CRITICALLY ENGINEERED WIRELESS POLITICS
Jussi Parikka

'Under the sea, under the sea
no little signals are coming to me.
Under the sea, under the sea.
Something has surely gone wrong.
And it's broke, broke, broke;
What is the cause of it does not transpire
But something has broken the telegraph wire
With a stroke, stroke, stroke,
Or else they've been pulling it too strong.'
(James Clerk Maxwell, 'The Song of the Atlantic Telegraph
Company', second verse, quoted in Mahon, 2003: 6)

James Clerk Maxwell was probably better off following a career as a scientist than as a poet. One of his poems, cited above, mocks the response one of his friends encountered when consulting the Atlantic Telegraph Company and asking about the laying of the original Atlantic cable. Maxwell was not of course the only one laughing at cable-laying efforts that seemed to run into endless difficulties. Besides such sarcastic critics, there were however lots of others who had a more optimistic view of the state of new communications technology: new worlds of communication and connection were just round the corner. On a material level, it lay on the sea bottom: the little coded signals, hidden inside cables, covered in gutta-percha, hidden inside the waves. The new aspirations of global communication also spilled out as enthusiasm for cabling as a form of Transatlantic supranational publicness. In a similar manner, the Crimean cable in 1855 had made 'the ocean a highway a thought' ('European Sub-Marine Telegraph'). Such a fantasy of a wired public(ness) was enabled by a range of materials and technologies, of cabling and insulating, of grey procedures of engineering. This can be referred to as the grey constitution of the public, an engineering of certain communication politics – that the

political is infused with matters technological. Greyness is here an allusion to Michel Foucault's thoughts on genealogy,[1] as well as to the greyness of technological components and structures.

Despite this opening, this article does not focus on past engineers or sea cables, but on the politics of transmission in the age of *wireless* communication. The perspective it takes on communication does not however assume successful frictionless transmission between sender and receiver as the normal state of things. Instead, the article looks at interruption, hijacking and the engineered parasitical event as replacing the idealistic discourse of media as communication. We are dealing with evil media: 'a manner of working with a set of informal practices and bodies of knowledge, characterized as stratagems, which pervade contemporary networked media and which straddle the distinction between the work of theory and of practice' (Fuller & Goffey 2009: 141).

Evil Media outlines a shift in the interest of analysis and practice, from assumptions of 'autonomous rationality and the ideal of knowledge' – for instance uncovering secrets in the name of democratic transparency – to 'trickery, deception and manipulation'. These are modes of production of reality, and evil media is about a technologically focused perspective on such knowledge practices that are interested in the manipulation of what is perceived. *Evil Media* flags a non-representational take on politics that picks up on evil as an ontological force. It insists on an ontology irreducible to humans and meanings to focus on 'the non-sense of something that cannot be exchanged for meaning' (141), which in the case of critical engineering works through technological infrastructures such as platforms.

Matters of engineering – and especially critical, evil engineering – of networks and platforms are investigated here through the artistic work of the studio group, Weise 7, and especially their February 2011 Transmediale Exhibition. Various pieces in the exhibition reveal a consistently speculative but yet engineered take on wireless network culture. Curated by Kristoffer Gansing, the exhibition, featuring technology based installations in various formats that are related to computers, transmission and data secrecy, investigates the politics of transmission and through the engineered level of 'what bodies can do' in network environments. This investigation is not limited to human bodies, but invokes a politics that extends to bodies of data, such as packets and their role in the constitution of publicness in the age of wireless networks. To quote a tweet by

Julian Oliver (Weise 7 and one of the writers of the Critical Engineering manifesto): 'If the air is considered public, why not that which passes through it?' (@julianoliver Tweet on June 28, 2012). Indeed, the projects often attach to principles of openness in code and networks as essential to artistic activity (see Bucher, 2011). This focus on wireless brings forth an important point about platforms: platforms can be considered as specific structurations (social and technological) that sustain different modes of interaction, but they are not necessarily locatable to a singular place and time. This is how we need to articulate wireless politics too: it is more of a vector than a stable place (Cf. Wark 2004).

Figure 1. Weise 7 Exhibition in Berlin, at Transmediale 2012

Such approaches are labelled and articulated as 'critical engineering': practices that are close to hacktivism, but for tactical reasons the allusion to engineering as the language of modernity has here been lifted to the forefront. Indeed, such 'art' projects are 'not just art' in the manner Matthew Fuller (2006: 91) pitches the term to refer to art practices' functions at 'social, political, technical, and many other scales.' We can speculate that such ideas and practices as Weise7-group's are an indirect response to what Geert Lovink (2012: 22) has called the need for 'materialist (read: hardware- and software-focused) and affect-related theory.' In this case, theory is not executed only in the normal written format but as engineered situations: the other material infrastructures and modes of expression in which power operates, from code to networks.

However, in this case 'affect' is less the work of emotions than about relations and affordances (see also Parikka, 2010; McQuillan, 2012a) which aim to both address a familiar political discourse concerning democracy, privacy and publicness and to suggest slightly unconventional, experimental insights into an agenda of platform politics – where the platform might be carefully opened, re-engineered, and reveal a different reality that touches on topics of hacktivism and even rethinking policy through new peer-oriented design practices (McQuillan, 2012a and 2012b).

Network and platform politics are in this article understood through such a notion of misplaced, hijacked and distorted communications. In order to twist a media ecological idea that a platform is an affordance for actions, perceptions, social behaviour and in general; that is as a way to understand Deleuzian control societies more concretely tuned to specific hardware and software configirations, we approach platforms through hackability and distortion. Understanding platforms as affordances for communication and the social – as algorithmic guidances to various modes of sociability (see Gillespie, forthcoming) – allows for a broad understanding of how they are double binds between a production of the social and its captivation through monetarisation, as well as for security. Hence, the politics of the various critical engineering projects that this article discusses are sorts of platform hacking that take the mode of the exploit. The exploit starts not from the assumed normal uses, but from the breaking-points, latent possibilities for exploiting the normalised uses, finding cracks, openings and new possibilities hidden but completely existant within the engineered reality. (See Oliver, Savičić, Vasiliev, 2011. Cf. Galloway & Thacker, 2007)

Platforms consist of topologies of relations that stretch across the technological and the social. The engineered is not removed from, but rather constitutes the social, and the social is embedded and afforded by a range of technological problems and solutions. This means acknowledging the centrality of practices of surveillance and engineering of network traffic. It includes questions about speed as well, and in general how traffic is governed by authorities and service providers; an argument that is picked up by Danja Vasiliev in his Netless-project (discussed below at greater length). Before going more into Critical Engineering, let's start with discussions of the public and the wireless.

Wireless

The modern political public is a technological phenomenon. It involves a lot of administrative measures that are sustained by technological infrastructures. In terms of academic literature, there has been an interest in administrative and management perspectives on power in the recent years of historically inclined research concerning cultural techniques of information and administration (see Gardey 2008, Beniger 1989, Krajewski 2010, Krajewski and Vismann 2007, Ernst 2013, Ebeling and Günzel 2007, Vismann 2008). In addition we have seen a special interest in the relations of management and technology. This resonates with the remark that Kittler, and the whole generation of German media theory that followed, made about Foucault's work needing to be updated to the technological age (Kittler 1990: 369). In addition, relating to a genealogy of texts debating 'network politics', curious interventions from early phases of real time network development such as H. Sackman's 'Public Philosophy for Real Time Information Systems' tried to argue for new ways of understanding politics in network culture. Long before the time of consolidated discourse concerning network politics, Sackman's perspective articulated, in the wake of John Dewey and the pragmatist tradition, the need for a democracy of real time.

Writing in the late 1960s meant engaging in discourses of computing in an age when the public 'rarely had direct interactions with computers' (Sackman, 1968: 1491. See also Suominen and Parikka 2010). Sackman was one of the voices in computing that articulated the gradual change in 'the public from spectator to participant' (Sackman, 1968: 1491), Indeed, in a manner that ties politics in with technological frameworks, for instance democracy as an administrative procedure (see Latour & Weibel 2005), such a change in perception of the public constituted the core for Sackman's argument. Sackman argues for a central role for computers as part of the 'regulation and control of social affairs' (Sackman, 1968: 1491). Computing and real time networks are about the regulation of the social. Embedded in the cybernetic vocabulary of governance and control of social situations, Sackman hones in on the otherwise often (still) too vague talk of information power in real time systems. Sackman pitches these as a 'social institution': 'The real time information system is a new class of social institution, a more radically powerful and rapidly responsive social form to recognize, meet and deal with specified problems at the time they occur and in time to modify their outcome' (Sackman, 1968:

1492). According to Sackman, in a true pragmatist manner, such systems connect knowledge to action. The real time system's possibility to act on its environment in 'real time' is what leads to specific regimes of knowledge about the system itself as well as its milieu. The ideas he presents suggest an undertone that premeditates the later information society discourse:

> In real time computing systems, however, the collection, organization and storage of information leads directly to action, to integrated surveillance and control over the object environment. This dynamic marriage of information and control in real time systems is a fusion of knowledge and action, and, through directed action in real time, information is expressed as power. (Sackman, 1968: 1492)

Information management can be seen as essential to the wider management of the public and politics, bringing practices of engineering into proximity with issues of democracy. The engineering and administrative procedures which contribute to Sackman's plea for a public philosophy of real time systems are something that take into account network infrastructures and design. Such a political perspective can be seen as stemming from the entanglement of experience with the multiscalar world of what Adrian Mackenzie (2010) calls 'wirelessness', transporting William James' radical empiricism into wireless network culture. Mackenzie is able to outline this techno-social entanglement as a constitution of experience. Besides technical elements ('things') as essential for a sense of the social and reality, it shows the necessary 'conjunctive relations' (21) as important bindings across scales, from things to organizations, perceptions to processes. For instance, a lack of interest in algorithms by users/consumers does still not mean that technological systems would have a similar lack of interest in catering for worlds of experience for us as users:

For instance, many people might say that they have no interest in, let alone experience of, the algorithmic signal-processing techniques implemented in wireless networks such as Bluetooth, Wi-Fi, or 3G cell phones. Despite that, their sensations of connection, their awareness of service availability, and their sometimes conscious preoccupation with connecting their wireless devices via service agreements or other devices all derive from the handling of

conjunctive relations in data streams implemented in wireless signal-processing chips. (McKenzie, 2010: 21)

Understanding the constituting nature of the wireless for subjectivity acts as a relay to the work of critical engineers at the Weise7-studio. The studio is located in Berlin, and consists of a collective of several media artist-hacktivist-critical engineers. This isemblematic of one sort of critical inquiry that extends between fields of media theory and hacktivism and was exemplified in their recent exhibition at Transmediale 2012 in Berlin. With various works that one could place under the umbrella term of hacktivist installations/devices, Weise7 participants, or at least several of the projects, are engaging in engineered excavations of the political in technological environments.

The works play with archaeologies and current practices in data sniffing, capture and exposure, which constitute the fundamental leaky elements of networks. This is the other side of publicness that does not easily fit in with the discourses of the public accountability or commons, but is the side exposed in surveillance, sniffing and in counter practices such as hacktivism. These works play with the idea of the unconscious of a platform that is tracked down as a concrete network technology problem. However, the notion of problem here might slightly mislead us, as we need to understand how these techniques are, even historically, part of the very constitution of the affordances of networks and wireless technologies. They are not just anomalies. For instance Bengt Sjölén's 'TEMPEST' project draws on the 1972 National Security Agency paper 'TEMPEST: A Signal Problem' (Friedman 1972/2007), declassified only a few years ago, to investigate the in-betweens of transmission. As such, it taps into the longer archaeologies of transmission and carrier waves and also into the idea of capture and exposure as unavoidable elements of technical communication. As a matter of engineering, it takes as its design a typical old radio receiver, but one modified so as to focus only on the 'unintentionally transmitted'. More specifically:

> A conventional radio transmitter and receiver uses a carrier wave of a specific frequency, and limits the transmitted and received energies to this frequency, but in fact any transition of an electric signal between on and off, between current and no current, will also transmit a burst of electromagnetic energy. These signals will not be limited to one carrier wave frequency but

> instead each such sharp transition will be constituted of all the odd harmonics that combined makes a square wave. Tempest radio listens to correlations between the harmonics at these odd multiples of the tuned frequency. (Weise 7, 2012)

The original Tempest document from 1972, an NSA project, expressed a concern for data capture as a danger for classified intelligence transmission. As part of histories of cryptography, information processing and transmission, the document addresses the problem of space radiation in terms of unintentional emissions of radio frequencies or acoustic energy released from 'the various switches, contacts, relays and other components' (Friedman, 1972/2007: 26). Hence, even in terms of seemingly isolated technologies, whether the cryptographic machine or the transmitted signal, radiation of the signals *in space* becomes a problem that articulates more widely the material, spatial context of such information machines. Problems of war, and problems of diplomacy, are here voiced in terms of their engineered contexts, as well as solutions that reveal this problematic publicness. The Public is not the idealised arena of democratic deliberation, but something that leaks out, and is constituted as the problem of desired secret communications.

As forms of data capture, such artistic projects express the problematics of urban space and time. They also indicate how publics and privacies are engineered. Something of the same spirit comes out in Julian Oliver's *Föhnseher* (2012) piece, that mobilizes a similar installation idea: an old broadcast age technology as the design face of a data capture system that sniffs the local wireless networks. The old technology becomes both an access point to the seemingly private worlds of urban wireless networks, and a television, or a public broadcasting device of a different sort. Indeed, this articulation of the possibility of publicness – whether through unintentional wiretapping or signal capture, or through sniffing image content from neighbour networks – is what is able to give insights that connect such projects to the earlier engineering of public data networks: the 20th century role of television as an integration of a sense of nationhood, imagined publics, as well as the emerging commercial advertising sphere. Television as the one-way broadcasting medium that created its sense of wireless publics and, for instance in the European context, a further integration of the idea

of nationhood as a broadcast based imagined community (see also Anderson, 2006) is re-engineered with the other, technical public of data packets and traffic.

Wendy Chun (2006: 4) picks up on these *other publics* in her elaboration of what actually happens when one is plugged in to the local network. With basic packet sniffing software one starts to understand the amount of things taking 'place' even without the human use of the computer. In its normal state, an Ethernet card rarely has a silent moment. Besides the individual, machine-to-machine communication that we as end users do not have a clue about, in the 'promiscuous' mode of packet sniffing one is able to access all of the network traffic and see how the private is filtered from the public only at a very late stage:

> Ethernet cards routinely read all in all packets and then discard those not addressed to it; promiscuous mode does not alter an Ethernet card's normal reading habits. The client-server model of the World Wide Web, in which your computer (the client) only receives data from machines designated as servers, is a software and cultural construction. Every computer with an Ethernet card serves information. (Chun, 2006:4)

Indeed, the idea of what articulates our senses of publicness, and even shared space, is expressed in such works as *Packetbrücke* (2012) - Packet Bridges. Tapping into the constituents of network packets, this beautiful installation retunnels data packets from the location of Weisestrasse 7 in the Neukölln district of Berlin to the exhibition venue, causing a sort of a technological dislocation of space and time. The 'hijacking' of data packets and the simultaneous distraction of mobile phones in the exhibition space causes a slightly schizophrenic situation of confusion for the sense of space of one's technologically enhanced being. Google maps one's iPhone produce an illusion of being situated in Neukölln (located several kilometres away), and by way of this confusion, the piece suggests that there is a whole layer of packets and electromagnetic architectures underlying the normalised (even if technologically augmented) sense of space. The sharedness of such situations is then not only something that happens on the human phenomenological level, but as a network and wireless situation: what is the location, how can it be displaced, how is it being

temporally tunnelled and routed, and what are the constituent architectures in which such data packet bodies are being channelled? This creates an imagined place through technology: an engineering of reality that is reliant on data based location as one effective spatializing cultural technique.
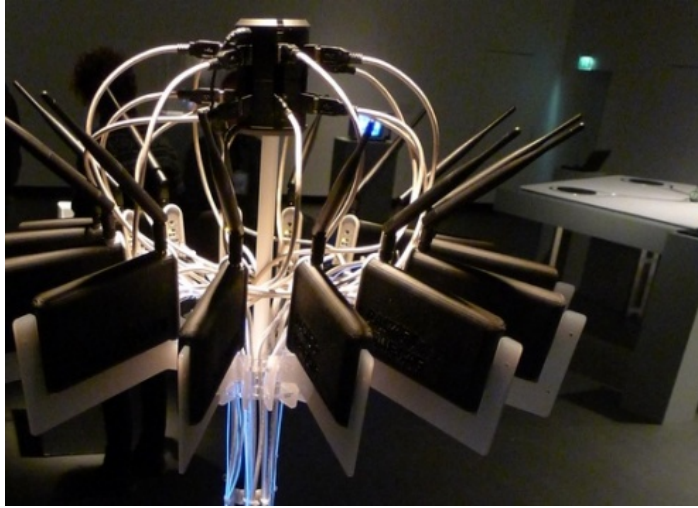

Figure 2. Packetbrucke. Used with permission.

Of course, such space or place does not just simply (pre)exist for the network, which creates its own link based on the transmission, routing, tunnelling and reception of signals. Indeed, this misperception is creative material aspect of a platform that can be sidetracked, wormholed. One way to conceptualise this is to say that it is about making infrastructures critical (cf. Renzi & Elmer 2012) so that they can be used in alternative ways relating to, say, (or indeed experimental questioning - on affordance in relation to critical hacktivism, see McQuillan 2012a). For Renzi and Elmer, critical infrastructures are significant in relation to the analysis of the new financial and security regimes of urban space as these unfolded around the G8 and G20 meetings in Toronto in 2010. The assumed danger to key national transportation, energy, and economic infrastructures was at the policy core of some of the preventive security measures launched against the demonstrators and activists.

What is highlighted as a question of network relations by Sackman, and then regarded as a central theme of network engineering, is the place of publicness, commonalities and transparency – or, indeed, the lack of it. The Weise7 projects play with precisely this narrative of contrasts between data secrecy, and network publicity. The introductory statement to the exhibition says: 'Opaque devices,

spyware, search engines and phones that talk about us behind our back: the deep reach of technology in our lives shapes both how we read the world and what we do in it' (Weise7, 2012). However, as becomes evident across the range of projects by Oliver, Sjölén, Vassiliev, and other Weise7-group members (although not all of the projects focus on the theme of wireless politics so directly), the idea of network publics is much more than one of public accountability, shared commons, and referencing democratic politics. Instead, network publics become a matter of *hidden data publics* that one is able to access through critical engineering techniques. This notion of devices talking behind our back is mobilized into a description that resonates with Chun's earlier note concerning sniffing – a machinic register of 'public' that demands a different political vocabulary for its 'public discourse' on the machinic level.

These sort of code publics do not refer to the more widely discussed agenda of 'politics of commons' as a way to think the relation between software and the public. In accounts such as David Berry's (2008), the connection between free software, intellectual property issues and the public domain, or the code based public sphere, becomes articulated well (see also Cox 2013: 79), but what the critical engineering projects argue or enact is a dirtier take on publics. Of course, these two positions are related – for instance they are both concerned with rethinking through peer-practices and how to bypass hierarchies of design and prototyping, and with 'critical hacktivism' (McQuillan 2012a). Both discourses do relate to issues of democracy, but they adopt different methodologies. This is why it makes sense to refer to Weise 7 projects as more 'evil' in the sense of engineering an ontological level of reality creation – ontogenesis.

Critical Engineering as Evil Media

The introductory lines for the Transmediale 2012 Weise7-exhibition express a narrativisation of the installations in relation to themes of secrecy and private systems, as well as the increasingly proprietary nature of technological networks. The danger of too readily succumbing to narratives of transparency and openness as the goals of activist intervention are clearly there – for instance in Julian Oliver's *Transparency Grenade* (2012), which pitches itself in a manner of anti-Corporate hacktivism, familiar with the discourse of past years of critique of corporate capitalism: 'The lack of Corporate and Governmental transparency has been a topic of great controversy in recent years, yet our only tool for encouraging greater

openness is the slow, tedious process of policy reform.' While clearly democratic accountability – and the lack of it – is a matter of importance, it is important to look at what we mean by 'transparency'.

Figure 3. Julian Oliver's Transparency Grenade. Used with permission.

Indeed, besides cheering for democratic values of transparency one can take such projects as critical engineering experiments in a more evil direction. To return to the words of Fuller and Goffey, the articulation of the object-perspective through secrecy is important in the context of the Weise7-projects:

> To put it another way, evil is a good name for the strategies of the *object*, for what things do *in themselves* without bothering to pass through the subjective demand for meaning. If secrecy is inherent to this agonism, this is perhaps because it is a process without subject, a machination, a process that depends on its imperceptibility and which must for that very reason surprise us, fox us or outwit us. (Fuller & Goffey, 2009: 143-144)

As a regime of non-meaning, *evil* bears more than a passing connection to media theory of signals and engineering. For some, a reference point is often Shannon and Weaver's mathematical theory of, but one could elaborate a wider signal-based range of communication theories of 20th century, (Genosko, 2012). This imperceptibility that comes out in the evil media manifesto characterises the politics of Weise7-projects; an imperceptibility that

connects to the ontological regime of wireless communication, part of the discourse of wirelessness since the 19th century. Imperceptibility relates to the sphere of secrecy and paranoia. These are further contexts for the birth of modern technical media in the manner of Thomas Pynchon's novels in their own way articulated, and is mobilized again with the recent years of network politics agenda (from Wikileaks to the material underwater cables, but nowadays time leaking in a different manner than what Maxwell pitched in his poem some 150 years earlier).

The Evil Media manifesto bears a relation to the idea of engineering, as introduced in another manifesto – the one on Critical Engineering by Julian Oliver, Gordan Savičić and Danja Vasiliev. Originating from October 2011, the manifesto is closely attached to the practice-based methodology of the Weise 7-studio. It picks up on language not too distant from evil media. Indeed, removed from ideas of transparency as the automatically valorized goal, it seems more closely to evince a love of engineered trickery and investigations of manipulation. Indeed, criticality becomes here a matter of excavation in the Foucault-cum-engineer sense, to look 'beyond the 'awe of implementation' to determine methods of influence and their specific effects.' (Oliver, Savičić, Vasiliev, 2011). In other words, and since Kittler, engineering is not only about machines in the restricted sense of the term, but of relations between 'devices, bodies, agents, forces and networks' (Oliver, Savičić, Vasiliev, 2011). Indeed, in one way one could see this as an exercise in the psychogeography of code: it is to do with mapping the architectures in which mind and body control work. It is an updated version of psychotechnics in the age of not only urban architecture but chip and wireless architectures where 'written code expands into social and psychological realms, regulating behaviour between people and the machines they interact with.' (Ibid.)[2] Such a position has its own implicit relation to media ecology (Fuller 2005) and is inherent to the hacktivist politics of critical engineering. However, even the references to hacktivism are misleading, as the notion of the critical engineer is meant to complement the idea of agency in art discourse.

So could we work this into a revised plea for a philosophy of engineered systems and public real time data networks – but one that starts from this other dimension of (mis)use and activism? Taking engineering as the starting point might invite some criticism concerning a slightly too technologically focused understanding of politics and practice, but it does however provide an extended

philosophy of excavating deeper than the polished, sanitized surface. It is not afraid to get its hands dirty, which besides a nice metaphorical relation to 'dirty' hacking practices, can be related to longer genealogies of purification of public space from excrement, and the current digital culture defined by such a polished surface. (Cox 2013: 75).

The beneath-the-surface regimes of technology, explored by the Critical Engineering manifesto and Weise7-projects does not denounce the social at all, but attempts to 'reconstruct user-constraints and social action through means of digital excavation' (Oliver, Savičić, Vasiliev, 2011). Excavation becomes a related figure or concept for such action, and one that transports media archaeology into a current political methodology. It also expands media archaeology's often non-political nature to take into account the engineered political economy of contemporary network structures and devices.

The project 'Newstweek', unfolding behind a spitting image of corporate-styled imagery and brand names, assigns itself into such 'network fixing', combining the discourse of mind control with network control. The discourse of media technological power that is familiar from the aforementioned Kittler-Pynchon trajectory of thought, often fixating on military contexts, is here extended to the corporate news world. The discourse of fact and mind control is located concretely in the technologies of wireless(ness), pinning down the ephemeral milieu into hotspots as the hub of potentials for exploits. Winner of the Golden Nica in Interact Arts at Ars Electronica 2011, Newstweek inserts itself into the politics of democratic discourse but through an observation and tweeking of network structures. The hierarchical structure of news organisations and reality creation, which in itself is not 'news' to any media studies scholar, is analysed through the simple news production-router-end user/computer situation in places of wirelessness: cafes, universities, hotels, libraries and so forth (see Mackenzie 2010). By placing itself between the router and the user's computer, hiding itself as inconspicuous wall plug, the device continues the lineage of 'data hijacking' discussed in Critical Engineering discourse. The Newstweek device reroutes and intervenes in the news passed on to the net browsers of users, and inserts manipulated news content. According to the engineers Oliver and Vassiliev, it provides 'opportunity for citizens to have their turn to manipulate the press; generating propaganda or simply 'fixing facts' as they pass across a wireless network. As such, Newstweek can be seen as a tactical

device for altering reality on a per-network basis' (Newstweek, 2011). Network politics starts from routes and routing. If platforms' functionality in the neoliberal capitalist context is based on trust – trusted interactions between users, economic exchange, information – then one can begin to understand the tactical function of playing with the easily producible cracks in trusted platform sociability.

As such, the device located in the infrastructures sustaining wireless traffic in cafes and other public places is what for this project, and some aspects of Critical Engineering, is pivotal in challenges to the control of space and critical infrastructure. It exposes how infrastructure is in most cases less stable than it seems. It also leaks data on many fronts, intervening in negotiations of public and private, also more broadly in wireless infrastructures across cities. (See Bucher 2011 for Oliver on modern cities and rationalisation of space).

At the network level, such concerns about infrastructure relate to discussing and engineering proprietary transmissions and routing, and are more specifically examined in the manifesto's point seven with regards to how the 'The Critical Engineer observes the space between the production and consumption of technology. Acting rapidly to changes in this space, the Critical Engineer serves to expose moments of imbalance and deception' (Oliver, Savičić, Vasiliev, 2011). The space of the wireless *in-between* functions as a possibility for intervention – for an evil trickster – or at least for a more gentle data hijacker. It also shows the possibility of extending media artistic/hacktivist methodologies into direct contact with discourse of network politics. In addition, it illuminates interesting possibilities in addressing the ontology of networks themselves through the already briefly mentioned themes of psychology, user experience, and what below are approached through dreams, zombies and other forms of involuntary agency that increasingly characterise network culture.

The Urban Wireless Nonconscious

The full passage of the above quoted reference to excavation underlines this relation between heterogeneous realms – a media ecology of sorts that binds the social, the psychological and the machinic:

The Critical Engineer notes that written code expands into social and psychological realms, regulating behaviour between people and the machines they interact with. By understanding this, the Critical Engineer seeks to reconstruct user-constraints and social action through means of digital excavation. (Oliver, Savičić, Vasiliev, 2011)

A lot of the discourse and the ideas put forward by both the Critical Engineering manifesto and the Weise 7 exhibition, points towards a specific understanding of networks. Elaborated in relation to the city architectures and informationalisation (Savičić, 'CPU City') and, for instance, to alternative public data transportation systems (Netless, Vasiliev), these various investigations of network topology refrain from a simple discourse of nodes and edges, and of rational, even if distributed, agencies (hive intelligence, etc.). Nonetheless, what is closer to the ideas elaborated in these works as well as earlier mentioned ones concerning data hijacking and Tempest, is the idea of much lower-level background transmission event characterising (wireless) networks. The networked environments become characteristic of non-user controlled 'zombie' processes, whereby involuntary and unconscious events and the language of psychology ('code expands into social and psychological realms') are entangled with networks to produce reality. This idea, in Newstweek as well, is what binds to notions such as the technological unconscious. This is approached here, however, through imagining a *technological* unconscious for the political. Indeed, the technological wireless infrastructure is implicitly taken as the backbone for reality creation, and as the backbone for politics. What Jacques Rancière (2004: 12) calls the distribution of the sensible, we can extend to a more engineered notion: 'The apportionment of parts and positions is based on a distribution of spaces, times, and forms of activity that determines the very manner in which something in common lends itself to participation and in what way various individuals have a part in this distribution' (Cf. Massumi 2011, 170-171). Take that description however as a technological one, and imagine the levels of wireless and more widely network technology that contribute to such a distribution, and you have another way to approach Critical Engineering and Weise 7-projects.

The concept of the technological unconscious (or non-conscious) has recently been mobilized by Nigel Thrift and picked up by N. Katherine Hayles to illuminate the work of technology as part of

human cognition. In her words, the notion registers the intimate effects of informational machines on human behaviour, especially in the age of increasingly environmental notions of computation.

> As computation moves out of the desktop into the environment with embedded sensors, smart coatings on walls, fabrics, and appliances, and radio frequency ID (RFID) tags, the cognitive systems entraining human behaviour become even more pervasive, flexible and powerful in their effects on human conscious and non-conscious cognition. (Hayles 2008: 28)

This is where techniques of data sniffing and data hijacking fit in perfectly as illustrations of the wider milieus of electromagnetic, wireless media as such 'spheres' of technological non-conscious; background processes which however continuously producereality in the sense that Deleuze and Guattari think of the unconscious: it does not act as a representational theatre, but is to be conceived as the arena for the *production* of reality. (See also Fuller & Goffey 2009, 143 on sorcery and reality production).[3] What Newstweek does is a critical engineered version of this, which also resonates with the evil media ideas of Fuller and Goffey. They use the idea of 'sorcery' to refer to function of power. By mobilizing archaic practices, they elaborate this in terms of how it suggests a notion of reality which can be adapted to media studies investigations too.

Besides such a glitch approach, projects like Vasiliev's 'Netless' illuminates the other connection to 'zombie processes' as network(ing) techniques. Netless is a different way of understanding the politics of wireless infrastructures that takes as its critical point of departure the monitorability of proprietary networks. Netless *imagines through engineering* an alternative city scape-cum-wireless communication (sneaker)network that bypasses existing internet and wireless infrastructure, but which still affords that 'data exchange between the participants can be easily tracked down… many internet service providers consider deep-packet inspection (DPI) and traffic shaping a necessary part of their business, undermining the neutrality of the network' (Vasiliev 2012).

As he outlines in the project introduction (Vasiliev 2012), even if darknets and Tor are able to offer alternative message spaces, access to the Internet is still heavily regulated as a customer relation. Hence, as an engineered piece of creative speculation, Netless taps

into the city infrastructure as an affordance for communication. Vasiliev refers to the idea of sneakernets (networks based on physical carriers, such as USB sticks transported person to person as a form of data transfer) where communication relay points are connected to the moving nodes of the city, such as buses and trams so that 'whenever those vehicles pass by one another a short-range wireless communication session is established among the approaching nodes and the data they contain is synchronized.' (Vassiliev, 2012). These data packets can then be 'received and sent to using any wifi enabled device – a laptop, pda or mobile phone' (Ibid.). With a familiar reference to viral patterns of information spread across the city transport networks (illuminating a further way to understand transport as media), the political nature of such a wireless system becomes evident through its untraceability – 'there are no addresses or routes in the netless network – any participant can potentially receive all data circulating in the network – all data is broadcast' (Ibid.).

The 19th and early 20th century sociological theme of the anonymous city experience and urban crowds becomes related to data 'crowds' as well. This is articulated in relation to how to one can bypass the data sniffing and packet inspection techniques through reimagining – and re-engineering – network infrastructures. In this sense, infrastructure becomes critical, as it is imagined through this automated zombie network of vehicles, innocently becoming infected, message carriers themselves. Such a reference to zombies, parasites, botnets, viruses, sneaking and somnambulism is made to employ the idea of cultural techniques of the unconscious and barely-alive to make sense of the processes of contagion as well as non-semantic communication (see Sampson 2011; 2012).

This adds a further dimension to the psychographical task of mapping the zones of experience of urban space. This makes sense when reflecting the work of the critical engineer as someone who maps the connections across such dimensions of technology, the social and the psychological in a media ecological manner. But it is also a media ecology that is cartographic, and maps these forces that constitute urban experience. And yet, it maps not only urban space, but by actively engineering it into a data transmission space, adds its own further media ecological layer of information to it. This too is about mapping the city but through actively tapping into its existing patterns of movement that form a crucial part of its modern legacy: trams and buses, for instance, as an expression of the logistics of city life, which itself is related to media technologies (Kittler 1996) and

which now are further layered by such 'transport vectors'. While 'proximity' might have been a theme for the earlier sociology of crowds and affect, the reliance on closeness (within wireless reach distance) now becomes   a different sort of affordance for a communication theory of affective transmission (Sampson 2011): data having its own relations, affects, as part of the architecture and transport routes.
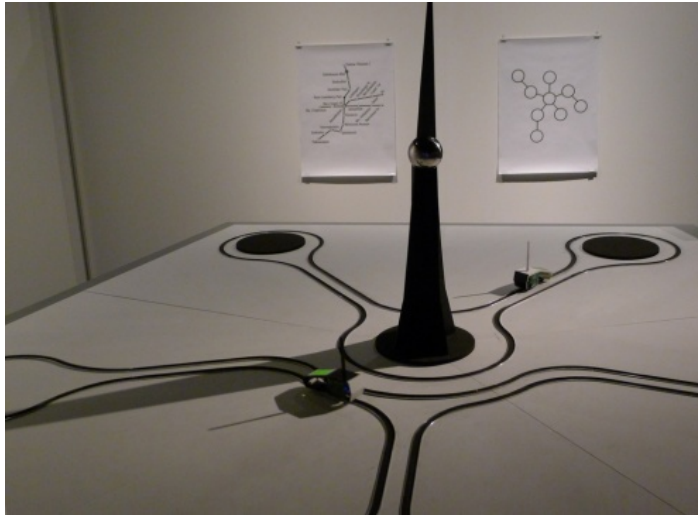

Figure 4. Vasiliev's Netless wireless communication system.

Information and especially wireless traffic in the city is part of what Mackenzie calls a proliferation of 'conjunctive relations' (2010: 64). They are instrumental in catalyzing, processing, enabling and disabling relations and experiences, and as such, part of the movement of not only information itself, but also people. Indeed, Mackenzie's point concerning wireless technologies actually rewiring the city takes into account the multiscalar ways in which cities are being re-engineered. As well as viewing city transport routes as information nodes and physical carriers on the move, chipsets are regarded as cities themselves, including the totality of wires and conductors as part of their own microscopic scale (Mackenzie, 2010: 65). The internationalization of the urban infrastructure as part of such chip worlds is significant for this particular scale of 'globalisation', and offers a powerful media ecological observation on how the catalysation of experiences and relations works across scales. The architectures of wirelessness crystallised in chip worlds are not removed from the city and its inhabitants, but create a further informational 'city', connected, one could say, to the otherwise 'critical infrastructures' such as 'roads,

pipes, cables, control centers, and ducts' (Mackenzie, 2010: 65). The control and governance of infrastructures as key elements of governance of *people* extends to the way in which the wireless functions. It is such a crucial resource for transactions of commercial and other interests; governance of access, use, as well as spectrum allocation (Mackenzie, 2010: 66), which further highlights the insights of such projects as Netless.

Conclusion

To briefly summarize the argument of this article, I want to refer back to the earlier part concerning the public and publicness. The text has presented a specific media practice that presents issues of the public, the city and especially wirelessness as inherent to the politics of platforms. The practice-based intervention pitched as 'Critical Engineering' by Julian Oliver, Gordan Savičić and Danja Vasiliev is one way to engage with platform politics. It is about 'opening up' wireless networks in order to illuminate some software and hardware related restrictions and affordances. It shows how to approach network and platform politics through art projects that are 'not just art' (Fuller, 2006), but gather momentum in the social contexts of where they function. Platforms can be conceived as software and hardware configurations that enable patterns of sociability to emerge. In this article, critical engineering has been discussed as a way to deceive and tactically poke such configurations so as to cause imbalances that are more than symbolic and act on the level of *engineered* sociability.

In terms of critical engineering as a form of an art practice, if Bruno Latour's (1996) work with engineering has been an inspiring insight into the work of non-human elements as part of wider planning and implementation of issues relevant to the social, then the Weise7-projects take such insights further into interrogations of information infrastructures. More specifically, several of these address wireless communication, and the experimental projects are able to specify issues relating to art methodologies as living, vibrant reality modification tools. They take the approach that engineering is about creations of perceptions, forms of trickstery that could be pitched as a sort of evil media practice (Fuller & Goffey, 2009; 2012). This trickstery resonates with an earlier insight in relation to design, articulated by Vilém Flusser (1999: 20): design and culture start with deception. Another way to underline this point is to argue that through engineering and design, we create modes of sensation,

perception and experience (see also Mackenzie, 2011; Rancière, 2004).

With Weise7, part of this takes place as pedagogic activity too. The Networkshop-workshops by Oliver and Vasiliev embody various similar principles of extending network politics into a hands-on approach to basics of network communication. Indeed, as they introduce the project:

> Ask anyone how the postal system works and they would give a vaguely correct description. Few however would come close to describing how email, let alone a computer network itself, actually functions. With this lack of knowledge comes a risk; we lack the practical understanding to effectively read the infrastructural and political implications of our increased dependency on this technology. (Networkshop, 2012)

The workshop engages with such methodologies of platform politics by demonstrating through the creation of network situations (a small scale model of the internet that interacts with local area network) how network topologies act 'as political control structures' (Networkshop, 2012), Power works in packets and through their routings: 'Students will learn to study these power structures by tracing the flow of packets as they pass over land and sea. Macro-economic and geostrategic speculations will be made' (Networkshop, 2012). The important thing here is to note the articulation of their practice in relation to the triangulation of theory-practice-pedagogy. Indeed, in relation to such ideas as 'critical hacktivism', this practice of pedagogy becomes clearer: as Dan McQuillan (2012a and 2012b) has argued, critical pedagogical practices in design and technology enable such peer-practices and communities (for instance, Social Innovation Camps, http://sicamp.org/) that demonstrate how experimental practices allow even rethinking processes of policy.

In this context of activity and a critical agenda, the 'broke, broke, broke' little wireless network – leaking, vulnerable to data sniffing, capture and distortion, to slightly modify Maxwell's poetic urge – is a great starting point for the investigation of how such grounding political notions related to publicness, democracy and participation leak on very fundamental, technologically engineered levels. We can address such leaks not only through social science methods, but also

with experimental artistic methodologies. Indeed, in this sense to investigate a platform through breaking, exploiting and imbalancing it sets a good example: critical engineering as platform politics.

Endnotes

[1] Foucault (1998: 369): 'Genealogy is gray, meticulous, and patiently documentary. It operates on a field of entangled and confused parchments, on documents that have been scratched over and recopied many times'.

[2] The relation of information and city, on the other hand, is investigated in Savičić's 'CPU City' contribution to the Weise 7-exhibition at Transmediale12: 'This CPU City Model is an undertaking to express a cartography of the usually unseen - a formal printed circuit board layout that blends the logical order with a new world mapping' (Weise 7, 2012).

[3] To quote the passage from Fuller and Goffey (2009, 143):

> Unlike the outmoded model of media spectacle, which simply proffered an image of a 'hidden' or occulted reality, hypnotic suggestion – a fact long known to the inventors of public relations is one of a number of means that are directly productive of a reality. Taking advantage of such mechanisms calls for the delicate negotiation of a different position to that commonly adopted in media studies. For those professionally or even incidentally embedded in media, to say that we are manipulated, that trickery and deception are effectively exercised on a regular basis, is not to deny that people cannot or do not think, but it would be to further deceive and manipulate ourselves to think that rational subjects are not outstripped by events.

References

Anderson, B. (2006) *Imagined Communities. Reflections on the Origin and Spread of Nationalism*. London and New York: Verso.

Beniger, J. (1989) *The Control Revolution.* Cambridge, MA: Harvard University Press.

Berry, D. (2008) *Copy, Rip, Burn: The Politics of Copyleft and Open Source.* London: Pluto Press.

Bucher, T. (2011) 'Network as Material: An Interview with Julian Oliver' Furtherfield 16/6/2011, http://www.furtherfield.org/features/network-material-interview-julian-oliver ,accessed 18.7.2012.

Chun, W.H.K. (2006) *Control and Freedom. Power and Paranoia in the Age of Fiber Optics.* Cambridge, MA: The MIT Press.

Cox, G., with McLean, A. (2013) *Speaking Code. Coding as Aesthetic and Political Expression.* Cambridge, MA: The MIT Press.

Ebeling, K. and Günzel , S. (2007) *Archivologie. Theorien des Archivs in Philosophie, Medien und Künsten* Berlin: Kadmos.

Ernst, W. (2013) *Digital Memory and the Archive.* J. Parikka (ed.), Minneapolis: University of Minnesota Press.

'European Sub-Marine Telegraph', *Scientific American,* May 19 1855, Vol. 10, issue 36.

Flusser, V. (1999) *The Shape of Things. A Philosophy of Design.* London: Reaktion.

Foucault, M. (1998) 'Nietzche, Geneaology, History' in *Essential Works of Foucault vol. 2, Aesthetics, Method and Epistemology,* (ed).. James D. Faubion, 369-391.

Friedman, J. (1972/2007) 'Tempest: A Signal Problem'. *NSA Cryptologic Spectrum,* Summer.

Fuller, M. (2005) *Media Ecology. Materialist Energies in Art and Technoculture.* Cambridge, MA: The MIT Press.

Fuller, M. (2006) *Softness: Interrogability; general intellect; art methodologies in software.* University of Huddersfield Digital Research Unit.

Fuller, M. & Goffey, A. (2009) 'Toward an Evil Media Studies'. In: J. Parikka & T. Sampson (eds), *Spam Book. On Porn, Viruses and Other Anomalous Objects from the Dark Side of Digital Culture.* Cresskill, NJ: The Hampton Press, 141-159.

Fuller, M. & Goffey, A. (2012*) Evil Media*. Cambridge, MA: The MIT Press.

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

Gardey, D. (2008) *Ecrire, calculer, classer. Comment une révolution de papier a transformé les sociétés contemporaines (1800-1940).* Paris: la Découverte,

Genosko, G. (2012) *Remodelling Communication. From WWII to the WWW.* Toronto: University of Toronto Press.

Gillespie, T. (forthcoming). 'The Relevance of Algorithms.' In: *Media Technologies*, by Tarleton Gillespie, Pablo Boczkowski and Kirsten Foot. Cambridge, MA: MIT Press.

Hayles, K. (2008) 'Traumas of Code' in A. Kroker & M. Kroker (eds), *Critical Digital Studies. A Reader.* Toronto: University of Toronto Press, 25-44.

Kittler, F. A. (1990) *Discourse Networks 1800/1900.* Trans. M. Metteer, with C. Cullens. Stanford, CA: Stanford University Press.

Krajewski, M. (2010) 'Ask Jeeves: Servants as Search Engines' trans. Charles Marcrum II, *Grey Room* 38, Winter 2010, 6-19.

Krajewski, M. & Vismann, C. (2007) 'Computer Juridisms.' *Grey Room* Fall 2007, No. 29: 90–109.

Latour, B. (1996) *Aramis, or The Love of Technology.* Trans. Catherine Porter . Cambridge, MA: Harvard University Press.

Latour, B. & Weibel, P. (2005) *Making Things Public. Atmospheres of Democracy* Cambridge, MA: The MIT Press and ZKM.

Mackenzie, A. (2010) *Wirelessness. Radical Empiricism in Network Cultures*. Cambridge, MA: The MIT Press.

Mahon, B. (2003) *The Man Who Changed Everything: The Life of James Clerk Maxwell.* Hoboken, NJ: Wiley.

Massumi, B. (2011) *Semblance and Event. Activist Philosophy and the Occurrent Arts.* Cambridge, MA: The MIT Press.

McQuillan, D. (2012a) 'Critical Hacktivism' blog post at http://www.internetartizans.co.uk/critical_hacktivism 31/7/2012.

McQuillan, D. (2012b) 'Could Prototyping Be the New Policy?' *The Guardian Professional*, 28/5/2012. http://www.guardian.co.uk/

Netless, Project webpage (Danja Vasiliev), http://k0a1a.net/danja/netless2, accessed 18.7. 2012.

Networkshop (2012) Workshop website at http://weise7.org/labor-berlin-8-workshops, accessed 11.7.2012).

Newstweek, project website http://newstweek.com/,accessed 11.7.2012).

Oliver, J., Savičić, G., Vasiliev, D. (2011) Critical Engineering Manifesto, The Critical Engineering Working Group, November 2011, Berlin, online at http://criticalengineering.org/, accessed 11.7. 2011).

Parikka, J. (2010) 'Ethologies of Software Art: What Can a Digital Body of Code Do?' in S. Zepke & S. O'Sullivan (eds), *Deleuze and Contemporary Art*. Edinburgh: Edinburgh University Press, 116-132.

Rancière, J. (2004) *The Politics of Aesthetics*. trans. Gabriel Rockhill. London: Continuum.

Renzi, A. & Elmer, G. (2012) *Infrastructure Critical. Sacrifice at Toronto's G8/G20 Conference.* Winnipeg: Arbeiter Ring.

Sackman, H. (1968) 'A Public Philosophy for Real Time Information Systems'. *Fall Joint Computer Conference*, 1968, 1491-1498.

Sampson, T. (2011) 'Contagion Theory Beyond the Microbe' *Ctheory*, 1/11/2011, http://www.ctheory.net/articles.aspx?id=675.

Sampson, T. (2012) *Virality. Contagion Theory in the Age of Networks.* Minneapolis: University of Minnesota Press.

Suominen, J. & Parikka, J. (2010) 'Sublimated Attractions – The Introduction of Early Computers in Finland in the late 1950s as an Audiovisual Experience' *Media History.* 16:3 (November), 319-340.

Vasiliev, D. (2012) 'NETLESS/independent, urban communication platform', project abstract, http://k0a1a.net/netless

Vismann, C. (2008), *Files*, trans. G. Winthrop-Young. Stanford, CA: Stanford University Press.

Wark, M. (2004) *The Hacker Manifesto*. Cambridge, MA: Harvard University Press.

Weise 7 (2012) 'The In/Compatible Laboratorium', curated by Kristoffer Gansing, http://weise7.org/labor-berlin-8.