Counter-Mapping Surveillance

A Critical Cartography of Mass Surveillance Technology After Snowden

van der Vlist, F.N.

Publication date
2017
Document Version
Final published version
Published in
Surveillance & Society

Surveillance & Society

Article

Counter-Mapping Surveillance: A Critical Cartography of Mass Surveillance Technology After Snowden

Fernando N. van der Vlist

University of Siegen, Germany; University of Amsterdam, The Netherlands.
fernando.vandervlist@uni-siegen.de

Abstract

This article critically examines mass surveillance technology revealed by Snowden's disclosures. It addresses that we do not only live in a society where surveillance is deeply inscribed but more urgently, that it is increasingly difficult to study surveillance when its technologies and practices are difficult to distinguish from everyday routines. Considerably, many of the technologies and systems utilised for surveillance purposes were not originally designed as proper surveillance technologies. Instead, they have effectively become surveillance technologies by being enrolled into a particular surveillant assemblage. Three contributions are made towards critical scholarship on surveillance, intelligence, and security. First, a novel empirical cartographic methodology is developed that employs the vocabularies of assemblages and actor–networks. Second, this methodology is applied to critically examine global mass surveillance according to Snowden. Multiple leaked data sources have been utilised to trace actors, their associations amongst each other, and to create several graphical maps and diagrams. These maps provide insights into actor types and dependence relations described in the original disclosed documents. Third, the analytical value of three ordering concepts as well as the logistics of surveillance are explored via notable actors and actor groups. In short, this contribution provides empirical cartographic methods, concepts, and analytical targets for critically examining surveillance technology and its particular compositions. It addresses challenges of resisting mass surveillance and some forms of data activism, and calls for the continuing proliferation of counter-maps to facilitate grounded critique, to raise awareness, and to gain a foothold for meaningful resistance against mass surveillance.

Introduction

Surveillance networking technologies have arguably lost their innocence after Snowden (Baumann et al. 2014; Lyon 2015). Snowden's disclosures regarding the United States' National Security Agency (NSA) in June 2013 have confirmed how prevalent information and computing technologies (ICTs) have become whilst surveillance has increasingly become hidden from view (Greenwald 2014; Harding 2014). As ICTs proliferate and permeate many distinct domains of social and human activity, a number of scholars and commentators have proclaimed the present era the post-industrial information age (Bell 1979; Lyon 1991; Webster 2006; Castells 1996–1998). Yet as several commentators have noted, it is also a surveillance society (Klauser 2013; Wood et al. 2006) in which surveillance increasingly hides itself from public view. As a result, issues related to the spatiality and politics of surveillance technologies and systems dealing with the generation, processing, tracking, monitoring, profiling, and sorting of information are still scarcely open to dispute and remain relatively understudied from an empirical or material point of view

van der Vlist, Fernando N. 2017. Counter-Mapping Surveillance: A Critical Cartography of Mass Surveillance Technology After Snowden. *Surveillance & Society* 15(1): 137-157.
http://library.queensu.ca/ojs/index.php/surveillance-and-society/index | ISSN: 1477-7487

(Klauser 2013; Lefebvre 2006). In the meantime, a new political economy of intelligence is emerging, the contours of which are difficult to identify due to official policies to keep relevant information secret (Crampton, Roberts, and Poorthuis 2013).

As David Murakami Wood argued in his review article situating Surveillance Studies through some of its leading practitioners (see Ball, Haggerty, and Lyon 2012; Hier and Greenberg 2007; Lyon 2007), there has been an obsession with technologies of surveillance and "new surveillance" (see Marx 1988, 2002, 2003) since the 1990s, whilst contemporary studies of surveillance from the late 2000s onwards have increasingly been concerned with the entanglements of surveillance and everyday life (2009: 57). Although much geospatial research has been done that utilises socio-technical theory from Latourian and post-Deleuzian approaches, relatively little empirical work has interrogated more recent developments such as geodemographics and consumer surveillance (ibid.), for instance with regards to a "surveillance–industrial complex" (Ball and Snider 2013; Hayes 2012; Stanley 2004). This research contributes thereto with a novel empirical cartographic methodology as well as by employing original empirical materials. Grounded in these methods and materials, a conceptual framework is proposed to address challenges inherent to resisting mass surveillance and particular forms of data activism (Milan and van der Velden 2016). Moreover, a dichotomy is revisited between top-down institutional forms of surveillance on the one hand (Lyon 1994, 2007), and bottom-up forms of inverse or counter-surveillance and "sousveillance" (Mann, Nolan, and Wellman 2003) that obtrude into the routine on the other hand. Instead, the aim is to understand the entanglement of these two forms by focusing on the milieus of relations that emerges between societies and practices by employing the logic of "pharmakon" (Ertuna 2009; Stiegler 2012, 2013). From this perspective, technical objects should always be understood as simultaneously remedy and poison, or as a source of resistance as much as exploitation. Surveillance technologies, consumer electronics, technological infrastructures, and computer databases render the individual exploitable by externalising knowledge whilst at the same time enabling them to deploy these technologies as a potential source of resistance. In this view, Snowden's disclosures have enabled a certain specific critical cartographic momentum by rendering discernible at least some of the many ways in which surveillance occurs in practice, and by providing insights into the global surveillance–industrial complex, enabling critical practitioners to produce maps that enable interventions and disruptions in the current state of affairs. Moreover, the disclosures present an opportunity to inventory what is known about these particular technological systems and to revisit existing theories and models as well as revisit strategic institutional and governmental alliances in light of these revelations.

In his critical theory of surveillance developed to examine the often intimate collaborations and burgeoning relationships between the market or private sector and state government for the development and implementation of surveillance systems, policies, laws, and standards, Ben Hayes has argued that the surveillance–industrial complex amounts to "several important theoretical assumptions about the corrosive nature of the state-corporate nexus on political culture, democratic governance and social control" (Hayes 2012: 167). Hayes provides three such assumptions: first, the complex intimate links between governments, state agencies, and the private sector or corporate world; second, the fact that governments outsource key aspects of security and surveillance practice to actors in the private sector that may benefit significantly from such relationships (e.g., software "backdoors" and "revolving doors" in this industry; c.f. Crampton, Roberts, and Poorthuis 2013; Murakami Wood 2013); and third, this is indicative of "a nexus so entrenched that it promises to deliver ever more pervasive, intrusive and effective surveillance technologies *in perpetuity*" (Hayes 2012: 167–168). As a "complex", this nexus of surveillance–industry relations consists of many distinct actors and is strategically positioned "at the heart of many of the transformations in population control, policing and intelligence gathering" (ibid.), while at the same time remaining largely out of public sight and only ever showing small bits and parts of itself without articulating the particularity of the parts in terms of their relationality. Such sites therefore remind of what Bruno Latour has termed "oligoptica" (2005: 181; Latour et al. 2012), which are defined in direct opposition to Michel Foucault's description of the "panopticon" (Foucault 1995). That is, oligoptica are

sites where one sees too little rather than too much. Moreover, they stand in stark contrast to models and strategies of surveillance that rely on internalising control, such as many CCTV systems in public spaces. Although this certainly complicates any attempt to map the surveillance–industrial complex, it also means that any successful map potentially challenges the actual power relations that sustain it in the first place.

Surveillance technologies and daily-used consumer electronics and services have become increasingly entangled with one another, yet it is also hard to determine when or where they actually overlap. In fact, as David Lyon points out, "[i]t is hard to pin down exactly who is conducting surveillance" (2015). This article therefore sets out to contribute a relational understanding of surveillance in action, grounded in a critical empirical cartography, and aims to complement more embedded analyses of surveillance. That is, rather than investigating specific instances of surveillance, the distributed logics and logistics of surveillance are examined through an analysis of how conditions, processes and relationships are (re)configured to condition and coproduce an "actual global surveillance" (Collier and Ong 2004). As Francisco Klauser has observed with regards to surveillance and the everyday, "Surveillance relates to, focuses on and projects itself into space, becomes inscribed there, and in the process contributes to the very production of the spaces concerned" (2013: 275). In order to address these challenges a critical methodological framework is developed that serves to facilitate resistance to mass surveillance. This article thus contributes to previous research in the areas of data activism, data countercultures, and tactics of resistance against surveillance and massive data collection (Milan and van der Velden 2016) whilst at the same time contributing to the development of "critical cartographies" (Crampton 2010) and digital research methods. The purpose is to take seriously the specificities present in the material arrangements of actors and their associations as sites of politics. This requires a sensitivity towards those very infrastructures that enable us to render the social perceptible, calculable, and surveillable in the first place (van der Vlist 2016). This point is especially urgent as many surveillance practices are built on top of web platforms or integrate off-the-shelf consumer electronics.

Mass surveillance is critically examined by bringing in original empirical materials, and as such provides a reality check for critical speculations about surveillance. The main goal is to examine mass surveillance technologies employed by the NSA in the surveillance programmes revealed by the Snowden leaks. It contributes to previous empirical research in this area, which has found that numerous NSA programmes can be classified in only a few categories of surveillance technology: wiretaps, PRISM, decryption, exploitation, analysis tools, and databases (Cayford, van Gulijk, and van Gelder 2014: 643). In recognition of the fact that many digital networking technologies operational in the "surveillant assemblage" (Haggerty and Ericson 2000; Murakami Wood 2013) overlap with those used in people's everyday routines (e.g., daily use of mobile devices, social media, and search engines largely controlled by a select group of very large American internet companies[1]) I argue for the need to revisit dichotomies of top-down institutional or state surveillance and bottom-up counter-surveillance in favour of a more productive view that departs from an understanding of their inseparability. This argument is developed over multiple sections. The first outlines an approach for operationalising a critical empirical cartography of the surveillant assemblage, employing the rich vocabularies of assemblages and actor–network theory. The second describes the methods and data sources used for this cartographic exercise and presents its outcomes. Specifically, it resumes the task of tracing actors and associations (Latour 2005). The objective is to derive empirical graphical maps that provide insights into the distinct actors and their relations among each other as they are described in original disclosed documents about mass surveillance and the NSA. Throughout the discussion that follows in the third and fourth sections, specific actors and associations are examined in detail while exploring the analytical value of modularity, functional

[1] Namely "GAFA", a shorthand referring to Google Inc., Apple Inc., Facebook Inc., and Amazon.com Inc., supplemented by a few others including Microsoft Corporation. Full company names are used throughout in order to make readers aware of the fact that each legal entity may comprise several subsidiaries and services owned by that entity.

dependency, and strategic alignment as three ordering concepts of surveillance as well as the logistics of surveillance. Finally, the conclusion outlines the main contributions for critical scholarship on surveillance, intelligence, and security and describes opportunities for further research.

Global Surveillance and Critical Cartography

Revelations about post-9/11 surveillance and intelligence practices, including the mass surveillance disclosures by Edward Snowden in June 2013, have repeatedly confirmed the existence of a suspected clandestine surveillance–industrial complex. In response to this mode of operation, the past decade has seen a number of efforts to leak, disclose or otherwise reveal details about surveillance and censorship technologies, signals intelligence exchanges, export and trade of technologies, and cyber-espionage (Appelbaum 2013; Appelbaum, Horchert, and Stöcker 2013; Haggerty and Gazso 2005; Kean and Hamilton 2004; Kruger and Haggerty 2006; Maurer, Omanovic, and Wagner 2014; Stanley 2004; Wagner 2012; WikiLeaks 2013). Such revelations allow critical commentators to raise questions and scrutinise the implementation, use, and abuse of networking technologies, devices, and software systems that partake in a "global surveillant assemblage" (Bogard 2006; Collier and Ong 2004; Haggerty and Ericson 2000; Murakami Wood 2013). At the same time, these revelations also highlight some of the dynamics of actual global surveillance. The contribution of this research to previous work in Surveillance Studies and related areas of scholarship, including investigative and data-driven journalism, data activism, and cyber-activism, partially lends itself to this point of departure. Namely, it provides novel ways of seeing enabled by Snowden's disclosures. Next, an approach is developed to allow for a critical cartographic analysis of this surveillant assemblage.

Assemblages and Actor–Networks

Assemblage theory has long been popular as an analytical framework for the study of surveillance. Murakami Wood's reading of the concept of "surveillant assemblage" extends the one pioneered by Kevin Haggerty and Richard Ericson (2000), who proposed to conceptualise surveillance through Deleuze and Guattari's concept of "assemblage" to make sense of the artifactual and hybrid quality of the control society that has become increasingly deterritorialised, operating instead as a network of heterogeneous elements that spread rhizomatically (Murakami Wood 2013: 319). Moreover, this surveillant assemblage is global in the sense that the proper scale for operations, decisions, and implications for political economy is now effectively global. The surveillance–industrial complex and the operations of the technological surveillance systems meet similar characteristics. Furthermore, several commentators have emphasised that it is important to realise that assemblages are never stable or in a static form; rather, "it is not the arrangement or organization but the *process* of arranging, organizing, fitting together" (Wise 2005: 77; c.f. DeLanda 2006). Assemblage-based analyses emphasise the heterogeneity of component elements and the specific "style of structuration" (Bennett 2010) through which particular formations hold together (Anderson et al. 2012: 174). The empirical cartographic analysis outlined in this article acknowledges this heterogeneity. In fact, it is argued to be of crucial importance to take into consideration how heterogeneous technological artefacts, software programmes, and systems are deployed to co-operate as technologies directed towards a common set of surveillance related objectives or interests. In turn, such insights invite further empirical analysis of the material specificities of these technologies. Additionally it is argued that modularity, as a guiding style of structuration, effectively reduces many of the problems associated with embedded systems that fail or require repair, maintenance, replacements, fixes, and updates (Graham and Thrift 2007).

Although approaches that engage with dynamism and relationality have proliferated over the recent years (Anderson et al. 2012), the value of assemblage theory lies in the study of processes of composition, distributed agency, and nonlinear forms of causality. Furthermore, Anderson et al. argue that "part of our attraction to assemblage thinking is that it does not point to any particular spatial imaginary. An assemblage approach demands an empirical focus on how these spatial forms and processes are

themselves assembled, are held in place, and work in different ways to open up or close down possibilities" (ibid.). As assemblages are continuously moving in their differential tendencies, and are therefore hard to trace and analyse empirically, this article draws on the complementary utility of actor–network theory (ANT) as developed by Latour (2005) and others. This move crucially allows one to operationalise a critical cartographic strategy to map the materiality and semiotic relationality of actors and the distinct networks in which they take part. Employing the theory of assemblages *vis-à-vis* critical cartography furthermore offers a practical workaround for the implicit risk of replacing assemblage as noun with assemblage as verb (Anderson et al. 2012: 174). In short, the value of utilising both vocabularies lies in developing an approach that is first and foremost grounded in an empirical cartography whilst being attentive to the rich conceptual nuances of assemblages as they have been used to study contemporary global surveillance.

Operationalising Critical Cartography

This article develops a "critical cartography" (Crampton 2010) of mass surveillance technology employed by the NSA. It aims to develop and employ a set of novel empirical cartographic methods and theoretical critiques grounded in critical theory. To this end the work of Jeremy Crampton in this area has been particularly instructive (2010). However it is one thing to draw the contours of a critical framework, and another to put it into practice. The methodological vocabulary of ANT is especially useful to operationalise a critical empirical mode of cartography sensitive to material and semiotic traces. In Latour's recasting of ANT the main task of the researcher is to follow "the actors themselves" (2005: 12) through "traceable connections", where sociality emerges and stabilises "against a much vaster backdrop of discontinuities" (ibid.: 245). Rather than producing a misguided, traditionalist "sociology of the social" based on *a priori* reductions of socio-spatial relations, this produces a "sociology of association" comprised of both human and nonhuman actors, and is open to emergent forms of causality. Moreover, Latour crucially differentiates between "mediators" and "intermediaries". While mediators actively translate or transform a given input into some other unpredictable output, intermediaries only transport meaning or force without transformation (ibid.: 39). Crucially, this proposition implies that agency is distributed among both human and nonhuman actors. This outlook thus questions what it means to make ontological distinctions between humans and nonhumans in the first place, instead inviting us to observe how their relations are patterned and structured (Anderson et al. 2012: 178). In other words, employing ANT for operationalising a critical cartography of the surveillant assemblage requires attending to distinct types of actors and stakeholders. The first task is then to create an inventory of actors and their associations in order to situate agency.

In order to develop a critical cartography of the NSA surveillant assemblage, this research relies on what is traditionally known to cartographers as a basemap. Basemaps provide a background setting with contours and details needed to orient the location or objectives of counter-maps. They are assumed "to ground the most fundamental, the most material, and, above all, the most physical reality", upon which journalists, anthropologists, economists, or others alike may impose their own perception of risks (November, Camacho-Lübner, and Latour 2010: 581). Accordingly, basemaps can be used to develop critiques and alternative maps (i.e., counter-maps) aiming to complement or even disprove mainstream or dominant narratives. As Crampton and others have pointed out with examples from the history of cartography and colonialism, "maps make space as much as they record space. This is quite literally 'map or be mapped'" (2010: 48; c.f. Bryan 2009; Rogers 2004; Stone 1998; Wainwright and Bryan 2009; Wood and Fels 2008). As such, counter-mapping questions what maps are for, the basis on which claims are made, and how maps are involved in such things as governance, geosurveillance, and identity construction. Once a basemap exists it can serve as a source of discussion, a reference for theory building, and a base for substantial critique. In this case the critique concerns a lack of attention paid to networking technologies and systems, especially regarding their co-operating as components part of larger constellations and towards achieving actual global surveillance. Therefore, rather than presenting an analysis or case study of isolated instances, I submit that many of these technologies gain a specific

meaning and purpose in relation to other actors in the network. That is, how they are directed to facilitate certain ends. In addition to focusing on specific actors like networking technologies and systems, it is equally important to consider how they are assembled, and indeed continuously disassembled and reassembled as new risks or threats develop.

Mapping NSA Advanced Networking Technology

Starting point for this mapping exercise of the NSA's advanced networking technologies and their configuration—itself being a subset of the larger surveillant assemblage as well as an entry point to analyse the surveillance–industrial complex—is a disclosed NSA/CSS Manual ("NSA/CSSM 1–52", dated "20070108", to be declassified on "20320108") that contains classified national security information. This catalogue of more than 50 pages includes detailed descriptions of technologies utilised by the Advanced Networking Technology division of the NSA's Tailored Access Operations (TAO) office for "computer network exploitation". TAO has existed since at least 1998 and is tasked to identify, monitor, infiltrate, and gather intelligence on computer systems in order to aid in cyber-surveillance and cyber-warfare intelligence gathering (Aid 2009). First published by *Spiegel Online*, the classified document includes descriptions about such things as gadgets and digital devices, software, hardware, projects and code names, their associated costs, launch dates and availability (Appelbaum 2013; Appelbaum, Horchert, and Stöcker 2013; NSA 2007, 2010). These distinct types of largely nonhuman actors are at the centre of this attempt to unravel the particular configurations of surveillance technologies.

As described below, many of these actors depend on other technologies and systems to achieve their goals. For example, software entities typically require quite specific hardware implants for active exploitation, and embedded hardware systems reversely require software for programmability and analysis. The objective is to map such relationships and dependencies between co-operating actors in order to rethink the configuration and impact of global surveillance. The first step is to follow the actors and their language as they appear in these disclosed documents. In addition to surveillance products, this also includes other types of actors. Second, this initial inventory of actors is appended with additional actors that appear in documents included in ACLU's NSA Documents database (Weinrebe 2014). Third, after mapping the relations between these products in accordance with the descriptions in the manual, it is possible to visualise and explore this complicated system of heterogeneous networking technologies. Furthermore, it should be noted that these technologies are utilised by the NSA as well as by their allies, especially members of the FVEY intelligence alliance[2] thus extending the capacities of this system far beyond US borders and jurisdiction. Since nearly all information about NSA surveillance technology is classified these disclosed documents are important for conducting this type of research and for developing an inventory of methods and devices employed for surveillance. Additionally there are numerous sources to draw from, not merely those leaked by Snowden. Snowden's disclosures represent just a portion of available knowledge and these leaks have been published across a multitude of media sources in various countries, thus rendering it more difficult to gather a meaningful ensemble (Cayford, van Gulijk, and van Gelder 2014). Although this research is not exhaustive it sketches the contours of a mass surveillance apparatus by providing analytical targets, useful concepts, and empirical methods for examining surveillance technologies and their compositions.

In total 240 distinct actors have been identified. These actors are densely connected by as much as 379 individual associations (i.e., averaging approximately 1.58 associations per actor). Within this network, at least five types of actors may be distinguished based on those found in the NSA/CSS Manual (Table 1; Figure 1). Most of all there are software entities (93), followed by hardware implants and gadgets (44), surveillance programmes (23), privately held companies (26), and human operators (17). In 37 cases the

[2] A post–Cold War alliance also known as "Five Eyes," comprising Australia, Canada, New Zealand, the United Kingdom and the United States, bound by the multilateral UKUSA Agreement.

actor type remains unclear from the descriptions in the source documents ("Unknown").[3] Especially for the first three categories (i.e., software entities, hardware implants, and surveillance programmes) all labels refer to secret code names used by the NSA. Although this network is largely composed of nonhuman actors, humans were found to be involved as operators, analysts, and special forces units such as those affiliated with the FBI and CIA. Interestingly, within this large-scale system, humans are not necessarily endpoints for data analysis or monitoring; rather, human actors may sometimes function as intermediaries, passing data along to another component or system without actually changing that data. Privately held internet companies were also mentioned frequently. These mentions sometimes refer to companies participating in the global surveillance industry (e.g., companies selling surveillance products to governments) but most often to internet-related companies and services explicitly targeted or exploited by the NSA. In case of the latter, mentions were found of open-source software initiatives such as Linux and Tor Browser as well as internet companies like Google Inc. and Facebook Inc. In this regard it is very interesting to get a glimpse of the kinds of companies that make allies or targets (either knowingly or unknowingly). Finally, mentions were found of several secret surveillance programmes, including the controversial "PRISM" programme, which function as umbrella programmes for gathering intelligence and are therefore typically centrally positioned.

Type	**Frequency**	**Description**
Software	93 (38.75%)	Secret code names for software entities. *Examples: "QUANTUMTHEORY", "IRATEMONKEY".*
Hardware Implant	44 (18.33%)	Secret code names for hardware implants and gadgets. *Examples: "COTTONMOUTH", "HOWLERMONKEY".*
Internet Company	26 (10.83%)	Privately held companies and corporations associated with the internet industry. *Examples: "Microsoft", "Tor".*
Surveillance Programme	23 (9.58%)	Secret code names for surveillance programmes. *Examples: "TURMOIL", "QUANTUM".*
Human	17 (7.08%)	Human operators, analysts, and special forces units. *Examples: "ROC", "FBI DITU".*
Unknown	37 (15.42%)	Not specified or unclear from source documents.

Table 1. *Overview of actor types, sorted by frequency count.*

Although the main data set for deriving this actor–network is the aforementioned NSA/CSS Manual, many of the codenamed products mentioned in it also appear in other disclosed documents. This provides an opportunity to append the initial inventory of actors and the associations among them. These other disclosured documents were made accessible through ACLU's NSA Documents, a queryable database hosted by the American Civil Rights Union, allegedly containing "[a]ll of the documents released since that day [June 5th, 2013]—both by the media and the government" (ACLU 2014). At that time, the database already comprised of 221 unique documents of different types, including internal slides and presentations, official reports to the United States Congress, and FISA Court orders and filings. This database was queried for each individual codename acquired from the NSA/CSS Manual so as to retrieve

[3] It is a deliberate decision to take a straightforward, naïve approach (Latour 2005) regarding the determination of actor types. That is, actor types are assigned solely on the basis of the observed empirical materials, and not on the basis of secondary materials and literature, hence resulting in a relatively large "Unknown" category. This category mainly includes minor actors.

additional information about each codenamed artefact and how it relates to others. Some new actors were encountered during this snowball sampling process. Although it is not the intention to be exhaustive in any way, this method does ensure that all trails from the starting point have been followed.

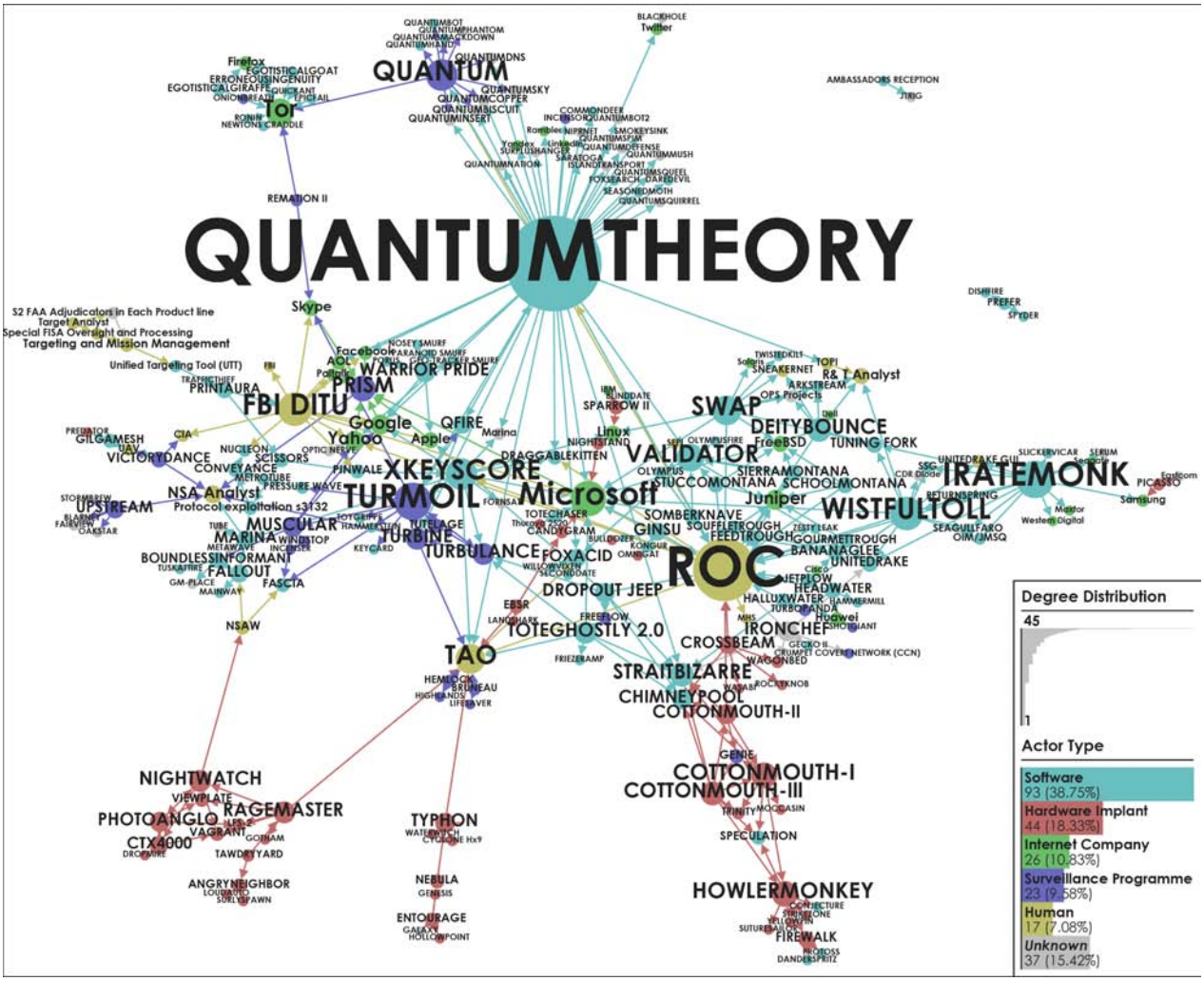

Figure 1. *Network diagram of the entire actor–network. Nodes represent distinct actors; edges are associations between those actors, based on traces found in the NSA/CSS Manual and ACLU's NSA Documents database. Nodes: 240; edges: 378; type: directed graph; filter: none. Node ranking: by degree; colour-coding: by actor type; layout: ForceAtlas2 (Jacomy 2011; Jacomy et al. 2012).*

After identifying distinct actors and their associations it is possible to further visualise and explore this particular actor–network of heterogeneous networking technologies. Figure 1 presents this actor–network in its entirety. Each node in this network represents a distinct actor and nodes are associated (i.e., connected by a directional edge) whenever two or more actors are, in one form or another, functionally dependent upon one another. These dependencies are determined based on in-text citations and diagrams found within the NSA/CSS Manual or ACLU's NSA Documents database. As a result, this map reveals unilateral relationships between actors, such as specific connections, sequences, and actor chains, as well as multilateral relationships such as alliances among actors that are jointly activated in the context of mass surveillance programmes. An example for the latter is "QUANTUM", a set of internet exploitation mechanisms focusing on malware and packet injection and collection that operate alongside "QUANTUMSKY", "QUANTUMCOPPER", and "QUANTUMSMACKDOWN" to name only a few (NSA 2010; Schneier 2015). Looking at the actor–network in its entirety, it is immediately striking to

observe the relative density of connections: there is a very strongly connected component in the centre (231 nodes) and only a small number of weakly connected components (3 nodes), with an average path length of 3.87 thus providing further support for the claim that most actors co-operate. Topologically speaking it is also interesting to find that software entities are much more likely to be positioned throughout the network (i.e., they tend to have high betweenness centrality scores) whilst hardware implants and gadgets tend to cluster together. This raises questions about which components are activated in particular instructions, operations, and programmes? In what sequential order, and for what purpose? Furthermore, since most associations are among nonhuman actors (79.63 per cent) it is intriguing to explore when humans are involved. Their involvement is typically described in terms of their role as operator, analyst (e.g., "R & T Analyst"), or even "man on the side" to oversee, manage, or feed through information. This is confirmed when a comparison is made between nodes ranked by in-degree or by out-degree (Figure 2). Whereas the first method shows actors with the highest *authority score*, or those receiving most relations, the second shows actors with the highest *hub score*, or those pointing towards most nodes (Kleinberg 1999). The former renders a view where humans and companies are highly centrally positioned, respectively as operators and targets, whilst the latter largely returns software and hardware implants whereby degree is more evenly distributed. Among humans alone, "ROC" (Remote Operations Center) and "TAO" (Tailored Access Operations) are most prominent when ranking by in-degree whilst "FBI DITU" (FBI Data Intercept Technology Unit) is most prominent when ranking by out-degree. Although this actor–network map presumably only represents the tip of the iceberg it already provides detailed insights into the topology, scope, scale, and reach of an sophisticated system of advanced networking technologies employed for surveillance. Next, the structure of this network will be explored in more detail.

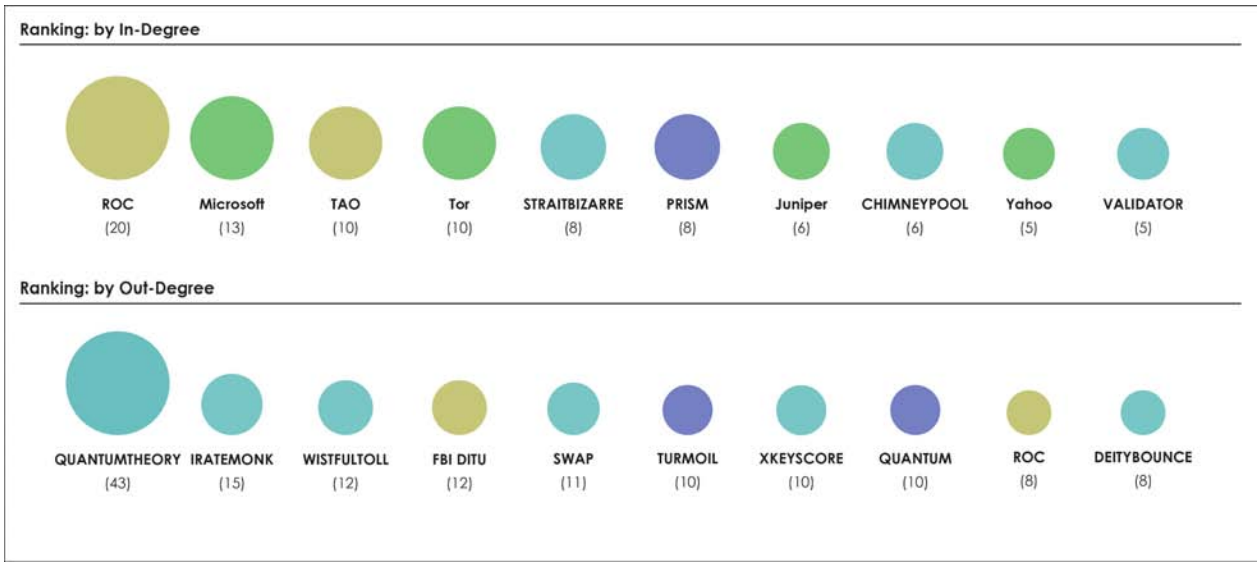

Figure 2. *Comparative bubble line diagram (small multiples) of top-ranked nodes, sorted by in-degree (upper) and by out-degree (lower). Filter: degree. Node scaling: by in-degree and by out-degree; sorting: by descending order; colour-coding: by actor type.*

Ordering, Strategy, and Heterogeneity

Global mass surveillance, conducted using myriad advanced networking technologies, may be understood as a patterned network of heterogeneous, interacting actors and materials (Law 1992). Throughout the discussion, the roles of certain specific actors and dependencies revealed by this actor–network map are examined by exploring the value of three ordering concepts or principles. These concepts I argue are crucial for the efficient, strategic, and reliable deployment of resources (e.g., computing and networking

technologies, big data storage and analytics capacities, and human resources). Based on the actor–network analysis, it is possible to distinguish at least three guiding ordering principles: modularity, functional dependency, and strategic alignment. Having produced an actor–network map enables zooming into and examining the significance of individual actors and alliances in terms of their properties as well as their relations. More specifically, in addition to considering properties and attributes of individual actors, the capacities of each actor or actor group are considered as a function of their associations, thereby distributing the agency of any individual actor. What can be learned from specific arrangements of actors into clusters or as part of chains?

Modularity

The first ordering principle of surveillance is *modularity*. According to Andrew Russell this concept describes "specific relationships between a whole system and its particular components" (2012: 257). In fact, it has a long and interdisciplinary history as an ordering concept and is a common strategy for the efficient organisation of information across disciplines. Modular structures are assemblages of actors, where individual actors may be entirely different from each other (i.e., in contrast to fractal structures, where all component parts have identical characteristics). Looking at the entire actor–network topology it is clear that most actors in this network co-operate and thereby form clusters like groups, chains, and alliances. Clusters enable individual actors to co-operate across scales: on a *micro-level scale*, such as engaging in pervasive surveillance and monitoring individuals, as well as on a *macro-level scale*, such as engaging in mass surveillance programmes, tasks, and processes. When smaller and larger scales of operation are linked, for example by a centralised database, it enables actors to move across scales, thereby facilitating intricate pervasive surveillance on a scale of entire populations or substantial fractions of populations. As an ordering principle, modular structures can thus be assembled, disassembled, and reassembled in any number of ways whilst retaining the separate identities of component parts (Baldwin and Clark 2000; Russell 2012). By themselves, these parts may be accessed, modified, or substituted without affecting the overall structure or whole system. This effectively distributes agency among associated actors, makes such a structure highly resilient, easily reconfigurable or replaceable, allowing for deletions or substitutions, or activating specific routines, while not activating others (Manovich 2001: 30–31). Moreover, drawing a computing analogy, modularity in ICTs allows for automated and self-sufficient conceptual modules such as (sub)routines, functions, procedures, and scripts (ibid.: 31). Similarly in case of organisations, a distribution of agency enables efficient, strategic, and reliable management and deployment of resources as well as enabling individual actors to diverge culpability to the whole system at any time. In other words, responsibility and accountability are not only distributed or dislocated, but rather *diffracted*, or spread out in varying degrees of spatio-temporal intensity. This is also crucial for any large-scale operation in order to manage a culture of secrecy within an organisation (Birchall 2016).

Functional Dependency

The second ordering principle is *functional dependency*. It describes a dependence relationship between or among particular actors, where one actor employs the capacities of another actor or actor group. As such, many individual actors, such as consumer hardware electronics and gadgets or social networking services, are only meaningful surveillance technologies insofar that they exist in relation to certain specific other components. Although each individual component has properties and attributes of its own, it is crucial to consider the ways in which additional capacities emerge in unanticipated ways as a function of its relations to other components in the assemblage. In this particular actor–network map, actors are associated whenever they are described in relation to another actor within any of the disclosed documents. This means that connections in this network are directed so as to describe dependence relations from one actor to another. In other words it generates hierarchies within the actor–network. These dependencies are typically *causal or logical dependencies* (e.g., specific sequences or chains of operations for data collection and monitoring) and *resource dependencies* (e.g., efficient use of limited computing resources for data storage and analytics). As a result of these functional dependencies it is important to make a

critical distinction between the properties or attributes of individual actors and the capacities they provide in relation to other actors. Whereas the former are knowable, finite and actual, the latter are potentially infinite and cannot be deduced from properties. As Manuel DeLanda writes in the context of assemblage theory, "capacities do depend on a component's properties but cannot be reduced to them since they involve reference to the properties of other interacting entities" (DeLanda 2006: 11; 2011). Furthermore, components can always be replaced, upgraded, or removed entirely, for example with a class of bugs known as persistent backdoors (PBDs). PBDs are implemented on target devices to gain and maintain access and to install software.[4] In addition, there are also physical hardware implants that then make sure that such a PBD will remain installed, even after a complete reinstall of the operating system or removal of a physical hard drive. As long as these PBDs are in place, new (tailor-made) software modules may be developed, upgraded, and implemented on a case-by-case basis. Thus it is not that an individual component's properties change, but rather that they potentially afford a broad range of capacities, enacted in particular events.

To illustrate, consider a simple off-the-shelf electronics product such as a monitor cable, available for online purchase to consumers in bulk. As individual artefacts, such products are clearly harmless and ubiquitous in their use, but product packages containing these artefacts may be intercepted for a process described as "interdiction", in order to implement software or hardware bugs that subsequently enables video signals to be transmitted to other system components. With the help of another bug called "RAGEMASTER", these signals can be transmitted as a continuous waveform and is subsequently "illuminated" by "PHOTOANGLO", and "remodulated" by "NIGHTWATCH" so that a human analyst may monitor and evaluate these signals. As these signals are transmitted to NSA headquarters they may be further logged, aggregated, stored, copied, fragmented, annotated, evaluated, or distributed. This is where a more familiar actor like "XKEYSCORE" (XKS) enters the assemblage (Figure 3). XKS is one of the widest-ranging systems and enables operators to index, search, retrieve, and analyse signals from remote servers or databases (Greenwald 2014; Lee 2014; Lyon 2015; Schneier 2015). In fact, it is a search engine designed to mine and sort much of this captured data. Analysts may employ XKS to construct a "fingerprint" in order to identify "targets" and even reconstruct impressions or profiles in retrospect using historical traces. The analyst may follow these data trails left behind by a target in real-time as databases are continuously updated. In this sense, XKS is first and foremost an organisational (sub)routine, a socio-technical procedure in which both human and nonhuman actors join forces (including a target).

Strategic Alignment

The third ordering principle is *strategic alignment*. In a general sense this concept refers to dependence relations established between internal and external actors and materials. Drawing on literature from organisation studies, it should be broadly viewed as encompassing not only resources within any particular organisation but also across organisations with complementary objectives. This includes forging social media and industry partnerships with key players and markets in the surveillance business (Hayes 2012) as well as repurposing the affordances of existing data sets or analytical devices towards mass surveillance. From a perspective of strategic information systems, Claudio Ciborra describes the concept as "the inherently dynamic fit between external and internal business domains, such as the product/market, strategy, administrative structures, business processes and IT" (1998: 10; 1997). He argues that "[i]t changes our representation of the interdependencies between some key business variables. We obtain a new 'geometrical' representation that materialises in front of our eyes the idea of 'alignment'" (ibid.: 11). As a graphical representation associating heterogeneous actors and materials, an actor–network map

[4] Backdoors to bypass normal authentication can be installed on devices such smartphones, laptops, routers, servers, phone towers, keyboards, monitors, to name only a few. Consequently, the data types that may potentially be acquired through this method could be anything: phone contacts lists, phone numbers and contact information, email traffic, SMS messages, voicemails, call logs, monitor video signals, keylogs, documents, live camera access, live microphone access, GPS or other radar-based geolocation, and more.

provides similar affordances. In fact, the concept helps to imagine how particular systems are utilising dependence relations in order to strategically orient themselves towards others thereby optimising human and other resources whilst minimising costs, risks, and waste. It is no coincidence that "PRISM" taps into resources from at least nine major internet companies. Not every relation is equal, which often has strategic implications, for example to gain a competitive advantage, circumvent or short-circuit legal accountability, or to influence public perception. Furthermore, strategic alignment provides unique ways to enquire how particular external governmental organisations and market institutions fulfill a role as repository to embed security or privacy in, or when they outsource such tasks to others (Agre 1999). This perspective could potentially benefit from other concepts like "core capabilities development" (Andreu and Ciborra 1996), which might be used to develop a critical perspective on the strategic instabilities inherent to using already-existing infrastructures, devices, formats, codecs, data types, data mining techniques, encryption and decryption methods, and pseudorandom-number generators, developed by public and private organisations. Indeed, such strategic instabilities can be targeted or utilised by activists.

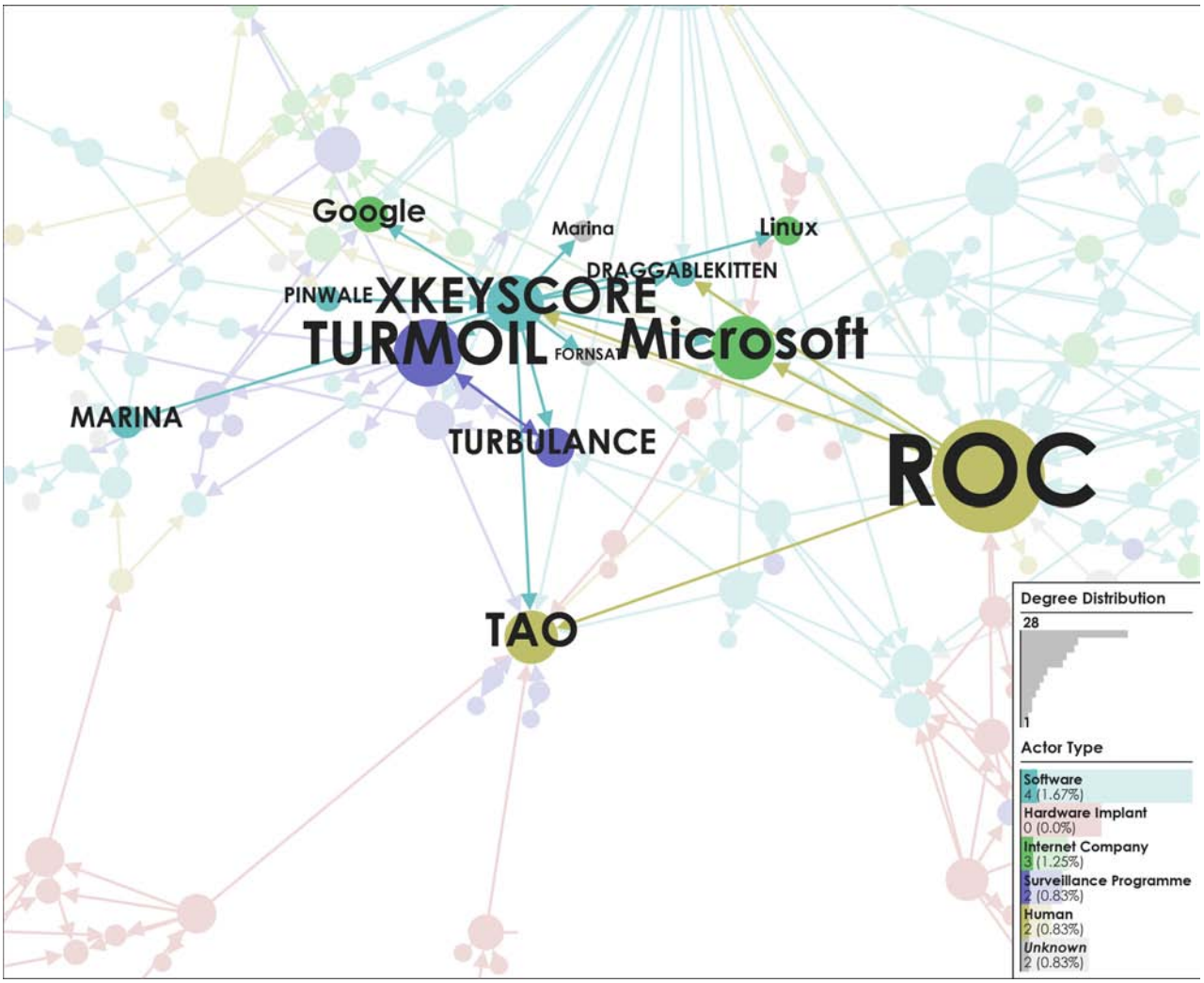

Figure 3. *Ego network diagram for "XKEYSCORE" (Software) showing its direct associations (zoom). Nodes: 13 (5.42% visible); edges: 17 (4.5% visible); type: directed graph; filter: topology (ego network, depth 1). Node ranking: by degree; colour-coding: by actor type; layout: ForceAtlas2.*

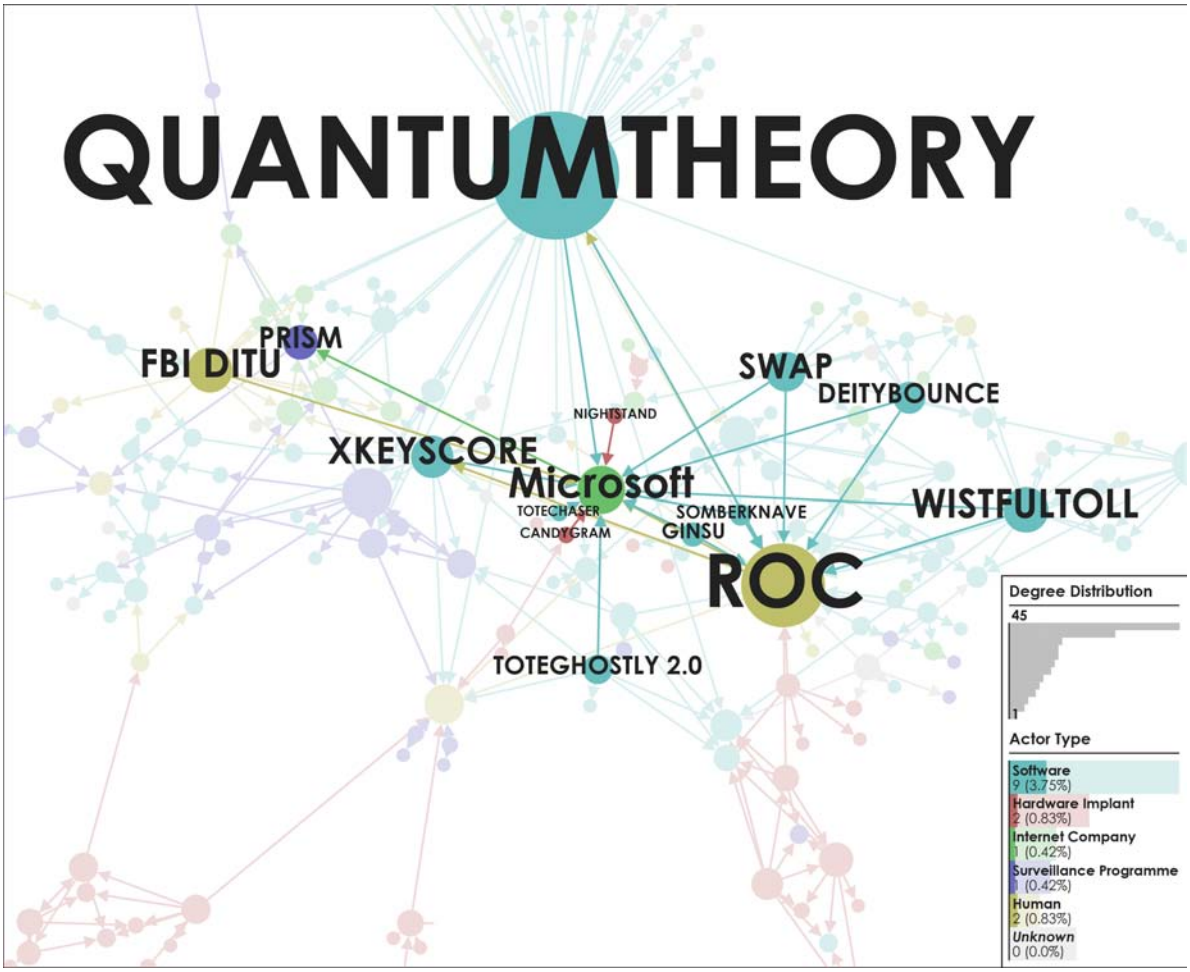

Figure 4. *Ego network diagram for "Microsoft" (Internet Company) showing its direct associations (zoom). Nodes: 16 (6.25% visible); edges: 22 (5.82% visible); type: directed graph; filter: topology (ego network, depth 1). Node ranking: by degree; colour-coding: by actor type; layout: ForceAtlas2.*

To illustrate the concept of strategic alignment, consider a major internet industry actor like "Microsoft" and its particular position within the actor–network (Figure 4). Like other companies, Microsoft Corporation co-functions with other actors in the context of "PRISM". This surveillance programme concerns legalised modes of access that the NSA has acquired to some of the largest internet companies (Greenwald 2014; Lee 2014; Lyon 2015; Schneier 2015). Even if the company is unwilling to co-operate, it is still legally bound to provide user data in some cases. Additionally, "Microsoft" also has other associations. For example, "NIGHTSTAND" is a hardware gadget used to implement a wire into a target device and is designed specifically for machines running Microsoft Windows. While companies like Microsoft Corporation are targets insofar they can extend the reach and scope of surveillance systems (i.e., extend the range of their capacities), they also claim to be unaware of these matters themselves. Co-functioning among actors can thus be the result of non-invasive exploitation methods. This also points to a more general observation that particular data-rich internet companies are strategically aligned as assets to acquire data through as well as to outsource storage for that data. Thus while Microsoft Corporation periodically updates its firewalls to secure the privacy of its users, the affordances for intelligence data collection enabled by secret backdoors built into their products potentially contributes to user privacy infringement. Consequently, responsibility and accountability are also diffracted unevenly among actors since not all actors in the network are equally responsible for exploiting the capacities of other assets. Similar profiles of association have been created for other large internet companies that appear in this

network (Figure 5a). Creating such profiles provides a detailed view of the different ways in which particular companies are integrated into this global surveillance system, or how they co-operate alongside other actors. Some companies are only associated with a single actor whilst others are associated with many more. Most companies are associated with software entities like "QUANTUMTHEORY" enabling non-invasive exploitation through software systems. Microsoft Corporation is most deeply integrated into the network, as evidenced by the number of associations it has to others. Additionally, Tor Browser and Skype (a Microsoft subsidiary) are associated with most surveillance programmes (namely three different programmes each). Similar associational actor profiles may be created to compare how surveillance programmes are aligned differently (Figure 5b). For example, "PRISM" is predominantly associated with internet company actors whilst "GENIE" is only associated with hardware implants and gadgets.

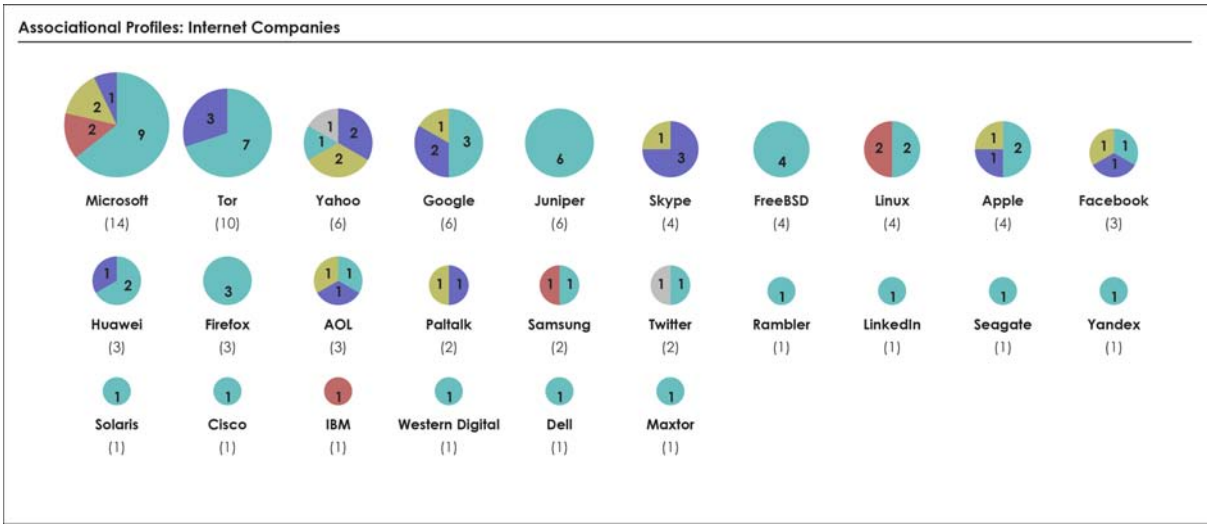

Figure 5a. *Comparative pie chart diagram (small multiples) of associational actor profiles per internet company, showing the distribution of co-operating actor types. Filter: attribute (Internet Company) and topology (ego network, depth 1). Node scaling: by degree; sorting: by descending order; colour-coding: by actor type.*

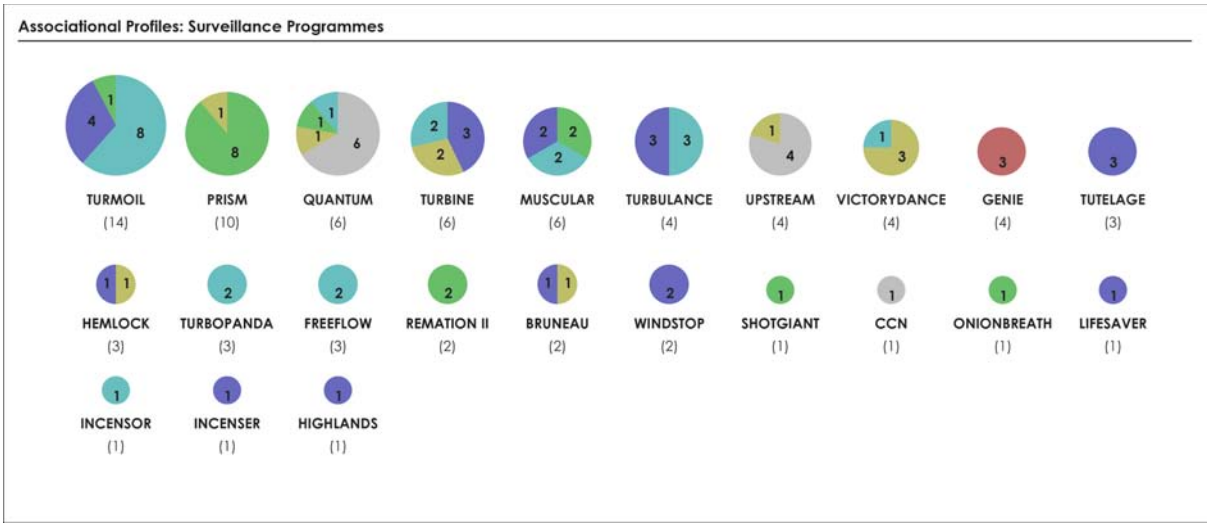

Figure 5b. *Comparative pie chart diagram (small multiples) of associational actor profiles per surveillance programme, showing the distribution of co-operating actor types. Filter: attribute (Surveillance Programme) and topology (ego network, depth 1). Node scaling: by degree; sorting: by descending order; colour-coding: by actor type.*

Logistics of Surveillance

Although actor–network analysis may be operationalised by means of critical cartography and network analysis, a purely distant, relational analytical approach would not do justice to the rich interactions between actors and materialities embedded in these networks. Therefore, taking these three concepts one step further, I briefly enquire into what may be termed the *logistics of surveillance* to examine some of the material repercussions of global surveillance.

As previously mentioned, most actors in this actor–network are software entities. This finding alludes to the point that we are witnessing traces of a particular logistics of surveillance. Namely, surveillance systems are tasked with detailed coordination of very large and complex operations involving many humans and other resources. It arguably reflects a broader "epistemic culture" (Knorr-Cetina 1999), which renders particular meanings and evaluations of media empiricism, analytical methods, objects, and social relations. What does it mean to treat digital media as the source for intelligence work in the first place? What is the intelligence value of "secondary social media" (DMI 2015), or those internet companies and services not targeted according to disclosed documents? Such questions directly concern the inseparability of a target, or the "observed object" of surveillance, and the "agencies of observation" (Barad 1998: 96) deployed within the surveillant assemblage. As a result, critiques should concern technologies and systems of the NSA as well as technologies and systems of external companies. The amount, reach, and scope of these external agencies of observation only grows as the number of internet users and their time spent online grows. Similarly it is crucial to consider specific hardware implants and software entities as component parts, co-operating as part of a heterogeneous system. Consequently, regardless of most actions taken in response to surveillance like encryption or anonymisation, skilled analysts can often correlate anonymous data points with other data sets in order to de-anonymise with reasonable statistical certainty.

In many cases similar rationales apply, namely determining a specific target, then infecting or bugging devices used by that target, and then generating or retrieving additional data about that target. In other cases software may be deployed to disrupt entire computer network systems, such as with distributed denial-of-service (DDoS) attacks or by installing malware. To illustrate, "QUANTUM" is a strongly connected surveillance programme, spanning across multiple clusters. According to *The Guardian* it is in fact "the one topsecret program the NSA desperately did not want us to expose" (Schneier 2015: 149). Among other things it relies on packet injection (Greenwald 2014; Lee 2014; Lyon 2015; Schneier 2015) and techniques for monitoring users' cookies that have already been implemented on their devices by other internet companies and services, but uses them as coordinates for attacks. Some techniques rely on employing already existing "software sorted" data spaces (Wood and Graham 2006), pre-configured with specific data types and categories as encoded in ordinary cookies that carry metadata about ordinary users of online services. Mundane functional elements thus facilitate intricate pervasive surveillance, while costly and demanding tasks like implementation, storage, and accountability strategically reside with market institutions. Moreover, it underlines the claim that the "agency of observation" resides at least partially in these market institutions. This means that the object of Surveillance Studies also extends into these institutions and their industries. Moreover, once powerful systems like "QUANTUM" have been developed and exposed they cannot be contained and will thus likely be deployed by other intelligence agencies.

Although this partial outsourcing of the logistics and burden of surveillance is highly efficient and secure on the side of the watchers it seems to exacerbate problems for those being watched. Perhaps most significantly there are problems associated with what Louise Amoore has termed "data derivatives", such as a risk flag or score derived from an "amalgam of disaggregated fragments of data, inferred from across the gaps between data and projected onto an array of uncertain futures" (2011: 24). As this global surveillant assemblage keeps growing in size, the data derivative increasingly serves as a "differential

curve of normality" (ibid.; Foucault 2007; c.f. van der Ploeg 2003, 2012), itself indifferent to people, places, and events whilst projecting outcomes and prescribing courses of action based on what may be inferred about them. Consider the aforementioned XKS. As a computer system for search, retrieval, and analysis it requires input from human analysts to assemble data points and define a "fingerprint". However, "fingerprints" may also be calculated and suggested automatically based on predefined risk profiles. For example, "TURMOIL" allows deep packet inspection for filtering and locating potential targets and executes similar operations in a fully automated manner. Furthermore, the disclosed documents also refer to multiple kinds of targets, both humans (e.g., terrorists, ministers, and system administrators) and nonhumans (e.g., information, cookies, machines, devices, and networks). From this perspective the logistics of surveillance do not only act upon representations of targets but especially also participate in producing new subjectivities.

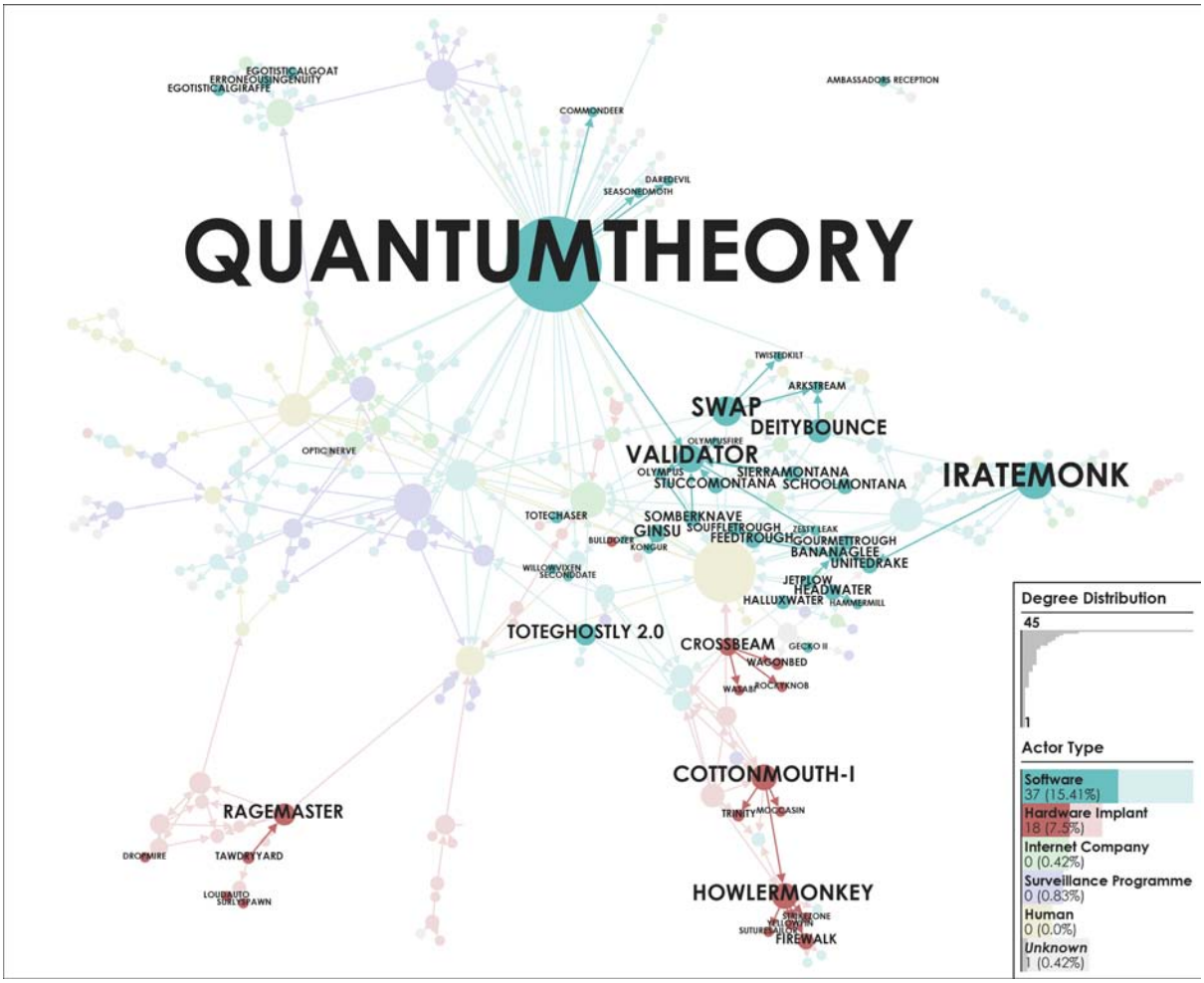

Figure 6. *Network diagram for actors associated with "interdiction" or "remote access". Hardware implants and gadgets are highlighted where interdiction is required; software entities are highlighted when remote access is required for implementation. Nodes: 56 (23.33% visible); edges: 36 (9.52% visible); type: directed graph; filter: attribute. Node ranking: by degree; colour-coding: by actor type; layout: ForceAtlas2.*

Finally, the devices, hardware implants, embedded systems, and software implementations used to capture data about targets are most often implemented via remote access or "interdiction" (Figure 6).[5] In case of hardware implants, interdiction refers to modifications of a target device at some point during logistical

[5] Interdiction is a process to intercept and prevent certain behaviours or action possibilities on the side of the target.

transport by attaching additional technologies onto an off-the-shelf device. Such an operation not only intercepts but actually disrupts, relays, or reroutes existing logistical patterns. In case of software implementations, remote access is typically acquired to target machines. Both forms of interdiction occur for instance with "BULLDOZER" and "GINSU". As long as "BULLDOZER" is physically attached to a device, rebooting the system will initiate a (re)installation of "GINSU", enabling "BULLDOZER" to transmit signals to "ROC". Although remotely controlled, both processes depend on interdiction.

Conclusion

The main argument developed throughout this article is not just how it is that we live in a society in which surveillance is deeply inscribed but more urgently, how one can proceed to study surveillance, intelligence, and security when their technologies and practices are increasingly difficult to distinguish from everyday routines—when surveillance has become something we live in on a daily basis. If surveillance technologies and daily-used consumer electronics and services have indeed converged to a large extent it is urgent to acknowledge the logic of "pharmakon", namely that the very same technologies serve simultaneously as source of exploitation and resistance. It has thus addressed challenges inherent to resisting mass surveillance and to some forms of data activism, and calls for the continuing development of critical cartographic methods to facilitate the proliferation of grounded critiques and alternative maps. As such it challenges an existing dichotomy of institutional or state surveillance one the one hand and various forms of inverse or counter-surveillance and "sousveillance" on the other hand, in favour of a more productive view that departs from their inseparability.

In order to develop this main argument at least three important contributions have been done towards critical scholarship in the areas of surveillance, intelligence, and security studies. First, a novel critical empirical cartographic methodology has been developed within this article. The approach employs the vocabularies of assemblages and actor–network theory in order to operationalise "critical cartography" for present purposes. Second, this methodology has been applied to critically examine global mass surveillance according to Snowden where multiple leaked data sources have been utilised to trace actors and their associations. To present the outcomes multiple graphical maps and diagrams have been produced, which provide insight into distinct actors, their types, and associations among each other as described in the original disclosed documents about the NSA. Although this particular actor–network might only represent the tip of the iceberg of surveillance it does provide insights regarding the topology, scope, scale, and reach of a sophisticated system of advanced networking technologies employed for surveillance. Significantly, one realises that many of the technologies and systems utilised for surveillance purposes were not originally designed as proper surveillance technologies. Instead, by being enrolled into this particular surveillant assemblage they have effectively become surveillance technologies. For this reason it is important to consider surveillance technology not merely *in situ*, as materially embedded in specific sites, but *in actum* as enacted by their very functioning as part of surveillant assemblages, with particular co-operating actors, input signals, and data sets. Third, a number of distinct actors and actor groups within this network have been examined in more detail whilst exploring the analytical value of three ordering concepts as well as the logistics of surveillance. Regarding the former, the concepts of modularity, functional dependency, and strategic alignment are useful for understanding how a set of diverse, heterogeneous networking technologies interact to achieve an efficient, strategic, and reliable deployment of ICTs, big data storage and analytics capacities, and human resources. Significantly, these ordering principles enable strategic outsourcing of some of the burdens of intelligence (e.g., computational resources, costs, responsibility, innovation) to industry actors such as very large internet companies. In other words, it exacerbates issues related to the corrosive nature of the state–corporate nexus, or the "surveillance–industrial complex". Moreover, based on different ways in which privately held internet companies are enrolled by the surveillant assemblage it is clear that there is more to this than just forced compliance. Identifying dependence relations instead provides a more productive account whereby different forms of exploitation and co-operation may be distinguished. Indeed, the cartographic

methodology developed in this article enables researchers to numerically quantify the types and strengths of each individual association among actors and perform calculations with path-based distance metrics in order to further nuance direct or indirect, implicit or explicit, strong or weak, and knowing or unknowing forms of co-operation. As a result we also require a more nuanced understanding of accountability in relation to these technologies and systems. Rather than concentrating on single actors, accountabilities are multiple and distributed across actors or actor groups.

This contribution thus provides analytical targets, concepts, and empirical cartographic methods for examining surveillance technologies and their composition. Further research could examine individual actors and actor groups in much more detail, linking to existing knowledge about these technologies and systems or linking to disclosed documents about other security agencies. This would yield insights into the intricacies of specific surveillance technologies and subsystems, related debates on how big data and the internet of things intensify surveillance with networked technologies (Lyon 2014), and ground some technologies geographically. The maps provided in this article could serve as basemaps for those research projects. Additionally the roles and types of actors could be explored as they change over time, for example in response to specific events or leaks. How has the topology of this particular actor–network changed since mid-2014? What may be learned about the broader intelligence community?[6] For such reasons it is important to continue developing critical cartographies and facilitate the proliferation of counter-maps. Maps may not only be represented graphically as networks—as in this article—but they may also be simple descriptions of logistical trajectories including hardware implants that capture specific signals, centralised databases, analytical software modules, and real-time human decision making. Thus, counter-maps are productive in raising awareness and gaining a foothold for meaningful resistance against mass surveillance.

Acknowledgements

I would like to thank Pascal Janssens and Wannes Sanderse as well as Rik van Eijk and Ezgi Akdağ for their research assistance during previous stages of this project. Additionally I would like to thank Esther Weltevrede, Anne Helmond, the editors, and the anonymous reviewers for their constructive critical comments on previous versions of the article manuscript.

References

Agre, Philip E. 1999. "The Architecture of Identity: Embedding Privacy in Market Institutions." *Information, Communication & Society* 2 (1): 1–25. doi:10.1080/136911899359736.

Aid, Matthew M. 2009. *The Secret Sentry: The Untold History of the National Security Agency*. New York: Bloomsbury Press.

American Civil Liberties Union (ACLU). 2014. "NSA Documents | American Civil Liberties Union." *American Civil Liberties Union*. https://www.aclu.org/nsa-documents-search.

Amoore, Louise. 2011. "Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times." *Theory, Culture & Society* 28 (6): 24–43. doi:10.1177/0263276411417430.

Anderson, Ben, Matthew Kearnes, Colin McFarlane, and Dan Swanton. 2012. "On Assemblages and Geography." *Dialogues in Human Geography* 2 (2): 171–189. doi:10.1177/2043820612449261.

Andreu, Rafael, and Claudio U. Ciborra. 1996. "Organisational Learning and Core Capabilities Development: The Role of IT." *Journal of Strategic Information Systems* 5 (2): 111–127. doi:10.1016/S0963-8687(96)80039-4.

Appelbaum, Jacob, Judith Horchert, and Christian Stöcker. 2013. "Shopping for Spy Gear: Catalog Advertises NSA Toolbox." *Spiegel Online*, December 29. http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.

Appelbaum, Jacob. 2013. "To Protect and Infect: The Materialization of the Internet (Part Two; In Three Acts)." *30th Chaos Communication Congress (30C3)*, December 27–30, CCH Congress Center, Hamburg, Germany.

Baldwin, Carliss Young, and Kim B. Clark. 2000. *Design Rules: the Power of Modularity*. Cambridge, MA: The MIT Press.

[6] Since 2014, ACLU's NSA Documents database alone has released several hundreds of documents (2014: 399; 2015: 217; 2016: 530). Additionally there are other sources to be further explored: first, sources not included in ACLU's NSA Documents database (e.g., Cryptome, Courage Foundation); and second, sources not related to Snowden's disclosures (e.g., FOIA, declassified documents around the Venona Project and Cold War espionage, the Church Committee Reports).

Ball, Kirstie S., and Laureen Snider, eds. 2013. *The Surveillance–Industrial Complex: A Political Economy of Surveillance*. New York and London: Taylor & Francis.

Ball, Kirstie S., Kevin D. Haggerty, and David Lyon. 2012. *Routledge Handbook of Surveillance Studies*. Abingdon: Routledge.

Barad, Karen. 1998. "Getting Real: Technoscientific Practices and the Materialization of Reality." *Differences: A Journal of Feminist Cultural Studies* 10 (2): 87–91.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R. B. J. Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance." International Political Sociology 8 (2): 121–144. doi:10.1111/ips.12048.

Bell, Daniel. 1979. "The Social Framework of the Information Society." In *The Computer Age: A 20 Year View*, edited by M. L. Dertoozos and J. Moses. MIT Bicentennial Studies. Cambridge, MA: MIT Press, 500–549.

Bennett, Jane. 2010. *Vibrant Matter: A Political Ecology of Things*. Durham and London: Duke University Press.

Birchall, Clare. 2016. "Managing Secrecy." *International Journal of Communication* 10: 152–163.

Bogard, William. 2006. "Surveillance Assemblages and Lines of Flight." In *Theorizing Surveillance: The Panopticon and Beyond*, edited by David Lyon, 97–122. Collumpton: Willan Publishing.

Bryan, Joe. 2009. "Where Would We Be Without Them?: Knowledge, Space and Power in Indigenous Politics." *Futures* 41 (1): 24–32. doi:10.1016/j.futures.2008.07.005.

Castells, Manuel. 1996–1998. *The Information Age: Economy, Society and Culture*. 3 vols. Oxford: Blackwell Publishing Ltd.

Cayford, M., C. van Gulijk, and P. van Gelder. 2014. "All Swept Up: An Initial Classification of NSA Surveillance Technology." In *Safety and Reliability: Methodology and Applications*, edited by Tomasz Nowakowski, Marek Młyńczak, Anna Jodejko-Pietruczuk, and Sylwia Werbińska-Wojciechowska, 643–650. London: CRC Press. doi:10.1201/b17399-90.

Ciborra, Claudio U. 1997. "De Profundis?: Deconstructing the Concept of Strategic Alignment." *Scandinavian Journal of Information Systems* 9 (1): 67–82.

Ciborra, Claudio U. 1998. "Crisis and Foundations: An Inquiry Into the Nature and Limits of Models and Methods in the Information Systems Discipline." *Journal of Strategic Information Systems*: 5–16. doi:10.1145/381823.381834.

Collier, Stephen J., and Aihwa Ong. 2004. "Global Assemblages, Anthropological Problems." In *Global Assemblages: Technology, Politics, and Ethics as Anthropological Problems*, edited by Aihwa Ong and Stephen J. Collier, 3–21. New York: Wiley-Blackwell.

Crampton, Jeremy W, Susan M. Roberts, and Ate Poorthuis. 2013. "The New Political Economy of Geographical Intelligence." *Annals of the Association of American Geographers*, 104 (1): 196–214. doi:10.1080/00045608.2013.843436.

Crampton, Jeremy W. 2010. *Mapping: A Critical Introduction to Cartography and GIS*. Critical Introductions to Geography. Chichester: Wiley-Blackwell.

DeLanda, Manuel. 2006. A New Philosophy of Society: Assemblage Theory and Social Complexity. London and New York: Bloomsbury.

DeLanda, Manuel. 2011. Philosophy and Simulation: The Emergence of Synthetic Reason. London and New York: Continuum.

Digital Methods Initiative (DMI). 2015. "Post-Snowden Media Empiricism and Secondary Social Media: Data Studies Beyond Facebook and Twitter." *Digital Methods Summer School 2015*. Digital Methods Initiative Wiki, July 11. https://wiki.digitalmethods.net/Dmi/SummerSchool2015.

Ertuna, Irmak. 2009. "Bernard Stiegler and the Question of Technics." *Transformations: Journal of Media & Culture* 17. http://www.transformationsjournal.org/journal/issue_17/article_07.shtml.

Foucault, Michel. 1995. *Discipline and Punish: The Birth of the Prison*. 1975. Translated by Alan Sheridan. 1977. 2nd ed. New York: Vintage Books.

Foucault, Michel. 2007. *Security, Territory, Population: Lectures at the Collège de France 1977–1978*. Basingstoke: Palgrave Macmillan.

Graham, Stephen D. N., and Nigel J. Thrift. 2007. "Out of Order: Understanding Repair and Maintenance." *Theory, Culture & Society* 24 (3): 1–25. doi:10.1177/0263276407075954.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books and Henry Holt.

Haggerty, Kevin D., and Amber Gazso. 2005. "Seeing Beyond the Ruins: Surveillance as a Response to Terrorist Threats." *The Canadian Journal of Sociology / Cahiers Canadiens De Sociologie* 30 (2): 169–187. doi:10.2307/4146129.

Haggerty, Kevin D., and Richard V. Ericson. 2000. "The Surveillant Assemblage." *The British Journal of Sociology* 51 (4): 605–622. doi:10.1080/00071310020015280.

Harding, Luke. 2014. *The Snowden Files*. London: Guardian Books.

Hayes, Ben. 2012. "The Surveillance–Industrial Complex." In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin D. Haggerty, and David Lyon, 167–175. Abingdon: Routledge.

Hier, Sean, and Joshua Greenberg, eds. 2007. *The Surveillance Studies Reader*. New York: Open University Press.

Jacomy, Mathieu. 2011. "ForceAtlas2, the New Version of Our Home-Brew Layout | Gephi blog." Gephi Blog, June 6. https://gephi.wordpress.com/2011/06/06/forceatlas2-the-new-version-of-our-home-brew-layout/.

Jacomy, Mathieu, Sebastien Heymann, Tommaso Venturini, and Mathieu Bastian. 2012. "*ForceAtlas2*, a Continuous Graph Layout Algorithm for Handy Network Visualization." Paris: Sciences Po Médialab.

Kean, Thomas H., and Lee H. Hamilton. 2004. *The 9/11 Commission Report*. New York: W. W. Norton & Company.

Klauser, Francisco R. 2013. "Political Geographies of Surveillance." *Geoforum* 49 (C): 275–278. doi:10.1016/j.geoforum.2013.08.010.

Kleinberg, Jon M. 1999. "Authoritative Sources in a Hyperlinked Environment." *Journal of the ACM* 46 (5): 604–32. doi:10.1145/324133.324140.

Knorr-Cetina, Karin. 1999. *Epistemic Cultures: How the Sciences Make Knowledge*. Cambridge, MA: Harvard University Press.

Kruger, Erin, and Kevin D. Haggerty. 2006. "Review Essay: Intelligence Exchange in Policing and Security." *Policing and Society* 16 (1): 86–91. doi:10.1080/10439460500399833.

Latour, Bruno, Pablo Jensen, Tommaso Venturini, Sébastian Grauwin, and Dominique Boullier. 2012. "The Whole Is Always Smaller Than Its Parts: A Digital Test of Gabriel Tarde's Monads." *British Journal of Sociology* 63 (4): 590–615. doi:10.1111/j.1468-4446.2012.01428.x.

Latour, Bruno. 2005. *Reassembling the Social: An Introduction to Actor-Network-Theory*. Clarendon Lectures in Management Studies. Oxford: Oxford University Press.

Law, John. 1992. "Notes on the Theory of the Actor-Network: Ordering, Strategy, and Heterogeneity." *Systems Practice* 5 (4): 379–93. doi:10.1007/bf01059830.

Lee, Newton. 2014. *Facebook Nation: Total Information Awareness*. 2nd ed. New York: Springer.

Lefebvre, Henri. 2006. *Critique of Everyday Life, Vol. 3: From Modernity to Modernism (Towards a Metaphilosophy of Daily Life)*. 1947. Translated by Gregory Elliott. London: Verso.

Lyon, David. 1991. *The Information Society: Issues and Illusion*. Cambridge: Polity Press.

Lyon, David. 1994. *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.

Lyon, David. 2007. *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Lyon, David. 2014. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." *Big Data & Society* 1 (2): 1–13. doi:10.1177/2053951714541861.

Lyon, David. 2015. *Surveillance After Snowden*. Cambridge: Polity Press.

Mann, Steve, Jason Nolan, and Barry Wellman. 2003. "Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments." *Surveillance & Society* 1 (3): 331–355.

Manovich, Lev. 2001. *The Language of New Media*. Cambridge, MA: The MIT Press.

Marx, Gary T. 1988. *Undercover: Police Surveillance in America*. Berkeley: University of California Press.

Marx, Gary T. 2002. "What's New About the 'New Surveillance'?: Classifying for Change and Continuity." *Surveillance & Society* 1 (1): 9–29. doi:10.1007/BF02687074.

Marx, Gary T. 2003. "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance." *Journal of Social Issues* 59 (2): 369–390. doi:10.1111/1540-4560.00069.

Maurer, Tim, Edin Omanovic, and Ben Wagner. 2014. *Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age*. Washington, DC and New York: New America Foundation.

Milan, Stefania, and Lonneke van der Velden. 2016. "The Alternative Epistemologies of Data Activism." *Digital Culture & Society* 2 (2): 1–18. doi:10.14361/dcs-2016-0205.

Murakami Wood, David. 2009. "Situating Surveillance Studies." *Surveillance & Society* 19 (2): 52–61.

Murakami Wood, David. 2013. "What Is Global Surveillance?: Towards a Relational Political Economy of the Global Surveillant Assemblage." *Geoforum* 49 (C): 317–326. doi:10.1016/j.geoforum.2013.07.001.

National Security Agency (NSA). 2007. "NSA/CSSM 1-52." *American Civil Liberties Union,* January 8. https://www.aclu.org/files/natsec/nsa/20140130/NSA's%20Spy%20Catalogue.pdf.

National Security Agency (NSA). 2010. "(U//FOUO) QUANTUMTHEORY." *American Civil Liberties Union*. https://www.aclu.org/sites/default/files/assets/the-nsa-and-gchqs-quantumtheory-hacking-tactics.pdf.

November, Valérie, Eduardo Camacho-Hübner, and Bruno Latour. 2010. "Entering a Risky Territory: Space in the Age of Digital Navigation." *Environment and Planning D: Society and Space* 28 (4): 581–599. doi:10.1068/d10409.

Rogers, Richard A. 2004. "Why Map?: The Techno–Epistemological Outlook." *Media Design Research*. Piet Zwart Institute, Willem de Kooning Academy, Rotterdam University of Applied Sciences.

Russell, Andrew L. 2012. "Modularity: an Interdisciplinary History of an Ordering Concept." *Information & Culture: A Journal of History* 47 (3): 257–87. doi:10.1353/lac.2012.0015.

Schneier, Bruce. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W. W. Norton.

Stanley, Jay. 2004. *The Surveillance–Industrial Complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society*. New York: American Civil Liberties Union.

Stiegler, Bernard. 2012. "Relational Ecology and the Digital *Pharmakon*." *Culture Machine* 13: 1–19.

Stiegler, Bernard. 2013. *What Makes Life Worth Living: On Pharmacology*. 2010. Translated by Daniel Ross. Cambridge: Polity Press.

Stone, Michael. 1998. "Map or Be Mapped." *Whole Earth* 94 (Fall): 54–55.

van der Ploeg, Inge. 2003. "Biometrics and the Body as Information: Normative Issues of Socio-Technical Coding of the Body." In *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, edited by David Lyon, 57–73. London and New York: Routledge.

van der Ploeg, Inge. 2012. "The Body as Data in the Age of Information." In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin D. Haggerty, and David Lyon, 176–183. Abingdon: Routledge.

van der Vlist, Fernando N. 2016. "Accounting for the Social: Investigating Commensuration and Big Data Practices at Facebook." *Big Data & Society* 3 (1): 1–16. doi:10.1177/2053951716631365.

Wagner, Ben. 2012. *Exporting Censorship and Surveillance Technology*. The Hague: Humanist Institute for Cooperation with Developing Countries (Hivos).

Wainwright, Joel, and Joe Bryan. 2009. "Cartography, Territory, Property: Postcolonial Reflections on Indigenous Counter-Mapping in Nicaragua and Belize." *Cultural Geographies* 16 (2): 153–178. doi:10.1177/1474474008101515.

Webster, Frank. 2006. *Theories of the Information Society*. International Library of Sociology. 1995. 3rd ed. London: Routledge.

Weinrebe, Emily. 2014. "Introducing the ACLU's NSA Documents Database." *American Civil Liberties Union,* March 4. https://www.aclu.org/blog/national-security/introducing-aclus-nsa-documents-database.

WikiLeaks. 2013. "Wikileaks—The Spy Files." *WikiLeaks*, September 4. https://wikileaks.org/the-spyfiles.html.

Wise, J. Macgregor. 2005. "Assemblage." In *Gilles Deleuze: Key Concepts*, edited by Charles Stivale, 77–87. Montreal and Kingston: McGill-Queen's University Press.

Wood, Denis, and John Fels. 2008. "The Natures of Maps: Cartographic Constructions of the Natural World." *Cartographica: The International Journal for Geographic Information and Geovisualization* 43 (3): 189–202. doi:10.3138/carto.43.3.189.

Wood, David, and Stephen D. N. Graham. 2006. "Permeable Boundaries in the Software-Sorted Society: Surveillance and the Differentiation of Mobility." In *Mobile Technologies of the City*, edited by Mimi Sheller and John Urry, 177–191. Networked Cities Series. London and New York: Routledge.

Wood, David, Kirstie S. Ball, David Lyon, Clive Norris, and Charles D. Raab. 2006. *Information Commissioner's Report to Parliament on the State of Surveillance*. London: Information Commissioner's Office.