Extended Abstract

Techno-Politics as Network(ed) Struggles

Laura Fichtner [1,*]

[1] University of Twente

E-Mails: laura.fichtner@gmx.de (L.F.)

* Author to whom correspondence should be addressed

Accepted:

Introduction

At least since the NSA disclosures of 2013th "Summer of Surveillance", internet surveillance and informational privacy and security have received widespread public attention and become a political concern for many. Taking the disclosures as a starting point, I follow up on this development and inquire into the *techno-politics of surveillance and counter-surveillance*. Instead of focusing on regulation applied to technological practices from outside, I investigate the socio-political dimensions of the internet infrastructure itself and the politics of concrete technological surveillance and counter-surveillance *practices*. I show how data infrastructures are not only regulated through policy, but can function as techno-political means which bring about a specific socio-technical structure. My question is: *How do surveillance and counter-surveillance technologies operate as a form of techno-politics within the internet infrastructure?* The answer to this question can enhance our understanding of the impact on the political landscape, which ubiquitous information technologies and their steady diffusion into every realm of our lives have.

Technological infrastructures and networks are of central importance to my research, as contemporary ICTs and ICT surveillance technologies operate in and through networks rather than as single artifacts. The network, one of the 21st century's most prominent entities, is both a potential threat and a potential point of control. Cumbers, Routledge and Nativel argue that "it is becoming increasingly difficult for ruling elites, usually located at the national scale, to play the gatekeeper role, through traditional territorialized hierarchies, with regard to information and communication flows across space" (Cumbers, Routledge & Nativel, 2008, p. 188). To exercise control then requires an "'empire' based upon a decentred and deterritorializing apparatus of rule that progressively incorporates the entire global realm" (Cumbers, Routledge & Nativel, 2008, p. 185). At the same time,

networks have the tendency "to create hubs as these provide more stability and robustness. Hubs establish a kind of 'hierarchy' within networks and this in turn gives a certain advantage to key positions of players'" (Cumbers, Routledge & Nativel, 2008, p. 189). In my research I explore how surveillance technologies exploit the internet's inherent hierarchies and operate through the global hubs that emerged within the infrastructure. Counter-surveillance technologies try to sabotage the centralized surveillance network this establishes. By using encryption technologies, they aim to make hubs dysfunctional for surveillance and to strengthen non-hierarchical network features. Consequently, the two antagonists are opposed in the way they use the network and are involved in a struggle over the network's very structure and technological design.

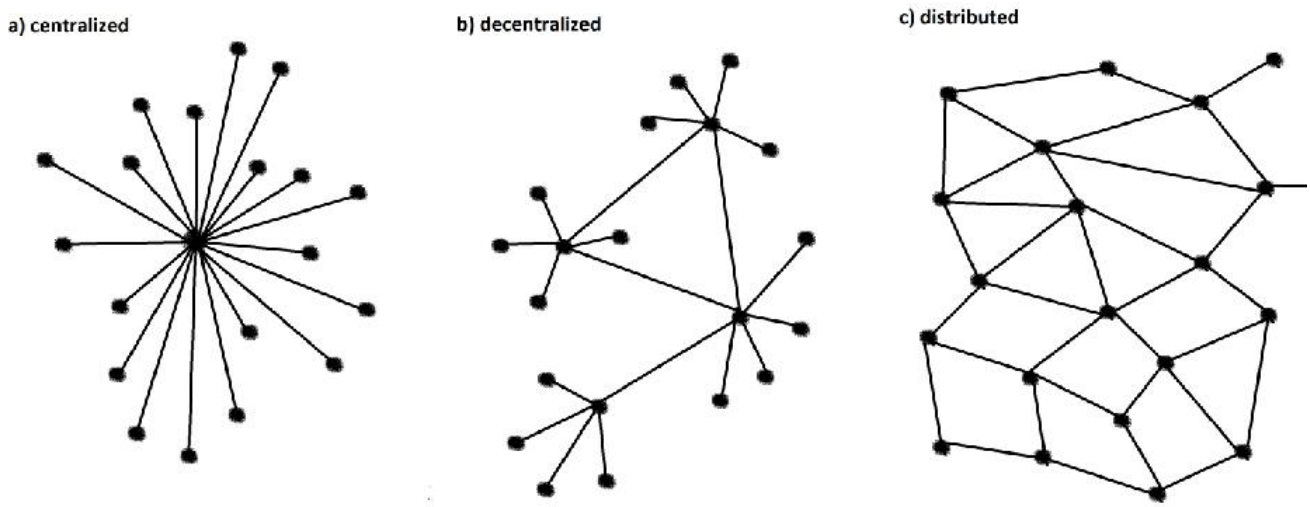
Methods

I base my framework on pragmatist John Dewey's approach to the relation between politics and infrastructures (Dewey, 1927) and extend it by analyzing the actual technological internet infrastructure. Susan Leigh Star and Geoffrey C. Bowker's work on infrastructures and Alexander Galloway's description of different network topologies to be found within the internet provide my basis for this analysis (Star & Bowker, 2006; Galloway, 2004). It builds the foundation for understanding surveillance and counter-surveillance technologies' operation in and on the internet and its political dimensions. In Dewey's political thought, technological infrastructures play a major role because he held politics to be concerned with governing the channels of human interactions, of which technological infrastructures are an essential part (Dewey, 1927, p. 30). Through these channels, people can purposefully organize within society, interact through networks of communication and collaboration, and engage in joint endeavors. Technologies become the means and ends of their purpose-directed activities and signify "the intelligent techniques by which the energies of nature and man [sic] are directed and used in satisfaction of human needs" (Hickman, 2001, p. 8). Politics exercise indirect control over people's behavior through governing technological channels and regulating infrastructural systems. It is through these systems that interactions amongst society's members propagate and actions translate into consequences through transmission over several instances.

Even though Dewey recognized their political importance, he did not analyze infrastructures in detail. According to Susan Leigh Star and Geoffrey C. Bowker, infrastructures are that "upon which something else rides, or works" (Star & Bowker, 2006, p. 230). As the technological structures that enable social phenomena, they are always underneath – transparent, invisible and embedded. Once in place, infrastructures only call for active investigation and attention when conditions of usability are altered and smooth use is prevented; otherwise they remain outside our awareness and active experiences. Because they organize flows of exchange within socio-technical complexes, infrastructures can be understood as the *technological ordering* of things. They consist of a plurality of technologies, agents and sub-networks and their actual configuration is contingent and dependent on implementation. Every configuration "represents only one of a number of possible contributions of tasks and properties between hardware, software and people" (Star & Bowker, 2006, p. 234). Network diagrams describe the structural features of different configurations and visualize their inherent distribution of power and control. To describe the control structures within the internet infrastructure, Alexander Galloway uses three different network types: the *distributed*, the *decentralized* and the

centralized network (Galloway, 2004, pp. 11-12 & pp. 30 ff.). The centralized network is a hierarchical network in which one central host wields power over subordinate nodes. The decentralized network is then the conjunction of several centralized networks and consists of multiple hosts which rule over their sub-set of nodes. In both networks, information flows one-directionally from the host(s) to the nodes. A distributed network on the other hand does not have a hierarchical order, but every node is an equally autonomous agent and can communicate with any other node peer-to-peer. Now, when it comes to surveillance, the centralized network is easiest, since all flows must pass through the central hub. To surveil a decentralized network, multiple host need to be intercepted, because information does not accumulate in one place. In a distributed network, surveillance is most complicated. Here, in order to access every information flow within the network, *all nodes* (network participants) must be monitored.

Figure 1. The centralized, decentralized and distributed network diagram.

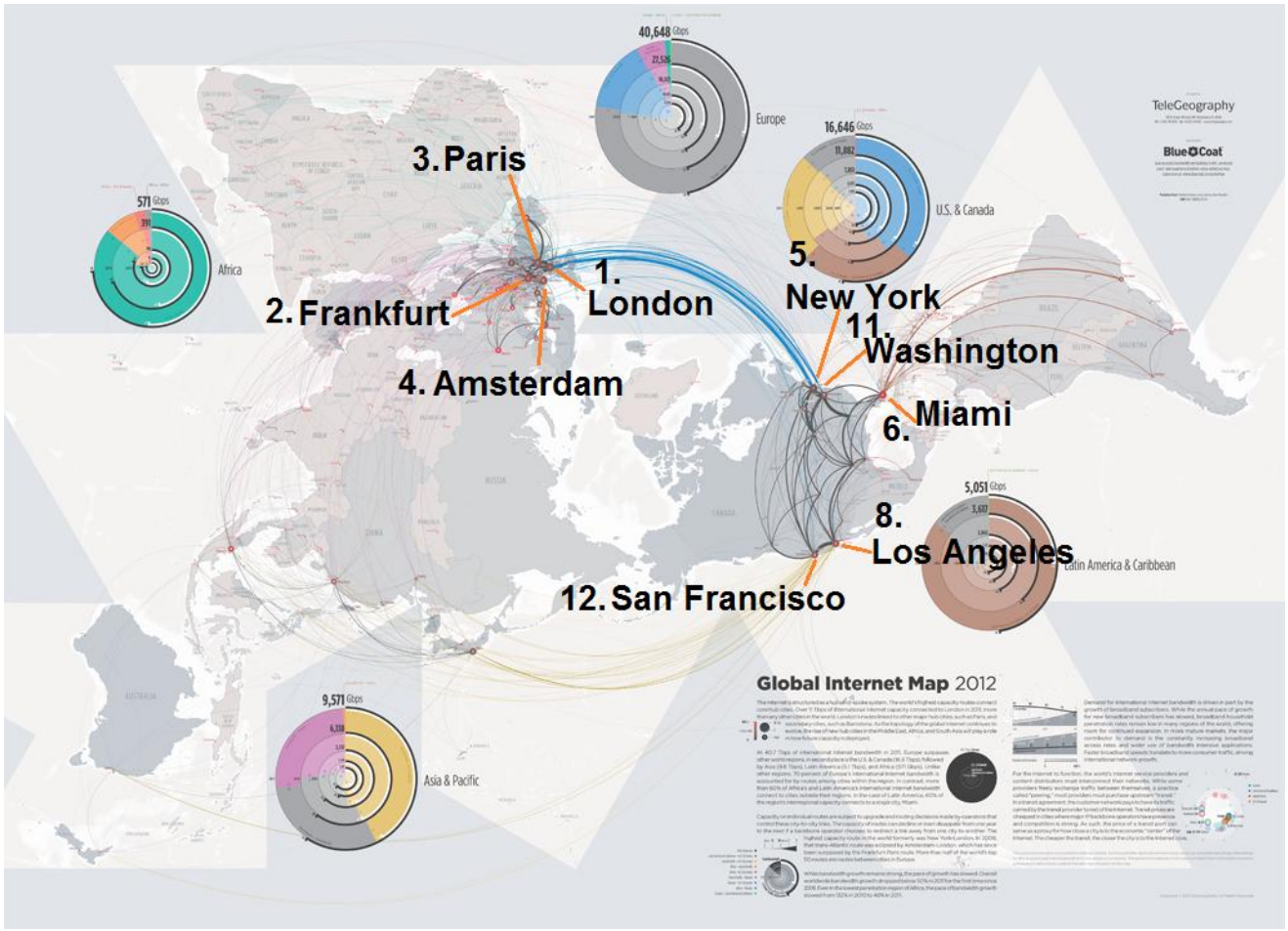


Results and Discussion

Within the internet infrastructure's different technological layers, we can find both distributed and (de)centralized network topologies. On the one hand, there is what I call the internet's "physical layer". This layer transmits actual data signals and consists of devices, cable networks, routers, servers, etc. When looking at its global constitution, we can see that this physical layer resembles a decentralized network. Across the globe, there are a number of major internet exchange points (IXPs). These are operated by internet providers like AT&T and most are located in the United States and Europe, for example in London, Frankfurt, Paris and New York (Figure 2). Nearly all internet traffic needs to pass one of them in order to get forwarded to its destination. Consequently, the IXPs build central internet hubs. Global (undersea) cable networks support this, because cables with the greatest bandwidth connect to these IXPs (TeleGeography, 2014). As it is cheapest to route through high bandwidth, data often does not take the geographically shortest path. Instead, it is linked through different high bandwidth cables across the globe and most likely across the United States. Therefore it is not surprising that NSA surveillance technologies exploit the decentralized structure of the physical layer (The Guardian, 2013). As most global hubs are are located on US soil or on the soil of US allies, the NSA can gain access to global information flows and retrieve data doubles secretly. One example

for how this is done is Room 641A in AT&Ts office in San Francisco. According to former technician Mark Klein, the NSA had installed a splitter device in the office's internet room, which is basically an IXP (Klein, 2007). From this splitter, it directs copies of all passing internet traffic to its secret room, where the data is analyzed with latest technology. From such interception points then, the NSA feeds the data into its own network and data center. This creates a centralized shadow-network on top of the actual internet infrastructure, in which the NSA is the central hub. From this position it can monitor information flows and oversee the whole network, but peripheral network participants remain unaware. Moreover, it is potentially able to manipulate data flows, as has been the case with the program Quantumtheory (Spiegel Online, 2013).

Figure 2. Global internet routes in 2012: © Copyright 2014 PriMetrica, Inc., retrieved from http://www.telegeography.com/telecom-resources/map-gallery/globalinternet-map-2012/index.html.



But there is also a reason for why we often consider the internet a distributed network. Operating 'on top' of the physical layer, the "protocological layer" creates a network of equal nodes and bi-directional communication flows. In this layer, the rules are defined according to which data is wrapped and transmitted by the physical layer. The internet's TCP/IP Protocol Suite logically assigns equal weight to all hubs and nodes (Cowley, 2012; Galloway, 2004). According to its predefined rules, IXPs have to route data but are not allowed to wield power over information flows. The protocols' universal rules count equally for all network participants communicating through the infrastructure. To a potential surveiller, this distributed network is a thorn in the eye, because surveilling all flows here is very complex. For this reason, counter-surveillance technologies operate on and strengthen the

protocological layer. Through encrypting data flows end-to-end, they make the decentralized physical structure dysfunctional for surveillance. Data still flows through the physical infrastructure and passes global hubs, but through encryption, communication is established peer-to-peer only. If someone intercepts the hubs, they cannot get any information usable for surveillance, because they cannot read the data. The Tor network does a similar thing (Tor Project, 2014); it hooks up to the regular internet infrastructure and allows user to access the internet. But by encrypting meta-data, surveillance of internet activities becomes impossible. In this way, encryption technologies have the power to strengthen the distributed features of the protocological layer and circumvent the decentralized physical one.

Conclusions

The results of my analysis show how the operation of surveillance and counter-surveillance technologies exploit different socio-political dimensions inherent to the internet infrastructure. Network diagrams helped me to describe these different dimensions and demonstrate how the two antagonists are engaged in a struggle over the network's (dominant) structure and particular socio-technical organization. NSA surveillance technologies aim at establishing a centralized network in which the agency provides the central hub and oversees all information flows. Counter-surveillance technologies aim at establishing a distributed network where all nodes have equal rights and no one host has centralized control. This techno-political struggle is carried out within the infrastructure itself and through technological means. Within a Dewian account of politics, surveillance and counter-surveillance technologies then operate as a form of techno-politics, because they organize the channels of human interaction and strive to systematically regulate structures of interactions and communications through technologies.

However, Dewey still thought infrastructures to be extrinsic to political forms. In the case of governmental internet surveillance, we now see they become *intrinsic*, as infrastructures are employed for political purposes. In such techno-politics, political solutions are not negotiated through public discourse but through the application and operation of technologies. The people implied in the global network are affected by these techno-politics, because they structure their interactions in the network. But when political struggles are carried out on infrastructural levels that are transparent to users by their very definition, people remain unaware of these ongoing political developments. The problem this poses to democracy is further intensified by the network's deterritorializing forces, which allow national agencies to access global hubs and wield power over a global public, while representing only a single nation state in whose interest they (supposedly) act. If technological solutions are provided to political problems, and if these solutions are applied on infrastructural levels that are transparent and invisible, then regular internet users and citizens are left unaware of political processes and cannot participate. Instead, it is technological elites who negotiate political decisions.

Acknowledgments

This paper is the result of my Master's graduation project in Philosophy of Science, Technology and Society, offered at the University of Twente in the Netherlands. At this point I would like to offer my special thanks to my first supervisor, Dr. Michael Nagenborg, who was very enthusiastic about my

project from the beginning on and provided me with the right starting points and a great introduction to Surveillance Studies. I would also like to express my great appreciation to my second supervisor, Prof. Peter-Paul Verbeek, who gave me feedback during the writing process and great support throughout the whole program. Finally, I wish to acknowledge all the people who make this outstanding Master's program possible, my fellow students with whom I had such great discussions, and my family and friends for always supporting me.

References and Notes

Cumbers, A.; Routledge, P.; Nativel, C. The entangled geographies of global justice networks. *Progress in Human Geography* **2008**, *32*(2), 183-201.

Cowley, C. *Communications and Networking*, 2nd ed.; Springer-Verlag: London, United Kingdom, 2012.

Dewey, J. *The Public and its Problems*; Swallow Press/Ohio University Press: Athens, OH, United States, 1927.

Galloway, A. *Protocol: How Control Exists after Decentralization*; The MIT Press: Cambridge, MA, United States, 2004.

Hickman, L. *Philosophical Tools for a Technological Culture*; Indiana University Press: Bloomington, IN, United States, 2001.

Klein, M. *Spying on the home front.* Interview with H. Smith, Interviewer, 2007, May 15. Retrieved from http://www.pbs.org/wgbh/pages/frontline/homefront/interviews/klein.html

Spiegel Online. *NSA-Dokumente: So übernimmt der Geheimdienst fremde Rechner;* Published 2013, December 12. Retrieved from http://www.spiegel.de/fotostrecke/nsa-dokumente-so-uebernimmt-dergeheimdienst-fremde-rechner-fotostrecke-105329-8.html

Star, S. L.; Bowker, G. C. How to infrastructure. *Handbook of New Media* **2006**, 230-245.

TeleGeography. *Submarine Cable Map 2014*; 2014. Retrieved from http://www.telegeography.com/telecom-resources/map-gallery/submarinecable-map-2014/index.html

The Guardian. *NSA Prism program slides*. Published 2013, November 1. Retrieved from http://www.theguardian.com/world/interactive/2013/nov/01/prism-slidesnsa-document

Tor Project. *Tor: Overview*. Project website, 2014. Retrieved from https://www.torproject.org/about/overview.html.en