to simply strengthen the protection of privacy and the right to anonymity on the Internet. Future research can therefore concentrate on projects such as TOR and analyse whether they qualify as forms of anti-globalisation movements or technological representations of the trajectory to increase resilience against surveillance.

On a final note, the perhaps most crucial aspect of future research on the globalisation of surveillance eludes the sphere of academics almost entirely: The act of whistle-blowing. Whether it is framed as *an act of treason* or understood as an integral part of democracy, a form of civil disobedience (Scheuerman 2014) or an *art de la révolte* (de Lagasnerie 2015) – whistleblowers enable us *to know* and resuscitate vital debates that cut to the core of contemporary societies. Perhaps one can think of whistleblowers as the epistemological equivalent of what has been termed *the exploit*: A hidden piece of software inserted into network structures that remains undetected until it enacts the disablement of the entire network (Galloway & Thacker 2007). Of course, whistleblowers seldom hope to bring down the very structures within which they operate, but they are part of a system – namely of unchecked secrecy – and remain unnoticed until they step forward and reach out to a respective audience. However, the fate whistleblowers face in most cases remains dire and gloomy for the price these individuals pay generally outweighs their personal benefits: While some may become exiled activists and pop-cultural icons, others, such as Chelsea Manning, end up incarcerated for decades, or persecuted relentlessly and mercilessly by Western and non-Western governments alike, while yet others face squalor, torture, assassination attempts, and death. The globalisation of surveillance apparently goes hand in hand with an unprecedented prosecution of whistleblowers across the globe. Nonetheless, these individuals step forward and risk everything in order to inform the ordinary citizenry. Without the acts of these individuals, this thesis and many other works by journalists and academics alike would not be possible. Their tenacity must be met with tenacious academic fervour.
May there be many more whistleblowers to come.

Appendices

Appendix 1: Third Party Relationships

Source: The Intercept 2014.

DYNAMIC PAGE -- HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET // SI / TK // REL TO USA AUS CAN GBR NZL

(U//FOUO) What Are We After with Our Third Party Relationships? -- And What Do They Want from Us, Generally Speaking?

FROM: the SIDtoday Editor and
NAME REDACTED FAD's Deputy Assistant for SIGINT Operations (DP1)
Run Date: 09/15/2009

(U//FOUO) We've posted articles recently examining specific NSA/Third Party relationships,* but today we'd like to step back and look at the big picture. What is NSA's underlying motivation behind its dealings with Third Party nations, and what approach do we use? To find out, SID*today* asked NAME REDACTED (pictured), from the SIGINT Operations Group in NSA's Foreign Affairs Directorate to answer a few questions. Here's what NAME REDACTED told us:

NAME REDACTED

- ***1. (U) Does NSA establish 3rd Party ties to meet specific short-term needs, or do we take a more long-term approach, thinking in terms of developing relationships over the course of decades, even though they may not bear fruit for some time?***

(S//SI//REL) We establish foreign partnerships to satisfy U.S. intelligence requirements. For specific short-term needs, it may be sufficient to work through CIA Chiefs of Station (CoS) at those locations where we do not have SIGINT partnerships established. Formal relationships require considerable resources, so if we can meet our objectives -- particularly short-term ones -- working through CIA, that's okay. If, on the other hand, our SIGINT exchanges increase in volume and/or complexity, or if a direct partnership is necessary because of Indications and Warning (I&W) considerations (i.e., we need rapid, direct exchange of information), then we will establish a formal SIGINT relationship, after DNI approval.

(C//REL) Many of our relationships have, indeed, spanned several decades, allowing us to establish higher degrees of trust with and reliance on one another. This, in turn, has led to greater levels of cooperation, where, for instance, NSA might be willing to share advanced techniques with a proven and reliable partner, in return for that partner's willingness to do something politically risky. Trust requires years to build up but it can be lost in a very short period of time.

- ***2. (U) What are we after, in general? Is it our partners' accesses, or their expertise on a specific target... or is it impossible to generalize, because it varies on a case-by-case basis?***

(C//REL) Yes, yes and... yes! Our partners' geography and access to high-priority target communications are a huge plus, as is their expertise on specific targets. With rare exception, they know their regional 'hoods better than we do and they exponentially add to our foreign language capability.

- ***3. (U) Are our foreign intelligence relationships usually insulated from short-term political ups and downs, or not?***

(S//SI//REL) For a variety of reasons, our intelligence relationships are rarely disrupted by foreign political perturbations, international or domestic. First, we are helping our partners address critical intelligence shortfalls, just as they are assisting us. Second, in many of our foreign partners' capitals, few senior officials outside of their defense-intelligence apparatuses are witting to any SIGINT connection to the U.S./NSA.

(S//SI//REL) There are exceptions, both on the positive and negative sides. For instance, since the election of a pro-American president, one European partner has been much more open to providing information on their own capabilities and techniques, in hope of raising our intelligence collaboration to a higher level. Conversely, another of our partnerships has stalled, due largely to that country's regional objectives not being in synch with those of the U.S.

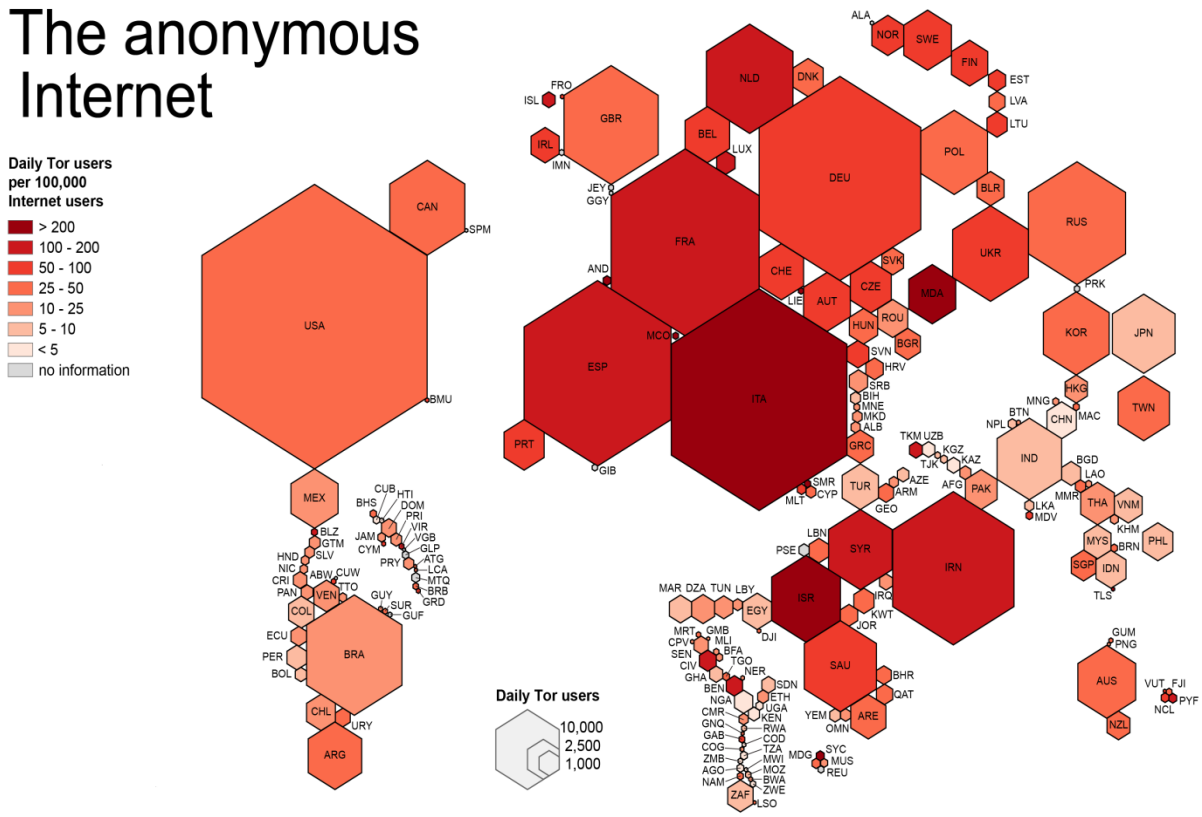
- ***4. (U) What do Third Parties typically want from us? What do <u>they</u> get out of the relationship?***

(S//SI//REL) Generally speaking, our Third Party partners want access to our technology, as well as our regional/global reach. In exchange for their providing unique accesses, regional analytical expertise, foreign language capabilities and/or I&W support, we provide them with technical solutions (e.g., hardware, software) and/or access to related technology. We must keep in mind that our partners are attempting to satisfy their own national intelligence requirements; with the exception of the assistance we provide during crises, we can only move our SIGINT relationships forward, when U.S. requirements intersect with theirs.

(C//REL) ...Thank you for the opportunity to describe some of our foreign partnering considerations. It's important for us to foot-stomp that FAD is an enabling organization. We do not conduct relationships in a vacuum; and our Country Desk Officers, front-end SIGINT Liaison Officers, Foreign Affairs Officers and staff are wholly committed to being in synch with -- or helping to synchronize -- SID, IAD, DIRNSA, DNI, the Under Secretary of Defense for Intelligence (USD(I)) and others in the Intelligence Community.

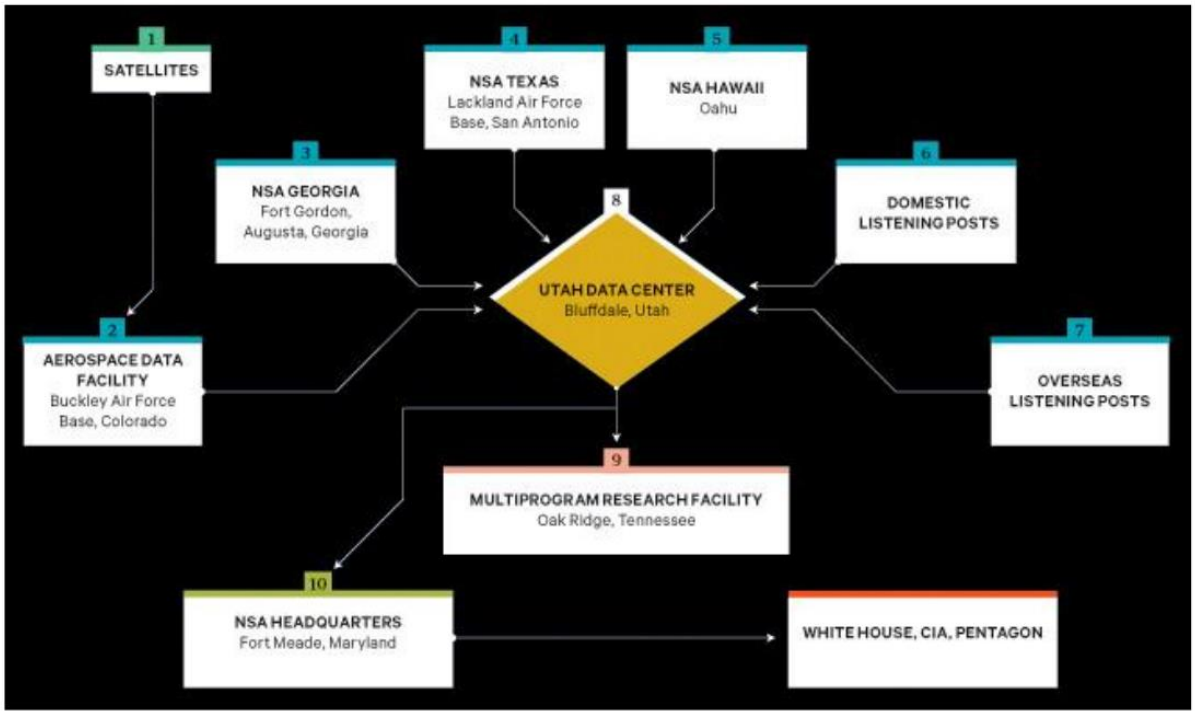
Appendix 2: TOR hexagons

Source: Oxford Internet Institute 2014.



Appendix 3: Nested NSA networks

Source: Jason Bamford, Wired Magazine, taken from Fichtner 2014, p. 75.



Bibliography

Academic journals and monographs:

Anderson, Ross (2001): *Why Information Security is Hard – An Economic Perspective.* Published in: Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual, pp. 358-365.

Anderson, Ross (2008): *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd Edition. Published online by Wiley. Last accessed April 7th 2016 at: https://www.cl.cam.ac.uk/~rja14/book.html .

Anderson, Ross (2014): *Privacy versus government surveillance: where network effects meet public choice*. Last accessed April 7th 2016 at: http://www.econinfosec.org/archive/weis2014/papers/Anderson-WEIS2014.pdf .

Anderson, Ross & Moore, Tyler (2009): Information security: where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society*, 367, pp. 2717-2727.

Austin, Lisa M. (2015): Lawful Illegality: What Snowden Has Tought Us about the Legal Infrastructure of the Surveillance State. In: Geist, Michael (ed.): *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: University of Ottawa Press.

Ball, Kirstie; Haggerty, Kevin D. & Lyon, David (eds.) (2012): *Routledge Handbook of Surveillance Studies*. New York: Routledge.

Baran, Paul (1964): On Distributed Communications Networks. *IEEE Transactions on Communications Systems*, 12(1), pp. 1-9.

Baran, Paul (2002): How packet switching works. *Pergamon Journal of the Franklin Institute*, 339, pp. 265-275.

Bauman, Zygmunt; Bigo, Didier; Esteves, Paulo; Guild, Elspeth; Jabri, Vivienne; Lyon, David & Walker, R. B. J. (2014): After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology*, 8, pp. 121-144.

Bauman, Zygmunt & Lyon, David (2013): *Liquid Surveillance*. Cambridge, Malden: Polity Press.

Beck, Ulrich (1986): *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Frankfurt am Main: Suhrkamp.

Bentham, Jeremy (1843): *Of Publicity*. In: The Works of Jeremy Bentham, vol. 2, Judicial Procedure, Ararchical Fallacies, works on taxation. Published under the Superintendence of his Executor, John Bowring. Edinburgh: William Tait, 1838-1843. Last accessed April 21st 2016 at <http://oll.libertyfund.org/titles/1921>.

Berry, David M. (2008): The Poverty of Networks. *Theory, Culture & Society*, 25(7-8), pp. 364-372.

Bigo, Didier (2010): 14 September 2001: the regression to the habitus. In: Dal Lago, Allesandro & Palidda, Salvatore (eds.): *Conflict, Security, and the Reshaping of Society*. Routledge Studies in Liberty and Security. New York: Routledge. Pp. 103-117.

Bigo, Didier (2016): The Möbius strip of national and world security. Retrieved from: www.mappingsecurity.net/blog/the-mobuis-strip-of-national-and-world-security/ (last accessed July 1st 2016).

Brenner, Neil (1997): Global, Fragmented, Hierarchical: Henri Lefebvre's Geographies of Globalization. *Public Culture*, 10(1), pp. 135-167.

Brenner, Neil (1998): Global cities, glocal states: global city formation and state territorial restructuring in contemporary Europe. *Review of International Political Economy*, 5(1), pp. 1-37.

Brenner, Neil (2004): Urban governance and the production of new state spaces in western[sic] Europe, 1960–2000. *Review of International Political Economy*, 11(3), pp. 447-488.

Brenner, Neil; Peck, Jamie & Theodore, Nik (2010): After Neoliberalization? *Globalizations*, 7(3), pp. 327-345.

Brown, Ian (2015): The feasibility of transatlantic privacy-protective standards for surveillance. *International Journal of Law and Information Technology*, 23, pp. 23–40.

C't – Magazin für Computertechnik (2014): TCP Stealth vs. Five Eyes. Mit Technik gegen staatliche Geheimdienst-Botnetze. *22*, pp. 170-174.

Canguilhem, Georges (2006): Die Position der Epistemologie muss in der Nachhut angesiedelt sein: Ein Interview. In: Schmidgen, Henning (ed.): *Wissenschaft, Technik, Leben.*, Berlin: Merve, pp. 103-122.

Castells, Manuel (2010[1996]): *The Rise of the Network Society*. Second edition with a new preface. Chichester, UK: Wiley-Blackwell.

Collier, Stephen J. & Ong, Aihwa (2005): Global Assemblages, Anthropological Problems. In: Ong, Aihwa & Collier, Stephen J. (eds.): *Global Assemblages: Technology, Politics, and Ethics as Anthropological Problems*. Malden, MA: Blackwell Publishing. Pp. 3-21.

Cooper, Russel & Madden, Gary (2008): Internet network externalities. *International Journal of Management and Network Economics*, 1(1), pp. 21-43.

de Goede, Marieke (2008): Beyond Risk: Premediation and the Post-9/11 Security Imagination. *Security Dialogue*, 39(2-3), pp. 155-176.

de Lagasnerie, Geoffroy (2015): *L'art de la révolte. Snowden, Assange, Manning*. Paris: Fayard.

Deleuze, Gilles (1992): Postscript on the Societies of Control. *October*, 59, pp. 3-7.

Deleuze, Gilles & Guattari, Félix (2005[1987]): *A thousand plateaus. Capitalism and Schizophrenia*. Minneapolis, University of Minneapolis Press.

DeNardis, Laura (2009): Protocol *Politics. The Globalization of Internet Governance.* Cambrige, MA: The MIT Press.

DeNardis, Laura (2012): Hidden Levers of Internet Control. *Information, Communication & Society*, 15(5), pp. 720-738.

DeNardis, Laura (2013): Multi-Stakeholderism: The Internet Governance Challenge to Democracy. *Harvard International Review*, 34(3), pp. 40-44.

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

DeNardis, Laura (2015): The Internet Design Tension between Surveillance and Security. *IEEE Annuals of the History of Computing*, April-June 2015, pp. 72-83.

DeNardis, Laura & Hackl, Andrea M. (2016): Internet control points at LGBT rights mediation. *Information, Communication & Society*, 19(6), pp. 753-770.

DiMaggio, Paul & Cohen, Joseph (2003): *Information Inequality and Network Externalities: A Comparative Study of the Diffusion of Television and the Internet*. Working paper #31 prepared for the Woodrow Wilson School, Princeton University.

Economides, Nicholas (2007): The internet and network economies. In: Brousseau, Eric & Curien, Nicolas (eds): *Internet and Digital Economics*. New York: Cambridge University Press. Pp: 239-267.

Fichtner, Laura (2014): *Scientia est Potentia: Techno-Politics as Network(ed) Struggles.* Master thesis submitted to the University of Twente.

Foucault, Michel (1995): *Discipline and Punish. The Birth of the Prison.* Translated by Alan Sheridan. New York: Vintage Books, Random House, Inc.

Frick, Jonas (2015): Kontrollgesellschaft. *GDI Impuls*, 3, pp. 76-80.

Fuchs, Christian (2013): Societal and Ideological Impacts of Deep Packet Inspection Internet Surveillance. *Information, Communication & Society*, 16(8), pp. 1328-1359.

Fuchs, Christian (2015): Surveillance and Critical Theory. *Media and Communication*, 3(2), pp. 6-9.

Galloway, Alexander R. (2001): Protocol, or, How Control Exists after Decentralization. *Rethinking Marxism*, 13(3-4), pp. 81-88.

Galloway, Alexander R. (2004): *Protocol. How Contol Exists after Decentralization*. Cambridge: The MIT Press.

Galloway, Alexander R. (2005): Global Networks and the Effects on Culture. *The Annals of the American Academy of Political and Social Science*, Vol. 597, pp. 19-31.

Galloway, Alexander R. (2006): Protocol. *Theory, Culture & Society*, 23(2-3), pp.317-320.

Galloway, Alexander R. (2011): Are Some Things Unrepresentable? *Theory, Culture and Society*, 28(7-8), pp. 85-102.

Galloway, Alexander R. (2012): Computers and the Superfold. *Deleuze Studies*, 6(4), pp.513-528.

Galloway, Alexander R. & Thacker, Eugene (2007): *The Exploit. A Theory of Networks*. Minneapolis: University of Minnesota Press.

Gammeltoft-Hansen, Thomas (2010): The Externalization of European Migration Control and the Reach of International Law. *European Journal of Migration and Law*, published by Brill. Pp. 1-23.

Gardeazabal, Javier & Sandler, Todd (2015): INTERPOL's Surveillance Network in Curbing Transnational Terrorism. *Journal of Policy Analysis and Management*, 34(4), pp. 761-780.

Gates, Kelly (2012): The globalization of homeland security. In: Ball, Kirstie; Haggerty, Kevin D. & Lyon, David (eds.): *Routledge Handbook of Surveillance Studies*. New York: Routledge. Pp. 292-300.

Georgieva, Ilina (2015): The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR. *Utrecht Journal of International and European Law*, 31(80), pp. 104-130.

Giroux, Henry A. (2015): Totalitarian Paranoia in the Post-Orwellian Surveillance State. *Cultural Studies*, 29(2), pp. 108-140.

González, Pablo Carballude (2013): Fingerprinting Tor. *Information Management & Computer Security*, 21(2), pp. 73-90.

Gregory, Derek (2011): The everywhere war. *The Geographic Journal*, 177(3), pp. 238-250.

Haggerty, Kevin D. & Ericson, Richard V. (2000): The surveillant assemblage. *British Journal of Sociology*, 51(4), pp. 605-622.

Haggerty, Kevin D. & Gazso, Amber (2005): Seeing Beyond the Ruins: Surveillance as a Response to Terrorist Threats. *Canadian Journal of Sociology*, 30(2), pp. 169-187.

Hall, Chris; Anderson, Ross; Clayton, Richard; Ouzounis, Evangelos & Trimintzios, Panagiotis (2011): *Resilience of the Internet Interconnection Ecosystem*. Paper presented at the Workshop on the Economics of Information Security.

Hall, Eric (2000): *Internet Core Protocols. The Definitive Guide*. Sebastopol, CA: O'Reilly

Harbisher, Ben (2015): Unthinking Extremism: Radicalising Narratives that Legitimise Surveillance. *Surveillance & Society*, 13(3/4), pp. 474-486.

Hardt, Michael & Negri, Antonio (2000): *Empire*. Cambridge, MA: Harvard University Press.

Kallus, Zsófia; Hága, Péter; Mátray, Péter & Gábor, Vattay (2011): Complex Geography of the Internet Network. *Acta Physica Polonica B*, 42(5), pp. 1057-1069.

Keiber, Jason (2014): *The Surveillance of Individuals in International Politics*. Dissertation. Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy in the Graduate School of The Ohio State University.

Keiber, Jason (2015): Surveillance Hegemony. *Surveillance & Society*, 13(2), 168-181.

King, Eric (2015): BILETA 2014 privacy and digital communications. *International Review of Law, Computers & Technology*, 29(1), pp. 4-15.

King, Gary; Keohane, Robert O. & Verba, Sidney (1994): *Designing Social Inquiry*. *Scientific Inference in Qualitative Research*. Princeton, NJ: Princeton University Press.

Klauser, Francisco (2013): Spatialities of security and surveillance: Managing spaces, separations and circulations at sport mega events. *Geoforum*, 49, pp. 289-298.

Klein, Naomi (2007): Disaster Capitalism. The new economy of catastrophe. *Harper's Magazine*, October, pp. 47-58.

Krogfoss, Bill; Weldon, Marcus & Sofman, Lev (2012): Internet Architecture Evolution and the Complex Economies of Content Peering. *Bell Labs Technical Journal*, 17(1), pp. 163-184.

Landau, Susan (2013): Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations. *Spotlight*, July/August, pp. 54-63. [Grammar mistake in original title]

Landau, Susan (2014): Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations. *Spotlight*, January/February, pp. 62-64.

Larner, Wendy & Laurie, Nina (2010): Travelling technocrats, embodied knowledges: Globalising privatisation in telecoms and water. *Geoforum*, 41, pp. 218-226.

Lelarge, Marc & Bolot, Jean (2008): Network Externalities and the Deployment of Security Features and Protocols in the Internet. *Sigmetrics'08*, June 2-6, pp. 37-48.

Lepore, Jill (2013): The Prism. *The New Yorker*, 2013: 32.

Liebowitz, S. J. & Margolis, Stephen (1994): Network Externality: An Uncommon Tragedy. *Journal of Economic Perspectives*, 8(2), pp. 133-150.

Lyon, David (2004): Globalizing Surveillance. Comparative and Sociological Perspectives. *International Sociology*, 19(2), pp. 135-149.

Lyon, David (2014): Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, July-December, pp. 1-13.

Lyon, David (2015): The Snowden Stakes: Challenges for Understanding Surveillance Today. *Surveillance & Society*, 13(2), pp. 139-152.

Lyon, David & Murakami Wood, David (2012): Security, Surveillance, and Sociological Analysis. *Canadian Review of Sociology*, 49(4), pp. 317-327.

Malecki, Edward J. (2002): The Economic Geography of the Internet's Infrastructure. *Economic Geography*, 78(4), pp. 399-424.

Mann, Michael (2008): Infrastructural Power Revisited. *Studies in Comparative International Development*, 43, pp. 355-365.

Margulies, Peter (2014): The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism. *Fordham Law Review*, 82(5), pp. 2137-2167.

Middell, Mathias (undated): De-territorialization and re-territorialization. Working paper distributed to the participants in the EMGS Master's programme.

Monahan, Torin (2011): The Future of Security? Surveillance Operations at Homeland Security Fusion Centers. *Social Justice*, 37(2-3), pp. 84-98.

Monahan, Torin (2012): Surveillance and terrorism. In: Ball, Kirstie; Haggerty, Kevin D. & Lyon, David (eds.): *Routledge Handbook of Surveillance Studies*. New York: Routledge. Pp. 285-291.

Mueller, John & Stewart, Mark G. (2012): The Terrorism Delusion: America's Overwrought Response to September 11. *International Security*, 37(1), pp. 81-110.

Murakami Wood, David (2009): The 'Surveillance Society'. Questions of History, Place and Culture. *European Journal of Criminology*, 6(2), pp. 1477-3708.

Murakami Wood, David (2012): Globalization and surveillance. In: Ball, Kirstie; Haggerty, Kevin D. & Lyon, David (eds.) (2012): *Routledge Handbook of Surveillance Studies.* New York: Routledge, pp. 333-343.

Murakami Wood, David (2013): What is global surveillance? Towards a relational political economy of the global surveillant assemblage. *Geoforum*, 49, pp. 317-326.

Murakami Wood, David & Coaffee, Jon (2006): Security is Coming Home: Rethinking Scale and Constructing Resilience in the Global Urban Response to Terrorist Risk. *International Relations*, 20(4), pp. 503-517.

Murakami Wood, David & Wright, Steve (2015): Editorial: Before and After Snowden. *Surveillance & Society*, 13(2), pp. 132-138.

Norris, Clive (2012): The success of failure: accounting for the global growth of CCTV. In: Ball, Kirstie; Haggerty, Kevin D. & Lyon, David (eds.): *Routledge Handbook of Surveillance Studies*. New York: Routledge. Pp. 251–258.

Nye, Joseph S. Jr. (2002): Globalization and American Power. In: Held, David & McGrew, Anthony (eds.): *The Global Transformations Reader*. Second edition. Hoboken (NJ): Wiley. Pp. 112-115.

Palan, Ronen (2002): Tax Havens and the Commercialization of State Sovereignty. *International Organization*, 56(1), pp. 151-176.

Penney, Jonathan W. (2016): Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal*, pp. 1-55. Last accessed April 28th 2016 at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645.

Price, David H (2014): The New Surveillance Normal. NSA and Corporate Surveillance in the Age of Global Capitalism. *Monthly Review*, 66(3), pp. 43-53.

Prince, Russell (2012): Policy transfer, consultants and the geographies of governance. *Progress in Human Geography*, 36(2), pp. 188-203.

Regan, Priscilla M. & Monahan, Torin (2014): Fusion Center Accountability and Intergovernmental Information Sharing. *Publius: The Journal of Federalism*, 44(3), pp. 475-498.

Reichert, Rámon (ed.) (2014): Big Data. Analysen zum digitalen Wandel von Wissen, Macht und Ökonomie. Bielefeld, Germany: transcript.

Sassen, Saskia (2005): The Global City: Introducing a Concept. *Brown Journal of World Affairs*, 11(2), pp. 27-43.

Sassen, Saskia (2012): *Cities in a World Economy*. Los Angeles: SAGE Publications, Inc.

Schmid, Gerhard (2014): Abhören in der Premiumklasse. *Zeitschrift für Außen- und Sicherheitspolitik*, 7, pp. 11-21.

Severson, Daniel (2015): American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change. *Harvard International Law Journal*, 56(2), pp. 465-514.

Sprenger, Florian (2015): Politik der Mikroentscheidungen: Edward Snowden, Netzneutralität und die Architektur des Internets. Lüneburg (Germany): meson press.

Shapiro, Carl & Varian, Hal R. (1999): *Information Rules. A Strategic Guide to the Network Economy*. Boston: Harvard Business School Press.

Star, Susan Leigh & Bowker, Geoffrey C. (2006): How to Infrastructure. In: Lievrouw, Leah A. & Livingstone, Sonia (eds.): *The Handbook of New Media*. Updated Student Edition. Thousand Oaks, CA: Sage. Pp. 230-245.

Thacker, Eugene & Galloway, Alexander R. (2014): Protokoll, Kontrolle und Netzwerke. In: Reichert, Rámon (ed.) (2014): *Big Data. Analysen zum digitalen Wandel von Wissen, Macht und Ökonomie*. Bielefeld, Germany: transcript, pp. 289-311.

Tranos, Emmanouil & Gillespie, Andrew (2011): The Urban Geography of Internet Backbone Networks in Europe: Roles and Relations. *Journal of Urban Technology*, 18(1), pp. 35-50.

van der Velden, Lonneke (2015): Leaky Apps and Data Shots: Technologies of Leakage and Insertion in NSA-Surveillance. *Surveillance & Society*, 13(2), pp. 182-196.

Verde Garrido, Miguelángel (2015): Contesting a Biopolitics of Information and Communications: The Importance of Truth and Sousveillance After Snowden. *Surveillance & Society*, 13(2): pp. 153-167.

Vinciguerra, Sandra; Frenken, Koen & Valente, Marco (2010): The Geography of Internet Infrastructure: An Evolutionary Simulation Approach Based on Preferential Attachment. *Urban Studies*, 47(9), pp. 1969-1984.

Walsh, Patrick & Miller, Seumas (2016): Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden. *Intelligence and National Security*, 31(3), pp. 345-368.

Weber, Jutta (2015): Keep Adding. On Kill Lists, Drone Warfare and the Politics of Databases. *Environment and Planning D: Society and Space*, 0(0), pp. 397-414.

Wright, David; Rodrigues, Rowena; Raab, Charles; Jones, Richard; Székely, Iván; Ball, Kirstie; Bellanova, Rocco & Bergersen, Stine (2015): Questioning surveillance. *Computer Law & Security Review*, 31, pp. 280-292.

Yong, Tan; Chiang, Robert & Mookerjee, Vijay (2006): An Economic Analysis of Interconnection Arrangement Between Internet Backbone Providers. *Operations Research*, 54(4): pp. 776-788.

Zook, Matthew (2009): Internet, Economic Geography. In: Kitchin, R. & Thrift, N. (eds): *International Encyclopedia of Human Geography*, 5, pp. 555-561.

Journalistic and NGO sources:

Bell, Emily (2013): The NSA files and the network effect. The modern leak needs a new kind of reporting, and news organisations are adapting by finding collaborations of scale. *The Guardian*. Available at: https://www.theguardian.com/world/media-blog/2013/dec/15/nsa-files-network-effect-journalism .

Currier, Cora (2016): NSA closely involved in Guantánamo interrogations, documents show. *The Intercept.* Available at: https://theintercept.com/2016/05/16/nsa-closely-involved-in-guantanamo-interrogations-documents-show/ .

Devereaux, Ryan; Greenwald, Glenn & Poitras, Laura (2014): Data pirates of the Caribbean. The NSA is Recording Every Cell Phone Call in the Bahamas. *The Intercept*. Available at: https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas .

Electronic Frontier Foundation (2006): AT&T's Role in Dragnet Surveillance of Millions of Its Customers. Internet Spying in San Francisco. Available at: https://www.eff.org/files/filenode/att/presskit/ATT_onepager.pdf .

Der Spiegel (2014): The Germany File of Edward Snowden Documents Available for Download. Available at: http://www.spiegel.de/international/the-germany-file-of-edward-snowden-documents-available-for-download-a-975917.html .

Gallagher, Ryan (2014): How Secret Partners Expand NSA's Surveillance Dragnet. *The Intercept*. Available at: https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/ .

Gellman, Barton & Soltani, Ashkan (2013): NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post.* Available at: https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html .

Greenwald, Glenn (2013a): NSA collecting phone records of millions of Verizon customers daily. Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama. *The Guardian*. Available at: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order .

Greenwald, Glenn (2013b): XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. *The Guardian.* Available at: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data .

Greenwald, Glenn & Ball, James (2013): The top secret rules that allow NSA to use U.S. data without a warrant. Fisa court submissions show broad scope of procedures governing NSA's surveillance of Americans' communication. *The Guardian*. Available at: https://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant .

Greenwald, Glenn & MacAskill, Ewen (2013a): NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Available at: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data .

Greenwald, Glenn & MacAskill, Ewen (2013b): Boundless Informant: the NSA's secret tool to track global surveillance data. *The Guardian.* Available at: https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining .

Greenwald, Glenn (2014a): *No Place to Hide. Edward Snowden, the NSA and the Surveillance State*. New York, Toronto, London: Penguin Books.

Greenwald, Glenn (2014b): Foreign Officials in the Dark about their own Spy Agencies' Cooperation with NSA. *The Intercept*. Available at: https://theintercept.com/2014/03/13/nsa-elected-officials-foreign-countries-unaware-countries-cooperation-us/ .

Hager, Nicky & Gallagher, Ryan (2015): Snowden revelations / The price of the Five Eyes club: Mass spying on friendly nations. *New Zealand Harald*. Available at: www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11411759 .

The Intercept (2014): Third Party Relationships. NSA document allegedly leaked by whistleblower Edward Snowden. Available at: https://theintercept.com/document/2014/03/13/third-party-relationships/ .

Khazan, Olga (2013): The Creepy, Long-Standing Practice of Undersea Cable Tapping. *The Atlantic.* Available at: http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/

Lee, Micah; Greenwald, Glenn & Marquis-Boise, Morgan (2015): Behind the Curtain. A Look at the Inner Workings of NSA's XKEYSCORE. *The Intercept*. Available at: https://theintercept.com/2015/07/02/look-under-hood-xkeyscore/ .

Lee, Timothy B. (2014): 40 maps that explain the internet. *VOX*. Available at: http://www.vox.com/a/internet-maps .

Lee, Micah & Williams, Margot (2016): The most intriguing spy stories from 166 internal NSA reports. *The Intercept.* Available at: https://theintercept.com/2016/05/16/the-most-intriguing-spy-stories-from-166-internal-nsa-reports/ .

Lindemann, Todd (2013): A connected world. *The Washington Post.* Available at: https://www.washingtonpost.com/apps/g/page/business/a-connected-world/305/

MacAskill, Ewan; Borger, Julian; Hopkins, Nick; Davies, Nick & Ball, James (2014): GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian.* Available at: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa .

Marquis-Boire, Morgan; Greenwald, Glenn & Lee, Micah (2015): XKEYSCORE: NSA's Google for the World's Private Communications. *The Intercept*. Available at: https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/ .

Miller, Greg; Tate, Julie & Gellman, Barton (2013): Documents reveal NSA's extensive involvement in targeted killing program. *The Washington Post.* Available at: https://www.washingtonpost.com/world/national-security/documents-reveal-nsas-extensive-involvement-in-targeted-killing-program/2013/10/16/29775278-3674-11e3-8a0e-4e2cf80831fc_story.html .

Müller-Maguhn, Andy; Poitras, Laura; Rosenbach, Marcel; Sontheimer, Michael & Grothoff, Christian (2014): Snowden Documents Indicate NSA Has Breached Deutsche Telekom. Treasure Map: The NSA Breach of Telekom and Other German Firms. *Der Spiegel*. Available at: www.spiegel.de/international/world/snowden-documents-indicate-nsa-has-breached-deutsche-telekom-a-991503.html .

Netzpolitik.org (2016): Live-Blog aus dem Geheimdienst-Untersuchungsausschuss: André Treuenfels und Ulrich Berzen vom Verfassungsschutz. Available at: https://netzpolitik.org/2016/live-blog-aus-dem-geheimdienst-untersuchungsausschuss-andre-treuenfels-und-ulrich-berzen-vom-verfassungsschutz/

Oxford Internet Institute (2014): Information Geographies at the Oxford Internet Institute. The anonymous Internet. Available at: http://geography.oii.ox.ac.uk/?page=tor .

ProPublica (2014): The NSA Revelations All in One Chart – Data. Available at: https://projects.propublica.org/nsa-grid/

Rensfeldt, Gunnar (2013): Read the Snowden Documents from the NSA. *Sveriges Television*. Available at: www.svt.se/ug/read-the-snowden-documents-from-the-nsa .

SPIEGEL ONLINE (2014): New Snowden Revelations on NSA Spying in Germany. New NSA Revelations: Inside Snowden's Germany File. Available at: www.spiegel.de/international/germany/new-snowden-revelations-on-nsa-spying-in-germany-a-975441.html .

ZEIT online (2015): NSA helps German domestic intelligence agency: XKeyscore - the document. Document pertaining to the agreement between the NSA and Germany's domestic intelligence agency BfV. Available at: www.zeit.de/digital/datenschutz/2015-08/xks-xkeystore-document .

Leaked files:

National Security Agency (2003): SID Around the World: The Rheinland. Alleged internal NSA file allegedly leaked by whistleblower Edward Snowden. Published by *Der Spiegel* 2014.

National Security Agency (2004a): TOR[terms of reference] log. Alleged internal NSA file allegedly leaked by whistleblower Edward Snowden. Published by *Sveriges Television* 2013.

National Security Agency (2004b): European Security Center to Begin Operations. Alleged internal NSA file allegedly leaked by whistleblower Edward Snowden. Published by *Der Spiegel*, 2014.

National Security Agency (2005): One-Year Anniversary for SUSLAG. Alleged internal NSA file allegedly leaked by whistleblower Edward Snowden. Published by *Der Spiegel 2014.*

National Security Agency (2007): US, German SIGINTers Increase Cooperation on African Targets. Alleged internal NSA file allegedly leaked by whistleblower Edward Snowden. Published by *Der Spiegel*, 2014.

National Security Agency (2011): TREASUREMAP Announces a New Release. Alleged internal NSA file allegedly leaked by whistleblower Edward Snowden. Published by *Der Spiegel*, 2014.

National Security Agency (2013a): FINAL Agenda SWEDUSA. Alleged internal NSA file allegedly leaked by whistleblower Edward Snowden. Published by *Sveriges Television.*

National Security Agency (2013b): VISIT PRÉCIS Hr. Dietmar B[name redacted], Director SIGINT Analysis and Production, German Federal Intelligence Agency (BND). Alleged internal NSA file allegedly leaked by whistleblower Edward Snowden. Published by *Der Spiegel*, 2014.

National Security Agency (2013c): NSA's Counterterrorism (CT) Relationship with the German Federal Intelligence Service (BND) and the German Federal Office of the Protection of the Constitution (BfV). Alleged internal NSA file allegedly leaked by whistleblower Edward Snowden. Published by *Der Spiegel*, 2014.

National Security Agency (undated): Bad guys are everywhere, good guys are somewhere! Alleged internal NSA file allegedly leaked by whistleblower Edward Snowden. Published by *Der Spiegel*, 2014.