**Munro I.**

**Organizational resistance as a vector of deterritorialization: The case of WikiLeaks and secrecy havens.**

***Organization* (2015)**

**DOI: 10.1177/1350508415591362**

# Organizational Resistance as a Vector of Deterritorialization: the case of WikiLeaks and Secrecy Havens

> 'We do not lack communication. On the contrary we have too much of it. We lack resistance to the present.' (Deleuze and Guattari, 1994: 108).


## Abstract

This paper investigates the relations of power and resistance manifest by the WikiLeaks network. The primary research question of this inquiry is, 'what power relations and possibilities for resistance are presented by WikiLeaks as a novel form of network organization?' The paper shows that WikiLeaks has been able to exert influence from the periphery of existing networks by exploiting vectors of 'deterritorialization' to destabilize existing power relations. The paper contributes to the literature on the network organization by developing an account of resistance to State and corporate power in terms of an 'absolute deterritorialization.' This idea has important implications for the tactics of resistance in network organizations, where vectors of deterritorialization have become a defining feature of resistance tactics of the WikiLeaks network.


## Introduction

This paper investigates the power relations and tactics of resistance of the WikiLeaks network in terms of its processes of 'deterritorialization' and 'reterritorialization'. The WikiLeaks network has been one of the most influential and controversial network organizations of the past decade[i]. The tactics of resistance of WikiLeaks have focused

on its inversion of existing hegemonic systems of surveillance, where this network has attacked the 'secrecy havens' of the powerful and endeavoured to create its own anti-secrecy havens. This analysis demands that we move beyond the boundaries of the workplace which has characterized much of the existing scholarship on organizational resistance (Alvesson and Willmott, 1992; Bain and Taylor, 2000; Ball and Wilson, 2000; Contu, 2008; Courpasson et al., 2012; Fleming and Spicer, 2003; Jermier, et al, 1994; Knights and McCabe 2000, 2003), and situate tactics of resistance within a broader context of socio-political processes of deterritorialization in order to explain how WikiLeaks has destabilized existing relations of power.

The profound creativity of network forms of organization has already been the subject of much research within organization studies and the sociology of organization (Borgatti and Foster, 2003; Brass, et al. 2004; Castells, 1996, 1997, 2012; Demil and Lecocq, 2006; Miles and Snow, 1992; O'Mahony and Bechky, 2008; Podolny and Page, 1998; Terranova, 2004; Wallemacq, 1998). Brass et al. (2004) have observed that a crucial aspect of the dynamics of network organizations is that they may be transformed from 'above' by their environments as well as from 'below' by their constituent elements. Existing studies of network organizations have revealed their economic potential in terms of their greater adaptability and creativity (Brass et al., 2004; Castells, 1996; Miles and Snow, 1992; Podolny and Page, 1998), and in terms of their development of governance systems that are designed to exploit network externalities (Demil and Lecocq, 2006; O'Mahony and Bechky, 2008; Von Hippel, 2001). New forms of organizational network have been pioneered in the open source community which have led to radical changes in organizational governance and the way that boundaries are negotiated and collaborations formed by organizations (Demil and

Lecocq, 2006; O'Mahony and Ferraro, 2007; O'Mahony and Bechky, 2008; Von Hippel, 2001; Von Hippel and Von Krogh, 2003). As well as being understood as a fertile site of innovation and productivity, the network organization has also been recognized as the site of social and political conflict (Castells, 1997, 2012; Lash, 2002; Tarrow, 2011, Terranova, 2004).

Existing research within organization studies on organizational networks has tended to focus on areas characterized by a convergence of interests (e.g. Brass et al., 2004; Demil and Lecocq, 2006; O'Mahony and Ferraro, 2007; O'Mahony and Bechky, 2008; Von Hippel, 2001; Von Hippel and Von Krogh, 2003). Radical conflict within networks has been the subject of study within other social sciences (e.g. Castells 1996, 1997, 2012, 2013; Lash, 2002; Tarrow, 2011; Terranova, 2004), but has yet to receive sufficient attention within the field of organization studies. Ball's (2005: 92) incisive analysis of power and resistance in contemporary organizations has highlighted the emergence of networks of 'surveillance rhizomes', where the 'central problematic is how to observe and analyse resistance in the absence of the large-scale formal protest and collective antagonism witnessed in the mid-20th century.' More recent events such as the Arab Spring of 2011 and the Occupy Movement have led Manuel Castells (2012) to argue that network organizations have played a crucial role in recent democratic struggles and the creation of 'spaces of autonomy' that lie beyond the reach of oppressive State control, where WikiLeaks has itself emerged as one such network. The present paper analyzes the tactics of resistance developed by the WikiLeaks network that invert existing hegemonic systems of surveillance by supporting privacy for the weak and transparency of the powerful.

This paper investigates the changing power relations and possibilities of resistance of network organizations by drawing upon Deleuze and Guattari's (1988, 1994) conception of 'deterritorialization' and 'reterritorialization'. The paper shows that WikiLeaks exploits vectors of deterritorialization to destabilize existing power relations and has thus been able to exert influence from the periphery of existing networks. This idea has important implications for the tactics of resistance in network organizations, where these tactics entail the deterritorialization of WikiLeaks' own activities and the reterritorialization of the activities of corporations. The main research question driving this inquiry is, 'what power relations and possibilities for resistance are presented by WikiLeaks as a novel form of network organization?' The paper makes three contributions to the understanding of power in network organizations: i) it shows how power can be exercised by organizations on the periphery of existing networks rather than as a function of central nodes, ii) it explains the destabilization of existing power relations in terms of the concepts of deterritorialization and reterritorialization, iii) and it explains the effectiveness of tactics of resistance of networks to the extent that they approach an 'absolute deterritorialization'.

The paper builds a case study of WikiLeaks based upon a diversity of sources in the public domain. These sources include first hand accounts of WikiLeaks that have been published by individual insiders who have worked for this organization and from the extensive data available on the website itself (Assange, 2011; Assange et al., 2012; Beckett and Ball, 2012; Domscheit-Berg and Klopp, 2011; WikiLeaks.org). In addition to these first hand accounts data has also been taken from leaked reports on WikiLeaks by the European Commission (2012) and from supporting secondary commentary in the media and academic sources (Amnesty International, 2011;

Brevini et al., 2013; Fuchs, 2011; Greenberg, 2012; Hood 2012; Leigh and Harding, 2011; Roberts, 2012; Sifry, 2011). The analysis of data is based on Eisenhardt's (1989) methodological principle of 'enfolding literature' by means of which existing conceptual developments are refined with reference to new empirical case studies. This approach to conceptual development is only partially inductive in its use of empirical material, drawing upon and refining existing philosophical concepts for the purposes of organizational analysis.

This paper begins with a review of the literature on network organizations followed by an analysis structured around five major vectors of 'deterritorialization' and 'reterritorialization' of the WikiLeaks network: i) WikiLeaks as a boundary spanning 'disorganization', ii) its distinctive role as the first 'Stateless' news organization, iii) its revelation of 'secrecy havens' that have been created to avoid democratic oversight and regulation, iv) the emergence of a system of extra-judicial control formed by a hybrid of State agencies and corporations in an attempt to undermine the activities of WikiLeaks, and v) attempts that have been made to 'reterritorialize' WikiLeaks by organizations that wish to attack it.

**Networks and Power**

The literature on network organizations contrasts the emergence of network forms of organization as flexible, adaptable, horizontal structures of authority with previous highly structured bureaucratic forms (Brass, 2004; Castells, 1996, 1997, 2013; Demil and Lecocq, 2006; Miles and Snow, 1992; Podolny and Page, 1998). This picture of open horizontal networks is complicated by studies of organizations that have shown

how networks have also been used to intensify power relations through new forms of surveillance (Ball, 2005; Bain and Taylor, 2000; Burrell, 1988; Clegg, and Baumeier, 2010; Lyon, 1994; Munro, 2000).

In their review of the mainstream literature on the network organization Brass et al. (2004: 798) concluded that 'actors in *central network positions* {italics inserted} have greater access to, and potential control over, relevant resources, such as information in a communication network.' Even in this rather functionalist perspective issues of power and control remain a pervasive feature of the network organization. From a more critical perspective Munro (2000) and Ball (2005) have described how networks of surveillance are beginning to supplement and supplant traditional panoptic forms of organizational control. Ball (2005) has demonstrated the emergence of networks of free-floating control that deploy technologies increasingly detached from particular sites of confinement which she terms 'surveillance rhizomes'. Others have described an intensification of social surveillance in terms the 'synopticon' which entails a reversal of hierarchical panoptic relations where communications networks are enabling the many to watch the few (Bauman, 2000; Clegg and Baumier, 2010; Mathiesen, 1997). Despite the relatively participative and democratic façade of these synoptic networks Mathiesen (1997: 225) notes that, 'even in the most interactive media, the basic conditions are increasingly … set from above rather than from below… though they may still contain the illusion of two parties on an equal footing.' This literature has done well in describing the ongoing transformation of organizational power relations in terms of the intensification of networks of surveillance, but less attention has been paid to the forms of resistance that are arising in opposition to these new networks.

In contrast to existing research that has tended to focus upon the intensification of surveillance (Ball, 2005; Bain and Taylor, 2000; Clegg, and Baumeier, 2010; Lyon, 1994; Munro, 2000) and instances of micropolitical resistance against corporate control (Alvesson and Willmott, 1992; Bain and Taylor, 2000; Ball and Wilson, 2000; Contu, 2008; Courpasson et al., 2012; Fleming and Spicer, 2003; Jermier, et al, 1994; Knights and McCabe 2000, 2003), the present paper focuses upon 'lines of flight' beyond these centres of power. An emerging literature has begun to look outside the boundaries of the workplace for sources of resistance that are developing on the periphery of centres of power, particularly in the formation of counter-hegemonic networks by social movement organizations (Böhm, et al, 2008; Davis et al, 2005; Kraemer, et al., 2013; Spicer and Böhm, 2007; Spicer and Van Bommel, 2011). The present paper extends this literature by showing how the new tactics of resistance developed by WikiLeaks are attempting to build counter-hegemonic systems of surveillance to reveal and oppose the 'secrecy havens' of corporate power.

Manuel Castells (1996, 1997, 2012, 2013) is perhaps the preeminent social theorist of power and resistance in the network society today. In his early commentary on the rise of network organizations he claimed that this was directly related to a decline of traditional hierarchical forms of power where power 'is no longer concentrated in institutions (the state), organizations (capitalist firms), or symbolic controllers (corporate media, churches)' (Castells, 1997: 359). Castells has since revised this conception of power, and in his recent work he has developed a technocratic analogy between power and computer programming where power networks are described as being

composed of ‘programmers’ and ‘switchers’ (Castells, 2012, 2013). He explains this distinction in the following terms:

> “…who holds power in the network society? The programmers with the capacity to programme each one of the main networks on which people’s lives depend (government, parliament, the military and security establishment, finance, media, science and technology institutions, etc.) And the switchers who operate the connections between different networks (media moguls introduced in the political class, financial elites bankrolling political elites…)” (Castells, 2012: 8-9).

In this revised definition, Castells argues that corporations and the State still hold significant power as central nodes in global networks of power in their new role as ‘programmers’ and ‘switchers’. Following this logic he explains that resistance to power occurs when people are ‘able to invent new programmes for their lives’ (Castells, 2012: 9). However, this technocratic analogy between power and computer programming is in danger of reducing the complex political conflicts that underpin network organizations to the relatively uncontentious matter of writing new code.

The concept of ‘deterritorialization’ is particularly suitable for analyzing the power relations of the network organization, where ‘power centers are defined much more by what escapes them or by their impotence than by their zone of power’ (Deleuze and Guattari, 1988: 217). Rather than seeing organizations as structures, Deleuze and Guattari (1986, 1988) argue that they are better understood in terms of the ‘lines of flight’ and the processes of ‘deterritorialization’ by means of which they are transformed (see also Brighenti, 2010; Elden, 2005; Linstead and Thanem, 2007). Paul

Patton (2012: 208) provides a concise but broad definition of deterritorialization as the 'movement or process by which something escapes or departs from a given territory, where a territory can be a system of any kind: conceptual, linguistic, social, or affective' (see also Deleuze and Guattari, 1988: 508)[ii]. Deleuze and Guattari (1988, 1994) primarily employ the term in their description of social formations such as nomadism, capitalism and the State (also see Elden, 2005). They distinguish between two general forms of deterritorialization, i) 'relative deterritorializations', which are subsequently reterritorialized in order to be exploited by power - for instance during the Industrial Revolution peasant labour was 'freed' from working on the land only to be reterritorialized as wage labour within the factory - and ii) 'absolute deterritorializations' which outpace attempts to recapture them, such as forms of nomadism. They argue that resistance to post-industrial capitalism requires an 'absolute deterritorialization' that entails the creation of new forms of 'resistance to the present' (Deleuze and Guattari, 1994: 108).

Existing research within the field of management and organization studies has already proposed that Deleuze and Guattari's concepts of the 'rhizome' and the 'nomadic war machine' can be used to understand transformation and creativity in modern organizations and organizational networks (Ball, 2005; Blaug, 1999; Chia 1999; Clegg et al., 2005; Linstead and Thanem, 2007; Sorensen 2005; Thanem, 2011). Historically, processes of deterritorialization have been crucial in the development of capitalism itself. Deleuze and Guattari (1988, 1994) show how the power of capitalism has been intensified through the circulation of deterritorialized flows of wealth and how State power has also been intensified through military-technological forms of deterritorialization (e.g. naval and air power). The emergence of network organizations is a key part of

this historical dynamic where, 'Organizational networks can be understood as vectors of deterritorialization that traverse national and geographic borders and are then reterritorialized within organizations through processes of ownership and access rights, such as branding and the imposition of intellectual property rights.' (Marachel et al., 2013: 200). The present study builds on these insights, with a focus on the relations of power and resistance in the ongoing mutation of the network organization. In the case of WikiLeaks, this paper shows that this network's ability to mobilize political and organizational resistance is characterized by the specific vectors of deterritorialization and reterritorialization that have been constitutive of the network's development.

In order to provide an adequate account of the contextual forces that underpin the development of WikiLeaks it is necessary to investigate the "cross level pressures" (Brass, et al., 2004) that have characterized its emergence. Difficulties arise with confining the analysis of network organizations to a single level because "levels of analysis… do not necessarily correspond in a simple way to the type of entities being studied" (Borgatti and Foster, 2003: 1001). Therefore, the present study undertakes a cross level analysis of WikiLeaks which encompasses the actions of isolated whistleblowers, the inter-organizational alliances formed with WikiLeaks, hacker groups, media corporations and social movement organizations, and a macro-level analysis of the broader political forces at work related to secrecy havens and the alliance between big business and the national security establishment. The analysis necessarily crosses between these different levels in its identification of the diverse vectors of 'deterritorialization' and 'reterritorialization' of the WikiLeaks network. We now turn to an analysis of the specific vectors of deterritorialization that have been exploited by the WikiLeaks network.

**WikiLeaks as a Boundary-Spanning 'Disorganization'**

One of the most puzzling characteristics of WikiLeaks is the difficulty in categorizing it in terms of traditional organizational forms, where it has been variously called a hacker organization, a whistleblowing organization, a publisher of the last resort, and a human rights organization (Beckett and Ball, 2012; Brevini et al., 2013; Leigh and Harding, 2011). It has emerged in collaboration with a variety of different organizations including hacker groups (e.g. the Chaos Computer Club, the Electronic Frontier Foundation), media organizations (e.g. The Guardian, The New York Times, Der Spiegel, El Pais), and social movement organizations (e.g. Amnesty International) in order to disseminate its message. To some extent WikiLeaks might be understood as a manifestation of what Scott Lash (2002) has termed a 'disorganization'. According to Lash the evolution of the network society has witnessed a proliferation of disorganizations. He argued that, 'Disorganizations are less local, less fixed, more often globally dispersed, constantly changing and literally on the move than are normal organizations.' (Lash, 2002: 40). Following Deleuze and Guattari, he described disorganizations as 'rhizomes' that spread across organizational boundaries. WikiLeaks exists on the boundaries of many other organizations and as such acts as a distinctive type of 'boundary organization' (O'Mahony and Bechky, 2008), which has rapidly changed its form as it has come into contact with and developed new alliances with these organizations.

The rapid mutation of WikiLeaks can be described in terms of three distinctive stages of development (Sifry, 2011). In the first stage of its development WikiLeaks was a

wikipage for raw information from leakers and whistleblowers, which could be used as a valuable resource by social activists and citizen journalists. The second stage of development was like the first with the addition of information edited and processed by members of the WikiLeaks network themselves, which emerged in an effort to encourage greater public attention towards the information posted on the site. Finally, the third stage of the organization's development witnessed the formation of a stronger alliance with the media to include information edited by select members of the traditional news media. At this stage WikiLeaks began to characterize itself less as a whistleblower platform and more in journalistic terms as a 'publisher of the last resort' (Assange, 2011). WikiLeaks has mutated rapidly as it has come into contact and developed alliances with a variety of outside organizations and has proven to be a highly unstable organizational form characterized by numerous vectors of deterritorialization as we shall see in the ensuing analysis.

**The Rise of the First Stateless News Organization**

WikiLeaks has endeavored to protect itself from corporate and State retaliation by identifying and exploiting favourable national laws in various countries in order to protect its sources, its content and the circulation of the leaked documents that it receives. It exploits the relatively deterritorialized nature of cyberspace in order to protect the identity of its sources. WikiLeaks has been 'mirrored' on hundreds of Internet sites in an effort to circumvent censorship by any particular nation state (The New York Times, 5.12.2010). It locates its servers in those countries that have the most favourable and open censorship laws (Assange, 2011; Domscheit-Berg and Klopp, 2011). In some respects this development reflects the tactics of the organizations that

it is opposing, rendering itself untouchable by moving to locations where more favourable laws apply. WikiLeaks is part of a deterritorialized flow of information, and in particular information that corporations and States have taken steps to ensure is kept secret. As corporations have endeavoured to make their activities invisible by locating them in poor, third world countries (Bakan, 2004), WikiLeaks has made their activities visible again in cyberspace. The nature of WikiLeaks was conceived in deterritorialized terms as part of a global movement for the free flow of information, as we can see from accounts given by its founding members:

> "A home is not an easy thing to contemplate when it comes to WikiLeaks: we have active servers operating at secret locations all over the world; we have a network of staff and contacts, most of them wishing to remain nameless, who are never found in the same place at the same time. WikiLeaks was different from any other kind of media organization: we were never going to have a reception desk or a coffee machine…" (Assange, 2011: 173)

> "Our servers were *located in countries with the most favorable laws* {italics inserted} and the best protection of sources." (Domscheit-Berg and Klopp, 2011: 125).

> "WikiLeaks' fundamental exceptionalism is that it is outside of a specific geographical legal framework. This gives it a large degree of immunity from normal legal sanctions on the media." (Beckett and Ball, 2012: 94).

> "… maybe we are a *post-state organization* {italics inserted} because of the lack of geographic control. I don't want to take this analogy too far, because I am under house arrest." (Assange et al., 2012: 128)

The deterritorialization of WikiLeaks is clearly apparent in its 'multi-jurisdictional' design where it has been explicitly 'structured in such a way to make use of those laws we have in this world that were created in times of openness and a vision of transparency, freedom of speech and protection of the press. It therefore is a project homed in all those countries of the world that offer protection to the revelatory work it is doing' (WikiLeaks.org/wiki/Draft:FAQ1). These tactics can be described as a 'vector of deterritorialization' where the earth 'ceases to be land, tending to become simply ground… or support' (Deleuze and Guattari, 1988: 381-382).

Giorgio Agamben (1995: 77) has observed that rendering people Stateless can be a biopolitical mechanism of power for dehumanizing and reducing them to 'bare life'. In the present case the 'Stateless' condition of WikiLeaks has played a somewhat ambivalent role in the evolution of the network. On the one hand, its Stateless condition has been exploited to protect WikiLeaks from State censorship, but on the other hand Assange has asked for protection and political asylum from those States that are sympathetic to his cause. Assange himself refers to the work of the Soviet dissident Alexander Solzhenitsyn in his discussion of protest as a form of Stateless activity. He discusses an incident in the novel *The First Circle* where Solzhenitsyn describes a person's induction into the prison system: "When filling in a form and asked for his nationality he puts not 'Russian,' but 'Prisoner'. His mind is set upon inventions and he feels he is nothing if not stateless.' (Assange, 2011: 92). Assange has been made

acutely aware of his relatively deterritorialized status as a political asylum seeker trapped in the Ecuadorian Embassy in London. Whilst he is not formally a prisoner in the embassy, Assange would be arrested by the police the moment that he set foot outside of this building and he is thus in the paradoxical situation that he must voluntarily confine himself to this building in order to maintain his freedom[iii]. The identity of prisoner transcends that of national identity in what might be termed as a process of deterritorialization. Indeed, the vectors of deterritorialization described by Deleuze and Guattari (1986) are as much concerned with identity as they are concerned with geographical territory.

These geographical arrangements make clear that it would be a mistake to conflate the process of deterriorialization with dematerialization (Cohen, 2007; Elden, 2006; Hayles, 1999). In this respect Julie Cohen's (2007: 225) commentary on the law that governs cyberspace has observed that, 'Debates about information access and control in cyberspace have consequences that bleed over into real space…' She argues that cyberspace is not a disembodied medium of communication and is better understood as a nexus of social practice grounded in real world activities, technologies, and laws. The material aspects of the WikiLeaks case are all too apparent in the power struggles over the relative visibility and invisibility of corporations and whistleblowers, in the concerns for the physical locations of communications terminals and infrastructure, and in the focus on Julian Assange's body as a point of reterritorialization and confinement. The diverse vectors of reterritorialization that surround the WikiLeaks network are discussed in greater detail below.

**The Reterritorialization of Secrecy Havens**

In Julian Assange's (2011) personal account of the WikiLeaks project he describes its aim as revealing the 'secrecy havens' of the powerful that allow their actions to go unnoticed. He picked out Guantanamo Bay and the Cayman Islands as two particular exemplars of such havens, but provides numerous detailed examples of the wider networks that facilitate the operation of such havens that have been revealed by the WikiLeaks network. For instance, one of the earliest leaks revealed by WikiLeaks concerned the embezzlement of over £1bn of Kenyan State funds by former president Moi. The leaks also revealed the complicity of international banks including Barclays Bank and HSBC in the use of tax havens to hide these embezzled funds. Assange (2011: 152) highlights the importance of revealing these 'secrecy havens' to the WikiLeaks network explaining that, "This is exactly the kind of corruption WikiLeaks was set up to reveal. And upending tax havens would be a future hobby of ours." As wealthy corporations and powerful States have endeavored to make their activities invisible by means of legal injunctions and the use of secrecy havens, WikiLeaks has found a way around this by itself becoming a Stateless organization in cyberspace.

One of WikiLeaks' earliest leaks concerned the operations of the Trafigura corporation, which provides a compelling example of the potential of WikiLeaks as a 'vector of deterritorialization'. In 2009 *The Guardian* newspaper and BBC Newsnight attempted to publish stories about the Minton Report on Trafigura, which showed how this corporation had illegally dumped tonnes of toxic waste off the Ivory Coast, poisoning around 30,000 of the nearby inhabitants (Greenpeace, 2010; The Guardian, 17.10.2009). Trafigura succeeded in obtaining a legal injunction against the press both in reporting this incident in the media and in reporting the existence of the in-

junction itself (known as a ‘super injunction’). However, the details of the injunction were leaked to the WikiLeaks website, and not long after the leak had spread across the Internet the High Court lifted its injunction against press coverage of the incident. Of particular note here is that the ‘super injunction’ taken out by Trafigura was not only aimed at the press but also at the British government, where the company had successfully prevented a discussion of its overseas activities in the British parliament. Here we have an attempt by a large corporation to obscure its harmful activities from scrutiny by means of geographical distance and by legal measures, where these measures were then circumvented by a leak of the relevant information to the WikiLeaks network.

WikiLeaks has not only revealed secrecy havens but has also been involved in the establishment of ‘anti-secrecy havens’ (Assange, 2011: 174). Apart from the WikiLeaks project itself, the most successful attempt to create such a haven in practice has arisen from their close involvement with the ‘Iceland Modern Media Initiative’. The IMMI initiative developed from the social upheavals of the Icelandic banking collapse and the political and financial corruption that were exposed in large part by the WikiLeaks network. This proposal has transformed the territory of Iceland into an anti-secrecy haven that offers strong legal protections for freedom of expression, as well as specific legal protections for journalists, publishers, whistleblowers and Internet intermediaries (see https://immi.org/ for an extended commentary on the nature of this haven passed by the Icelandic Parliament in June 2010). Hintz (2013) has described the legal framework of this new anti-secrecy haven as ‘policy hacking’, where WikiLeaks has provided advice to the Icelandic parliament on legislation from a host of countries that

serve as useful models for the creation of a haven for media organizations and activists.

In the so called 'information society' the role of secrecy has taken on a new level of significance not only concerning matters of security (both State and corporate) but also concerning the protection of individual privacy, and in supporting intellectual property rights laws. Secrecy is a crucial concept for the WikiLeaks network where on the one hand the secrets of powerful social institutions, such as corporations and the State, are made more open and transparent, and on the other hand a level of secrecy is given to the weak, in particular to the whistleblowers who may otherwise be victimized by the institutions whose secrets they have revealed (Brevini et al., 2013). In important respects WikiLeaks functions as a double of the State, and even describes itself as being 'the first intelligence agency of the people' (http://wikileaks.org/wiki/Draft:FAQ1).

The control of secrecy is deemed to be such an important factor of State security that encryption technology is classified under US law as being a 'dual use technology' – a tool that can also be used as a weapon where the export of encryption software is regulated as a munition. WikiLeaks explicitly allies itself with the 'cypherpunk' hacker movement which holds that secrecy and privacy ought not to be the privilege of the powerful (Assange et al., 2012; Hughes, 1993). The cypherpunks have developed many tools in order to democratize and promulgate privacy by 'building anonymous systems… defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.' (Hughes, 1993: 2). The secret allows a vector of movement that would otherwise not be possible for such

groups. The practice of secrecy is a key element of what Deleuze and Guattari (1988) have called the 'nomadic war machine'. They note that secrecy is a powerful weapon for social transformation used by elite social groups to maintain their power base as well as by underground insurgent movements in efforts to fundamentally transform the prevailing social order. The revelation of State secrets has clearly been the most contentious aspect of WikiLeaks' operations, which has led to it being denounced as an insurgent operation and a terrorist organization (Domscheit-Berg and Klopp, 2011; Greenwald, 2014; *The Washington Post,* 2010).

Strictly speaking the creation of an anti-secrecy haven entails both vectors of deterritorialization and reterritorialization, where deterritorialized information flows are first protected and circulated by the haven, and may then be subsequently reterritorialized by the State. A key objective of an anti-secrecy haven is to make the activities of corporations more transparent in order to subject them to increased oversight and therefore to 'temper the madness' of capitalism (Deleuze and Guattari, 1994: 98). Despite its deterritorializing manoeuvres within cyberspace, WikiLeaks' finances have emerged as a key tactical vulnerability, which I shall now examine in greater detail.

**The Reterritorialization of WikiLeaks by 'Extra-Judicial' Controls**

Even during the early days of WikiLeaks, measures were being taken by the US Army Intelligence Centre to disrupt its operations, recommending that WikiLeaks be supplied with misinformation in an attempt to discredit it and to initiate legal proceedings against the organization and its leakers in order to: 'damage and destroy this center of gravity and deter others from using Wikileaks.org to make such information public.'

(Hovarth quoted in McCurdy, 2013: 132). Hood (2012) has observed that the operations of WikiLeaks have prompted a massive legal response, including over 100 threatened law suits and secret grand jury proceedings taken against Assange in the USA (Centre for Constitutional Rights, 2012).

Many of the organizations that facilitated its financial transactions have been subject to lobbying and influence from the political establishment in the United States (Benkler, 2011; Brevini et al., 2013). Political, financial and business institutions in the US have built an informal alliance in their campaign to destroy WikiLeaks, depriving it of its financial support. Harvard Law professor Yochai Benkler (2011) has described this as a fundamentally new approach to government, which subverts many of the legal protections provided by the First Amendment. Benkler (2011) notes that WikiLeaks has not been accused or convicted of any crime, and that in the US its activities are protected as a form of freedom of expression under the First Amendment. His analysis of the legal status of the organization highlights an extremely worrying development in the way that government and big business have collaborated in persecuting WikiLeaks that circumvents its First Amendment rights. The US political establishment has managed to persuade major corporations including Amazon, Paypal, Visa, MasterCard and Bank of America, to blacklist WikiLeaks as a customer and thus disrupt both its online presence and its financing. This was most notable from the revelation that Joe Lieberman, chairman of the Senate's Homeland Security Committee, had contacted Amazon.com to stop hosting the WikiLeaks website on its own servers and MasterCard in an effort to persuade them to stop providing the website with financial services (Brevini et al., 2013; European Commission, 2012).

The emergence of a system of extra judicial governance is not simply a concern in the United States but has also been identified by an investigation undertaken by the European Commission (2012) into the prosecution of WikiLeaks by corporations, where it has uncovered evidence that corporate networks are acting as a 'para-regulator' operating outside the reach of European governments. Therefore, we can see that whilst WikiLeaks has used cyberspace to work around national censorship and data protection laws, it has been far more difficult to work around a financial system in which US corporations act as central nodes within the network and are obligatory points of passage for the sites' finances.

The other key vulnerability of WikiLeaks is the body of Julian Assange himself. One consequence of Assange's identification of himself with the organization is that he has presented himself as an easy target, especially given the relative sophistication of technical aspects of the WikiLeaks project. The WikiLeaks project has become re-territorialized around the body of its founder. The almost complete identification of WikiLeaks with Assange has led some commentators to describe WikiLeaks as a 'Single Person Organization' or 'Unique Personality Organization' (Lovink, 2010: 3). Assange himself has been quoted as claiming that, "I am the heart of soul of this organization, its founder, philosopher, spokesperson, original coder, organizer, financier, and all the rest" (quoted Beckett and Ball, 2012: 90). Since WikiLeaks began releasing whistleblower leaks into cyberspace Assange has been accused of being a liar, a spy, a terrorist, and a rapist.

The status of WikiLeaks as an outlet for the truth about the activities of governments and big business has certainly been tarnished by these accusations. Writing for the US

news outlet CNN, Micah Sifry has argued that Assange ought to have stepped aside from WikiLeaks for the good of the organization, when his legal troubles first emerged (CNN, 2012). There is little doubt that these accusations have had the effect of undermining the reputation of WikiLeaks and the perception of the information that it has released (Brevini et al., 2013). Despite these accusations there is still a surprisingly high level of public support for the project, given the allegations made against it and its members, although the level of support varies greatly from country to country. For instance public opinion in Australia and the UK has been broadly in favour of the project (Lester, 2011; Martinez, 2010). In contrast, public opinion in Germany and the USA has been significantly more hostile to WikiLeaks (Pew Research Center for the People & the Press, 2010; Marxist Institute for Public Opinion, 2010).

We can therefore see that WikiLeaks displays a distinctive vector of deterritorialization in the continuing evolution of the network organization. The deterritorializing flows of information that have been facilitated by WikiLeaks have been challenged by a reterritorialization of conflicts around its financial infrastructure and the emergence of a hybrid system of 'extra-judicial' governance, even in the face of pre-existing legal guards against such alliances between the corporate elites and the State. These conflicts will now be analyzed in greater detail by drawing on the concept of information warfare.

**WikiLeaks and Information War**

A wide variety of commentators have described the WikiLeaks network in the terms of information warfare (Beckett and Ball, 2012; Leigh and Harding, 2011; Lovink, 2010; Sifry, 211). This may be considered unsurprising given that Julian Assange, the founder of WikiLeaks, comes from a background in hacking and was a figure of some renown during the 1990s in Australia's hacker community (Assange, 2011). As a hacker Assange is fully aware that information can be employed as a weapon and in 1996 he pleaded guilty to 24 counts of hacking against high security organizations including NASA, the Pentagon, and Lockheed Martin amongst others (Leigh and Harding, 2011). The WikiLeaks network has itself been accused of being engaged in two forms of information warfare: a) cyber-terrorism against the State, and b) 'brand damaging activities' against corporations.

*a) Cyber-terrorism against the State*

WikiLeaks has been denounced as a foreign terrorist organization in the popular media and by senior US politicians including Vice President Joe Biden and Homeland Security chairman Peter King (Beckett and Ball, 2012; Leigh and Harding, 2011). Other US politicians including Peter Hoekstra and Mike Hukabee have called for the execution of leakers, and the Attorney General Eric Holder has proposed that Julian Assange be investigated for treason under the Espionage Act (Brevini et al., 2013; Thorsen, et al., 2013). These accusations were supported by statements from military spokespersons, such as Admiral Mike Mullen, who in response to the leaking of the Afghan war logs claimed that Assange had 'blood on his hands' (CNN, 29.07.2010).

Media commentators have explicitly described WikiLeaks as being engaged in information warfare and cyber-terrorism. In a rather shrill article published in *The Washington Post* (7.10.2010) Marc Thiessen compared WikiLeaks with cyber-terrorism arguing that, "If WikiLeaks is treating this as a war in cyberspace, America should do the same". The article continued by berating the Obama administration for its lack of action in launching a counter-attack against the website. One might find such comments a trifle exaggerated, however, in a less restrained tone published in *The Washington Times* (2.12.2010) Jeffrey Kuhner titled his article "Assassinate Assange?" In this piece he claimed that Assange was engaged in cyber warfare against the United States and continues that, "He is a willful enabler of Islamic terrorism." Former disgruntled insiders like Daniel Domscheit-Berg and Klopp (2011: 131) have claimed that Assange has himself described WikiLeaks as being an 'insurgent operation.'

Geert Lovink (2010: 4) has explained this conflict in less incendiary terms arguing that, "What some see as 'citizen journalism' others calls 'info war'." Nick Davies, a Guardian journalist who worked closely with WikiLeaks over the release of the Afghanistan war logs, described the US response to the WikiLeaks network directed against Assange and its other members as an information war against WikiLeaks (Leigh and Harding, 2011: 99). Seen in this light it can be argued that WikiLeaks has been the target of an information war rather than the perpetrator. The transparency activist Micah Sifry describes this dynamic in more technological terms arguing that, "Infowar can mean only one thing: the conflict between the naturally open information systems of the present and the closed ones of the past." (Sifry, 2011: 41). These commentaries on the structural aspects of the WikiLeaks project are very much

in line with Tiziana Terranova's (2004) account of network culture resembling a battlefield rather than a democratic forum for debate.

The militarization of the Internet has been a recent topic of discussion for both military analysts (Arquilla and Rondfelt, 1997; Coker, 2004; Rid, 2013) and social theorists (Munro, 2010; Terranova, 2004; Virilio, 2000). Assange himself remarked that, 'there is now a militarization of cyberspace… We are all living under martial law as far as our communications are concerned…' (Assange et al., 2012: 33). The relevant international laws that are supposed to govern conflicts in cyberspace are detailed in the Tallinn Manual (Schmitt, 2013), which has attracted attention within the hacker community for its justification of the use of lethal force by States against hackers who are deemed to be engaged in cyber warfare (The Guardian, 18.3.2013).

One of the major difficulties identified in this advisory document is addressing extra-territorial attacks that take place in cyberspace where the document begins with the assertion of the right for a State to 'exercise control over cyber infrastructure and activities within its sovereign territory' (Schmitt, 2013: 15). However, following this assertion the manual proceeds by outlining a large number of difficulties that arise in the enforcement of this territorial right due to the 'extra territorial' nature of cyber warfare. The very next line in the manual remarks somewhat ambiguously that while the principle of territorial sovereignty must be upheld, 'no State may claim sovereignty over cyberspace *per se*' (Schmitt, 2013: 16). There is no clearer statement about the deterritorializing aspects of cyber-conflict than the efforts of States to regulate conflicts that are enacted within this realm.

The difficulties in establishing State sovereignty within cyberspace proliferate with each new page of the manual, requiring a growing number of caveats and sub clauses to clarify how territorial integrity might be maintained under the special conditions of cyber warfare (Schmitt, 2013). Rule 2 of the manual explains that, 'It may be difficult to determine jurisdiction within cyberspace because cloud or grid distributed systems can span national borders, as can the replication and dynamic relocations of data and processing… data can be located in multiple jurisdictions simultaneously… (and) the location of mobile devices can change during a computing session.' (Schmitt, 2013: 19). The manual attempts to address this thorny problem by appealing to the principle of 'objective territorial jurisdiction,' which permits States to prosecute criminal acts that were originated abroad but completed on their own territory. This implicitly recognizes that cyber operations are of a relatively deterritorialized nature, and concedes that drafting legislation to prevent such operations will often prove fruitless 'because doing so would have no meaningful effect on the outcome of the operation' (Schmitt, 2013: 28). Similar frustrations over the capacity to contain the activities of WikiLeaks have also been expressed within the corporate community.

*b) Brand damaging activities against corporations*

Many of the corporations that came into conflict with the WikiLeaks network have explicitly described the situation in terms of an information war. This is clearly illustrated in leaked documents from the European Commission (2012), where various corporations explained to the Commission the potential damage that the WikiLeaks network could cause their corporate brands. Official documents from MasterCard and Visa have revealed that they have a quite extraordinary interpretation of how Wik-

iLeaks' activities could affect their business operations. In response to an investigation into this affair by the European Commission (2012), MasterCard wrote that any association with WikiLeaks, 'will be damaging for the public perception of MasterCard and consequently {risk} damage for MasterCard's goodwill or of its Marks.' (MasterCard, quoted in European Commission, 2012). The company cited the relevant sections from their Rules of Conduct pertaining to both the 'Integrity of Brand and Network' and 'Illegal or Brand-damaging Transactions'. This response letter also outlined the concern of MasterCard for cyber-attacks in retaliation to their actions against WikiLeaks in which they referred to 'several conversations with the FBI, US Treasury and the Department of Homeland Security (DHS) about the possibility of MasterCard becoming a target of … DDOS {Distributed Denial of Service} attacks.' (MasterCard, quoted in European Commission, 2012). Visa Europe followed MasterCard's lead in wanting to 'disassociate its brand from WikiLeaks' (Visa, quoted in European Commission, 2012). Governments and corporations have been united in a shared concern for informational attacks against their brand image and have also been united in developing 'defensive strategies' (MasterCard, quoted in European Commission, 2012) against such perceived attacks by WikiLeaks.

Of great concern here is the close relationship that has been forged between these private corporations and key organizations within the US national security establishment including the FBI and the Department of Homeland Security (Benkler, 2011). This leaked correspondence (European Commission, 2012) reveals the way in which these corporations have become an informal arm of the national security state and have framed their branding activities in terms of cyber attack where their brands are the subject of 'attacks' and 'damage' and must be provided with 'defensive strategies.'

This correspondence suggests that these corporations understand the promulgation of their business very much in the terms of information warfare, where their leaders feel quite justified in taking preemptive action against organizations that are deemed to be a potential threat to their brands.

The aggressive response by the corporate world against WikiLeaks has prompted some hacker groups, most notably Anonymous, to respond with retaliatory informational attacks in support of WikiLeaks. Under the monikers 'Operation Payback' and 'Operation Avenge Assange' the Anonymous collective launched a series of cyber attacks against targets that they deemed were hostile to the WikiLeaks network. Using a distributed denial of service attack Anonymous was able to disable the main website of Mastercard for a few hours and inflicted modest financial harm (PayPal claimed $5.5m of damage). Their attacks against the websites of Amazon.com and Paypal were of insufficient scale to cause any significant disruption to these large corporations. A few prominent individuals were also targeted, such as the Republican politician Sarah Palin, who had her credit card account temporarily disrupted. This was a truly deterritorialized attack, involving 7,800 members of Anonymous, geographically dispersed and unknown to each other beyond their online pseudonyms, in addition to the remote use of many thousand more terminals by means of botnets (Coleman, 2014). The broader significance of these different informational skirmishes is a matter of some contention. John Barlow, the founder of the Electronic Frontier Foundation, described the event as being the 'first serious information war' (quoted in Beckett and Ball, 2012: 65). In contrast, the legal scholar Alasdair Roberts (2012: 121) has argued that the counter attack by Anonymous against Amazon and MasterCard did little to disrupt their business and that, "The 'first serious info war' was over, with negligible

damage to the targeted institutions." Notwithstanding the academic debate over the significance of these informational attacks, the FBI has subsequently arrested and charged 16 people for cyber-crimes related to Operation Payback (The Guardian, 23.11.2012).

In summary, the scope of the information warfare in the WikiLeaks case is broad, including accusations of cyber-terrorism against the State and brand damaging activities against corporations. This information war has evolved over a series of attacks and counter-attacks including: i) WikiLeaks release of sensitive corporate, diplomatic and military secrets onto the Internet, ii) defensive tactics by WikiLeaks locating the website in countries that have favourable freedom of information laws and 'mirroring' it at hundreds of other locations throughout the Internet, iii) attempts by the State to discredit WikiLeaks and to prosecute its members and allies, especially Assange himself, iv) attempts by US corporations to disrupt the communication networks and financial networks upon which WikiLeaks is reliant, v) hacker attacks targeting WikiLeaks to disable its website, and vi) cyber attacks targeting corporations by hacktivist groups such as Anonymous that are sympathetic to WikiLeaks' aims. This information war demonstrates that the State has clearly struggled to contain the deterritorializing tactics of WikiLeaks (points i and ii) and those of its allies (point vi). In retaliation, the State and business corporations have employed reterritorializing tactics (points iii and iv), and have also promoted their own informational attacks against the site (point v). These vectors of deterritorialization and reterritorialization are indicative of a transformation of information systems into weapon systems. As Deleuze and Guattari (1988:204) themselves explained, 'It is on lines of flight {deterritorialization} that new weapons are invented, to be turned against the heavy arms of the State.'

Now that I have outlined the different vectors of deterritorialization and reterritorialization that have characterized the evolution of WikiLeaks as a network organization, I shall turn to an evaluation of the broader implications of this analysis for understanding current transformations in the network organization.

**Discussion: Redefining Resistance as Vectors of Deterritorialization**

The WikiLeaks network can be understood as a rapidly changing 'rhizomic' network (Chia, 1999; Linstead and Thanem, 2007) whose emergence has had significant implications for organizational power relations. This inquiry has described the destabilization of power relations through vectors of deterritorialization where the 'power centers are defined much more by what escapes them or by their impotence than by their zone of power' (Deleuze and Guattari, 1988: 217). The paper shows that WikiLeaks' efforts to create a deterritorialized 'space of autonomy' (Castells, 2012) has prompted aggressive counter-measures from central nodes of influence in an effort to re-assert their control over informational flows and resources. As such this paper would not go as far as Castells' (2012: 2) utopian assertion that 'Internet social networks… are spaces of autonomy, largely beyond the control of government and corporations', but instead has highlighted the contested nature of these spaces and the tactics of resistance that can be employed to destabilize existing forms of control in the attempt to create new spaces of autonomy.

It is true that WikiLeaks has met with only limited success where many of its operations have now been blocked as a result of internal conflicts within the organization

(Beckett and Ball, 2012; Domscheit-Berg and Klopp, 2011) and the financial blockade that has been levelled against it by corporate interests. Nevertheless, the WikiLeaks' model has spawned a significant number of imitators online (see Greenberg, 2012 and http://leakdirectory.org/index.php) as well as in the traditional media. It has also been highly influential in the work of social movements (Amnesty International, 2011; Sifry, 2011) and in the establishment of Iceland's new constitution and its aim to become a national anti-secrecy haven (IMMI.org). Many of these imitators have focused on the issues of particular countries, such as TuniLeaks, RuLeaks, BalkanLeaks, IsraeliLeaks, and VatiLeaks. Others are more narrowly confined to special interests such as Copyleaks, devoted to academic plagiarism, GreenLeaks, devoted to environmental issues, and TradeLeaks which is devoted to consumer activism. Large media corporations have also created their own leaking websites including the Wall Street Journal Safehouse and the Al Jazeera Transparency Unit.

In contrast to the original WikiLeaks website, its imitators tend to offer little protection for whistleblowers. A major flaw that has been identified in these imitators is that they do not offer full anonymity to their whistleblowers as did WikiLeaks, and the newspapers mentioned above explicitly reserve the right to pass on whistleblower details to State authorities (Greenberg, 2012). It would thus appear that although the WikiLeaks' model has been hugely influential across a range of social domains, it has been increasingly watered down as it has been imitated by others. There are a few important exceptions to this general observation, including a minority of leaking sites that employ strict technological protection to ensure anonymity (e.g. TOR software), and the Icelandic Modern Media Initiative (IMMI.org), which has developed strong

legal protection for whistleblowers and the media outlets that publish their revelations.

The mutation in relations of power and resistance represented by WikiLeaks can be understood as exhibiting both a liberal reformist aspect and a more radical insurgent aspect. The liberal reformist aspect of WikiLeaks is apparent in its own rhetoric where it describes its mission in terms of facilitating good corporate governance through increased transparency: 'Open government answers injustice rather than causing it. Open government exposes and undoes corruption. Open governance is the most effective method of promoting good governance' (https://wikileaks.org/About.html, see also Fuchs, 2011). This rhetoric presents the WikiLeaks network as an extension of the Fourth Estate and a part of the free press that serves as a crucial democratic check on State power (Benkler, 2011; Sifry, 2011). In contrast to this reformist rhetoric the more radical tendencies of the WikiLeaks network have become apparent from its deterritorializing processes, which have been characterized as being a threat to corporate power and to national security (Brevini et al., 2013; Centre for Constitutional Rights, 2012; Leigh and Harding, 2011)[iv].

WikiLeaks can be understood as a form of 'resistance to the present' that pursues an 'absolute deterritorialization' (Deleuze and Guattari, 1994: 99-108)[v]. This absolute deterritorialization moves well beyond its initial status as a whistleblowing platform to its more ambitious initiatives in the creation of anti-secrecy havens that support privacy for the weak and transparency of the powerful. In contrast to existing research within the field of organization studies (Ball, 2005; Bain and Taylor, 2000; Burrell, 1988; Clegg, and Baumeier, 2010; Munro, 2000), which has provided a detailed anal-

ysis of how communication networks have intensified organizational surveillance this paper has shown how a network organization can invert the existing hegemonic systems of surveillance. The tactics of resistance that have been examined in the above analysis follow vectors of deterritorialization which escape the control of other organizations and vectors of reterritorialization that attempt to re-exert control. The present inquiry has shown how WikiLeaks exploits vectors of deterritorialization to destabilize existing power relations and has thus been able to exert influence from the periphery of existing networks (see Table 1 for a summary) [vi].

Table 1. Vectors of Deterritorialization and Reterritorialization

| **Vectors of Deterritorialization** | **Vectors of Reterritorialization** |
|---|---|
| WikiLeaks' multi-jurisdictional exploitation of censorship laws | State/Corporate para-regulatory control of the Internet |
| Mirror websites to decentralize and deterritorialize WikiLeaks | Financial blockade of WikiLeaks by major corporations |
| Corporate/State secrecy havens (e.g. Offshore banking, Guantanamo Bay) | Anti-secrecy/transparency havens (e.g. Iceland's IMMI and WikiLeaks itself) |
| Legal and technological protection of privacy | Law suits and grand jury proceedings against WikiLeaks |
| Cypherpunk information movement | The body of Assange under house arrest and subsequent political asylum |

| | |
|---|---|
| Cyber warfare operations targeting WikiLeaks as well as corporations (e.g. Operation Payback against Paypal, MasterCard and Amazon) | 'Objective territorial jurisdiction' of nation states to regulate extra-territorial cyber conflicts |

Table 1 reveals a complex interaction between the tactics of resistance of WikiLeaks and its diverse vectors of deterritorialization and reterritorialization. There is a significant isomorphism between WikiLeaks' tactics of resistance and its vectors of deterritorialization, and conversely between tactics of power and the attempts to reterritorialize its operations. Despite considerable isomorphism between the vectors of deterritorialization and tactics of resistance, there are important instances where this is not the case. There are two vectors of deterritorialization that are not employed by WikiLeaks but by corporations and the State. These include the offshore activities of corporations to avoid democratic oversight, as well as the State's ventures into cyberspace and its employment of information warfare. There is also a single case where WikiLeaks itself has resorted to an important reterritorializing tactic, using transparency as a tool to bring the activities of corporations and agents of the State (e.g. the military) under greater democratic oversight.

In summary, whilst there is a considerable overlap between resistance and deterritorialization, and power and reterritorialization, this cannot be taken for granted. This analysis is in keeping with Deleuze and Guattari's (1988) own analysis of power where they note that whilst nomadism creates a line of escape that approaches an 'ab-

solute deterritorialization', capitalism is also a deterritorializing force, but one that always attempts to reterritorialize and recapture the forces that it sets in motion.

## Conclusion

WikiLeaks is an 'alternative organization' (Parker et al., 2014) that has built up a network of resistance to corporate and State power from the periphery of existing networks (Böhm, et al, 2008; Davis et al, 2005; Kraemer, et al., 2013; Spicer and Böhm, 2007; Spicer and Van Bommel, 2011). In contrast to existing studies of power which have tended to focus on the intensification of workplace surveillance (Ball, 2005; Bain and Taylor, 2000; Burrell, 1988; Clegg, and Baumeier, 2010; Munro, 2000) and micropolitical acts of resistance within the workplace (Alvesson and Willmott, 1992; Bain and Taylor, 2000; Ball and Wilson, 2000; Contu, 2008; Courpasson et al., 2012; Fleming and Spicer, 2003; Jermier, et al, 1994; Knights and McCabe 2000, 2003), the present paper has looked beyond the boundaries of the workplace for sources of resistance. This paper provides a conceptual contribution to the literature on the network organization (Brass et al., 2004; Castells, 2012, 2013; Clegg, and Baumeier, 2010; Lash, 2002; Munro, 2000; Terranova, 2004) by identifying the diverse vectors of deterritorialization that have allowed WikiLeaks to act from the *periphery* of existing networks in its attempt to destabilize power and build a counter-hegemonic system of surveillance.

This inquiry is in partial agreement with Castells' (2013: xxv) own analysis of the WikiLeaks network regarding its democratic potential to create 'new opportunities for citizen control over their representatives.' However, the focus of the present investi-

gation has been on the identification of the distinctive tactics that have enabled WikiLeaks to exert power from the periphery and how these tactics have exploited particular vectors of deterritorialization. The paper makes three contributions to the understanding of power in organizations: i) it shows how power can be exercised by organizations on the periphery of existing networks rather than as a function of central nodes, ii) it explains the destabilization of existing power relations in terms of the concepts of deterritorialization and reterritorialization, iii) and it shows how tactics of resistance are effective to the extent that they approach an 'absolute deterritorialization'. This paper demonstrates how WikiLeaks has amplified micropolitical acts of workplace resistance (Alvesson and Willmott, 1992; Contu, 2008; Courpasson et al., 2012; Fleming and Spicer, 2003; Jermier, et al, 1994; Knights and McCabe 2000) to engage in a broader counter-hegemonic attack upon the secrecy havens of the powerful.

This paper opens up new avenues for research in organization studies with respect to a number of important issues. Further research is needed into processes of deterritorialization of the development of new forms of network organization. What are the more general implications of the increasingly deterritorialized aspects of networks for organizational innovation and organizational politics? The role of secrecy havens is in need of further empirical research (see Sikka 2003 for an excellent step in this direction). In particular, there is a clear need for further investigation of the interface between the State and corporations, especially with respect to the possible existence of an 'extra judicial' regulatory system.

**References**

Agamben, G. (1995) *Homo Sacer: Sovereign Power and Bare Life*, Stanford University Press, Stanford, CA, USA

Alvesson, M. and Willmott, H. (1992). On the idea of emancipation in management and organization studies, *Academy of Management Review*, 17, 432–464.

Amnesty International (2011) *Annual Report 2011*, http://www.amnesty.org/en/annual-report/2011

Arquilla, J., and Ronfeldt, D. (eds.) (1997) *In Athena's camp: Preparing for conflict in the information age*, Washington: RAND National Defense Research Institute.

Assange, J. (2011) *Julian Assange: The Unauthorized Autobiography*, Canongate Books Ltd

Assange, J., Appelbaum, J., Mueller, A. and Zimmerman, J. (2012) *Cypherpunks: Freedom and the future of the Internet*, OR Books. London

Assange, J. Goodman, A. and Zizek, S. (2013) Amy Goodman in Conversation with Julian Assange and Slavoj Zizek, in Brevini et al., (2013), pp.254-271

Bain, P. and Taylor P (2000) Entrapped by the electronic panopticon? Worker resistance in the call centre, *New Technology, Work and Employment*, 15(1): 2-18

Bakan, J. (2004) *The Corporation: The Pathological Pursuit of Profit and Power*, London, Constable & Robinson Ltd.

Ball, K. (2005) Organization, surveillance and the body: towards a politics of resistance, *Organization*, 12(1): 89–108.

Ball, K., and Wilson, D. (2000) Power, control and computer-based performance monitoring: Repertoires, resistance and subjectivities, *Organization Studies*, 21(3): 539–565.

Bauman, Z. (2000) *Liquid Modernity*, Cambridge, Polity Press.

Beckett, C. and Ball, J. (2012) *WikiLeaks: News in the Networked Era*, Polity, Cambridge

Benkler, Y. (2011) WikiLeaks and the protect-ip Act: A New Public-Private Threat to the Internet Commons, *Daedalus*, 40(4): 154-164

Blaug, R. (1999) The Tyranny of the Visible: Problems in the Evaluation of Anti-Institutional Radicalism, *Organization*, 6(1): 33-56

Böhm, S. Spicer, A., and Fleming, P. (2008) Infra-political dimensions of resistance to international business: A Neo-Gramscian approach, *Scandinavian Journal of Management*, 24: 169–182

Borgatti, S. and Foster, P. (2003) The Network Paradigm in Organizational Research: A Review and Typology, *Journal of Management*, 29(6): 991-1013

Brass, D., Galaskiewicz, J., Greve, H., and Tsai, W. (2004) Taking stock of networks and organizations: A multilevel perspective. *Academy of Management Journal*, 47: 795-819

Brevini, B. Hintz, A. and P. McCurdy (eds.) (2013) *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society*, Palgrave MacMillan, Basingstoke, UK.

Brighenti, A. (2010) On Territorology: Towards a General Science of Territory, *Theory, Culture and Society*, 27(1): 52-72

Burrell, G. (1988) Modernism, Post Modernism and Organizational Analysis 2: The Contribution of Michel Foucault, *Organization Studies*, 9(2): 221-235

Castells, M. (1996) *The rise of the network society: The information age, economy, society and culture. Vol. 1*, Oxford: Blackwells.

Castells, M. (1997) *The power of identity*. Oxford: Blackwells.

Castells, M. (2012) *Networks of Outrage and Hope: Social Movements in the Internet Age*, Polity Press

Castells, M. (2013) *Communication Power*, Oxford University Press, Oxford

Centre for Constitutional Rights (2012) CCR condemns reported sealed indictment against Wikileaks founder Julian Assange, http://ccrjustice.org/newsroom/press-releases/

Chia, R. (1999) A 'Rhizomic' Model of Organizational Change and Transformation: Perspective from a Metaphysics of Change, *British Journal of Management*, 10(3): 209–227

Clegg, S. and Baumeier, C. (2010) Essai: From Iron Cages to Liquid Modernity in Organizational Analysis, *Organization Studies*, 31(12): 1-21

Clegg, S., Kornberger, M. and Rhodes, C. (2005) Learning/Becoming/Organizing, *Organization*, 12(2): 147–167

CNN (29.07.2010) Top military official: WikiLeaks founder may have 'blood' on his hands.

CNN (17.8.2012) Assange's stubborn grip hurt WikiLeaks.

Cohen, J. (2007) Cyberspace As/And Space, *Columbia Law Review*, 107(1): 210-256,

Coker, C. (2004) *The Future of War: The Re-enchantment of War in the Twenty-First Century*, Oxford. Blackwell

Coleman, G. (2014) *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*, London: Verso

Contu, A. (2008) Decaf resistance: On misbehavior, cynicism, and desire in liberal workplaces, *Management Communication Quarterly*, 21: 364–379.

Courpasson D., Dany, F. and Clegg, S (2012) Resisters at Work: Generating Productive Resistance in the Workplace, *Organization Science*, 23(3): 801 - 819

Davis, G., McAdam, D., Scott, R. and Zald, M. editors (2005) *Social movements and organization theory*, Cambridge: Cambridge University Press.

Deleuze G. and Guattari F. (1986) *Kafka: Toward a Minor Literature*. Minneapolis: University of Minnesota Press.

Deleuze, G. and F. Guattari (1988) *A Thousand Plateaus: Capitalism and Schizophrenia Volume 2*, Athlone, London

Deleuze, G. and F. Guattari (1994) *What is Philosophy?*, Verso, London

Demil, B. and Lecocq, X. (2006) Neither Market nor Hierarchy nor Network: The Emergence of Bazaar Governance, *Organization Studies*, 27(10): 1447-1446

Domscheit-Berg, D. and Klopp, T. (2011) *Inside WikiLeaks: My Time with Julian Assange at the World's Most Dangerous Website*, Jonathon Cape, London

Elden, S. (2005) Missing the point: globalization, deterritorialization and the space of the world, *Transactions of the Institute of British Geographers*, 8: 8-19

Eisenhardt, K. (1989) Building Theories from Case Study Research, *Academy of Management Review*, 14(4) 532-550

European Commission (2012) Case COMP/39921 - Datacell/Visa&Mastercard, http://wikileaks.org/IMG/pdf/EUPreliminaryDecision1.pdf

Fleming, P., and Spicer, A. (2003) 'Working at a cynical distance: Implications for power, subjectivity and resistance', *Organization*, 10(1): 157–179.

Fuchs, C. (2011) WikiLeaks: power2.0? Surveillance 2.0? Criticism 2.0? Alternative media 2.0? A Political-economic analysis, *Global Media Journal (Australian Edition)*, 5(1): 1-17

Greenberg, A. (2012) *This Machine Kills Secrets: How WikiLeaks, Hacktivists and Cypherpunks Aim to Free the World's Information*, Random House

Greenpeace (2010) Trafigura, http://www.greenpeace.org/international/en/

campaigns/toxics/trafigura/

Greenwald, G. (2014) *No Place to Hide: Edward Snowden, the NSA, and the Surveillance State*, Penguin, London.

Hayles, K. (1999) *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature and Informatics*, The University of Chicago Press, London

Hintz, A. (2013) Dimensions of Modern Freedom of Expression: WikiLeaks, Policy Hacking, and Digital Freedoms, in Brevini et al., p.146-165

Hood, C. (2011) From FOI to WikiLeaks World: A New Chapter in the Transparency Story, *Governance: An International Journal of Policy, Administration and Institutions*, 24(4): 635-638

Hughes, E. (1993) *A Cypherpunk's Manifesto*, http://activism.net/cypherpunk/

Jermier, J., Knights, D. and Nord, W. editors (1994) *Resistance and power in organizations*, London: Routledge.

Knights, D. and MacCabe, D. (2000) 'Ain't misbehavin'? Opportunities for resistance under new forms of "quality" management, *Sociology* 34(3): 421–436.

Knights, D. and MacCabe, D. (2003) Governing through teamwork: Reconstituting subjectivity in a call centre, *Journal of Management Studies*, 40(7): 1587–1619.

Kraemer, R., Whiteman, G. and Banerjee, B. (2013) Conflict and astroturfing in Niyamgiri: The importance of national advocacy networks in anti-corporate social movements, *Organization Studies*, 34(5): 823-852

Lash, S. (2002) *Critique of Information*, Sage, London

Leigh, D. and Harding, L. (2011) *WikiLeaks: Inside Julian Assange's War On Secrecy*, GuardianBooks, London

Lester, T. (6.1.2011). "Strong support for WikiLeaks among Australians". *The Age*.

Linstead, S. and T. Thanem (2007) Multiplicity, Virtuality and Organization: The Contribution of Gilles Deleuze, *Organization Studies*, 28(10): 1483-1501

Lovink, G. (2010) Twelve theses on WikiLeaks, *Eurozine*, http://www.eurozine.com/articles/2010-12-07-lovinkriemens-en.html

Lyon, D. (1994) *The Electronic Eye: The Rise of the Surveillance Society. Cambridge: Polity Press*, and Minneapolis: University of Minnesota Press.

McCurdy, P. (2013) From the Pentagon Papers to Cablegate: How the Network Society Has Changed Leaking, in Brevini et al. (eds.), pp.123-145

Marachel, G., Linstead, S. and Munro, I. (2013) The territorial organization: History, divergence and possibilities, *Culture and Organization*, 19(3): 185-208

Martinez, M. (14 December 2010). "Poll: Almost half of Britons feel WikiLeaks sex charges are "excuse"". CNN.

Marxist Institute for Public Opinion (2010) "McClatchy-Marist Poll National Survey December 2010", pp. 21–24.

Mathiesen, T. (1997) The Viewer Society: Michel Foucault's 'Panopticon' revisited, *Theoretical Criminology: An International Journal*, 1(2): 215-232

Miles, R. and C. Snow (1992) Causes of Failure in Network Organizations, *California Management Review*, 34: 53-72

Munro, I. (2000) Non-Disciplinary Power and the Network Society, *Organization*, 7(4): 679-695

Munro, I. (2010) Defending the Network Organization: An Analysis of Information Warfare with Reference to Heidegger, *Organization*, 17(2): 199-222.

O'Mahony, S. and F. Ferraro (2007) The Emergence of Governance in an Open Source Community, *Academy of Management Journal*, 50(5): 1079-1106

O'Mahony, S. and B. Bechky (2008) Boundary Organizations: Enabling Collaboration among Unexpected Allies, *Administrative Science Quarterly*, 53(3): 422-459

Parker, M., Cheney, G., Fournier, V., and Land, C. (eds) (2014) *The Companion to Alternative Organization*. London: Routledge.

Patton, P. (2012) Deleuze's political philosophy, *The Cambridge Companion to Deleuze*, Cambridge University Press, Cambridge, pp. 198-219

Pew Research Center for the People & the Press (2010) "Public Sees WikiLeaks as Harmful"

Podolny, J. and K. Page (1998) Network Forms of Organization, *Annual Review of Sociology*, 24: 57-76

Rid, T. (2013) *Cyber War Will Not Take Place*, Hurst and Company, London

Roberts, A. (2012) WikiLeaks: the illusion of transparency, *International Review of Administrative Sciences*, 78(1): 116-133

Schmitt, M. (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge

Sikka, P. (2003) The Role of Offshore Financial Centres in Globalization, *Accounting Forum*, 27(4): 365-399

Sifry, M. (2011) *WikiLeaks and the Age of Transparency*, Counterpoint, Berkley, US

Sorensen, B. (2005) Immaculate defecation: Gilles Deleuze and Felix Guattari in organization theory, *The Sociological Review*, 53(1):120 - 133.

Spicer, A. and S. Böhm (2007) Moving Management: Theorizing Struggles against the Hegemony of Management, *Organization Studies*, 28(11): 1667-1698

Tarrow, S. (2011) *Power in movement: social movements and contentious politics*, 3rd edn. Cambridge: Cambridge University Press.

Terranova, T. (2004) *Network Culture: Politics for the Information Age*, Pluto Press, London

Thanem, T. (2011) All talk and no movement? Homeless coping and resistance to urban planning. *Organization*, 19(4): 441-460

The Guardian (17.10.2009) Revealed: Trafigura-comissioned report into dumped toxic waste

The Guardian, (23.11.2012) Prosecution of Anonymous activists highlights war for Internet control.

The Guardian (18.3.2013) Rules of cyberwar: don't target nuclear plants or hospitals, says Nato manual

The New York Times (5.12.2010) Hundreds of WikiLeaks Mirror Sites Appear-

The Washington Post (7.10.2010) You're Either With Us, or You're With WikiLeaks.

Thorsen, E., Sreedharan, C. and Allan, S. (2013) WikiLeaks and Whistleblowing: The Framing of Bradley Manning, in Brevini et al., pp.101-122

Van Bommel, K., and Spicer, A. (2011). Hail the snail: Hegemonic struggles in the Slow Food Movement, *Organization Studies*, 32: 1717–1744.

Virilio, P. (2000) *The Information Bomb*, London. Verso

Von Hippel, E. (2001) Innovation by User Communities: Learning from open source software, *Sloan Management Review*, 42(4): 82-86

Von Hippel, E. and Von Krogh, G. (2003) Open source software and the 'private-collective' innovation model: Issues for organization science, *Organization Science*, 14 (2): 209-223

Wallemaq, A. (1998) Totem and Metaphor: The Concept of Network as a Symbolical Operator, *Organization*, 5(4): 593-612

[i] The founder of WikiLeaks, Julian Assange, was voted the Reader's Choice for Time Magazine's "Man of the Year" in 2010, where Facebook's founder, Mark Zuckerberg, was the official Man of the Year.

[ii] This general definition does not capture the importance of processes of deterritorialization to Deleuze and Guattari's conception of the rhizome and the process of becoming. They define the rhizome and becoming in terms of different vectors of deterritorialization, where their classic exemplar is the wasp/orchid rhizome. They explain how a line of deterritorialization passes between the wasp and the orchid, where the wasp is 'deterritorialized, becoming a piece in the orchid's reproductive apparatus' (Deleuze and Guattari, 1988:9). In the present paper, the first section of the analysis of WikiLeaks investigates the rhizomatic alliances and mutations of this network, and the later sections attend to the more geographical and political nature of its deterritorializations.

[iii] The NSA whistleblower, Edward Snowden, was in a far more precarious situation, where he was truly stateless having had his US passport revoked and then forced to confine himself to the relatively deterritorialized space of Moscow airport, being unable to leave this space without fear of arrest and rendition.

[iv] The coexistence of reformist and radical aspects in the WikiLeaks network has led to radically different interpretations of this organization where some focus on the project's libertarian rhetoric (see Fuchs, 2011) and others on its status as an insurgent project (see Zizek in Assange et al., 2013).

[v] Deleuze and Guattari explain this process of 'absolute deterrritorialization' in terms of radical resistance that is able to overcome further reterritorialization by the State or capital by creating 'utopias of immanence' and a 'new earth' (Deleuze and Guattari, 1988: 510; 1994: 99-113).

[vi] Note, this summary table is inclusive of those vectors analyzed in the sections on information warfare and the previous sections on secrecy and anti-secrecy havens and the structure of WikiLeaks.