Networked Resistance:
The Case of WikiLeaks

Abstract:

In this article, WikiLeaks is embedded within broader debates relevant to both social movement and mediation theory. First, the nature of the ties between a variety of relevant actors are assessed. Second, the networked opportunities and constraints at a discursive and material level of analysis are highlighted and finally the resistance strategies they employ towards mainstream culture are addressed. It is concluded that at the heart of information and communication resistance a dynamic dialectic can be observed between mediated opportunities for disruptions and attempts of the powers that be to close down these opportunities. Furthermore, it has to be acknowledged that reliance on mainstream actors and structures for exposure, funding or hosting contentious content comes with risks for radical activists.

Keywords:

Opportunity Structure, Mediation, Hacktivism, Networks, WikiLeaks

Word-Count:

8.597 (refs and endnotes included)

Networked Resistance:
The Case of WikiLeaks

'it takes networks to fight networks'
(Arquilla & Ronfeldt, 2001, p. 15)

Introduction

In about five years time Wikileaks evolved from a faceless intermediary enabling whistleblowers to publish documents while remaining anonymous to being an active actor, selecting/redacting material and reaching out to mainstream media to increase exposure. In November 2007, WikiLeaks had its first big scoop when they published the Guantánamo Bay military manual entitled *Camp Delta Standard Operating Procedures* which outlined day-to-day operations and detailed procedures at the US controlled detention center on the Cuban Island. By 2008 WikiLeaks had gained worldwide notoriety and respectability within the hacking community, which resulted in more whistleblowers using the site to reveal sensitive documents such as those incriminating the Swiss bank Julius Bär with regards to tax evasion and money laundering, the 'secret' Scientology handbooks, private e-mails from Sarah Palin or the membership list of the fascist British National Party (BNP).

In doing so, WikiLeaks 'established a powerful brand identity as a technologically sophisticated service capable of distributing purloined data anonymously and publicizing its release' (Fenster, 2011: 7). In subsequent years the amount of information revealed and released by WikiLeaks increased exponentially. Absolute highlights were the publication in 2010 of subsequently (1) the 'Collateral Murder' video showing an attack of a U.S. Army Apache helicopter on a group of unarmed men in Baghdad, among which two Reuters journalists; (2) the Afghan War Diaries, (3) the Iraq War Logs and (4) the US diplomatic cables, all emanating from the same source[1].

WikiLeaks, Ludlow (2010) argues, is 'the product of decades of collaborative work by people engaged in applying computer hacking to political causes, in particular, to the principle that information-hoarding is evil' (p. 25). From this perspective, the case of WikiLeaks should be positioned within a broader legacy of information and communication activism and more specifically related to newly emerging repertoires of networked contentious action also at times denoted as hacktivism. Hacktivism compounds hacking and activism and as such it represents the extension of socio-technological struggles into the realm of politics beyond the technological and the networked computer infrastructures (Jordan, 2008, p. 71). At a tactical level hacktivism is clearly differentiated from cyber-terrorism and more aligned with tactics of civic disobedience – i.e. hacktivism refers more to disruption than destruction (Conway, 2007, p. 88).

The two main conceptual lenses through which WikiLeaks will be analyzed here are opportunity structures and mediation. The mediation opportunity structure is proposed as an over-arching concept to make sense of the WikiLeaks case as both information and communication activism – mediation processes capture the discursive and symbolic struggles as well as attempts to increase mainstream media resonance and the newly emerging networked repertoire of contentious action on which organisations such as WikiLeaks rely.

The mediation opportunity structure for activists should be seen as partially overlapping with the political opportunity structure (Tarrow, 1994: 85), but at the same time also semi-independent in that it holds its own peculiar opportunities and constraints. For activists today the mediation opportunities as well as the structural constraints on mediation situate themselves at three interwoven levels of analysis: the discursive, mainstream media resonance and networks. In terms of networks we can refer here not only to the material network infrastructure, but as much to the connections and ties between various actors which the network makes possible, but also extending into the offline realm. The case of WikiLeaks is situated within this broader framework of the meditation opportunity structure by addressing 1) the network of actors with a variety of latent, weak and strong ties; 2) the interplay between opportunities and constraints at the symbolic/discursive and the material level; and 3) the communicative strategies of contention enacted by WikiLeaks and its sympathizers.

Networks are often understood as direct and indirect connections between individuals and/or organisations in collaborative endeavours. In this regard, while network theorists identifies the strength of weak and latent ties (Haythornthwaite, 2005), the remaining importance of strong (offline) ties for social and political action is stressed by others (della Porta & Diani, 2006). In light of the WikiLeaks case the importance of and interaction between these various ties is being highlighted.

Furthermore, by drawing on theories from political science and media and communication studies, the mediation opportunity structure can be seen as operating both at a symbolic/discursive level and a material one, with the latter relating to a social constructivist approach to the social shaping of technology (Livingstone, 2007). Mediation processes are prime examples of the intricate inter-play between agency and structure. Those that strive for change are locked in a permanent war of position with those aiming to preserve and protect the status quo. At a material level of analysis, the network opens up opportunities to resist, but such opportunities for networked resistance tend to be closed down very quickly, after which new opportunities emerge and so on. This results in a kind of cat-and-mouse dynamic between corporate and state actors on the one hand and hacktivists on the other (Collins & Mansell, 2005). The case of WikiLeaks is illustrative for how mediation through networks enables agency and resistance, but also shows how structure can strike back and reassert itself.

Finally, the combining of symbolic and discursive struggles with mediated communicative practices of resistance enabled by the network as an

infrastructure exposes the use and appropriation of the mediation opportunity structure as catering to a variety of strategies of contention in dealing with the mainstream political culture they contest. Independent self-mediation practices, partial adaptation to the mainstream media logic, attacking mainstream actors and abstention from the mainstream public space, all distinct media strategies of activists, are often combined to achieve movement aims (Rucht, 2004). This is certainly observable in the case of WikiLeaks, where the activists involved use self-mediation practices in addition to strategies of adaptation, critique and abstention.

Network of Actors: strong, weak and latent ties

While weak ties are often seen to be primarily instrumental, strong ties are more emotional and entail more frequent exchanges and interactions. The strength of weak ties lies in the ability of individuals and organisations to draw support from their weak ties network in terms of experiences, information and resources. The strength of strong ties lies in more determined motivations and higher degrees of loyalty. Besides weak and strong ties, Haythornthwaite (2005) identifies a third type. Networked technologies, she argues, 'support latent social network ties, used here to indicate ties that are technically possible but not yet activated socially' (p. 137).

From a social movement perspective the inter-connections between various actors and the networks they form are a crucial aspect of social movements and of activism. Networks are increasingly seen to be central to understanding present-day social movements, influencing their impact, their ability to sustain and coordinate social action (della Porta & Diani, 2006, p. 117). In the social movement literature the importance of strong offline ties is foregrounded, such as family, local networks, membership of associations, etc. Recent examples of fluid and less formally organized resistance and debates regarding the exact role of information and communication technologies have challenged these more traditional conceptions, but at the same time there is still evidence that close connections and offline ties to build trust and solidarity remain of importance, certainly when it comes to sustaining an organisation or struggle.

When approached from the level of actors, the case of WikiLeaks exposes a variety of strong and weak, but also of latent ties. WikiLeaks as an organisations combines the development of very strong ties amongst core-members and journalists with the strength of weak and latent ties when it comes to volunteers and those that leak information or the loose and latent inter-connections with the hacktivist collective Anonymous.

Strong Ties

The book *'Inside WikiLeaks'* by former number two of the organisation Daniel Domscheit-Berg (2011) reveals how the organisation was structured and run. In the book Domscheit-Berg outlines the closed and tight-knit nature of the organisation with a small core of highly dedicated activists, a clear-cut division of labour and quite hierarchical. However, beyond such eye-witness

accounts from former insiders, it is very difficult to get a sense of who the actors inside WikiLeaks are and how it is structured today.

One of the contradiction at the center of WikiLeaks is that striving for transparency of governance and freedom of information requires a degree of internal secrecy and above all concealment of the identity of those that take the risk of relegating government or corporate 'secrets' to the public domain. Assange (2011) justifies this strategic opacity as follows:

> one of our core principles is to protect the identities of whistleblowers. So sometimes one needs to be opaque to protect people. We are an organisation facing extraordinary threats from a superpower (np).

While the at some point WikiLeaks claimed to have 800 volunteers and some 40 core-members working for them (Burns & Somaiya, 2011, p. 36), the organisation also gradually became identified with the personality and charismatic figure of its founder Assange. In his book, Domscheit-Berg (2011) accuses Assange of turning WikiLeaks into a one-man show and loosing sight of the values it preached. Assange became the sole personification of WikiLeaks and to strengthen this perception he created an 'informational vacuum at the heart of a secretive organization whose motto is transparency' (p. 1).

In the introduction to the book *WikiLeaks: Inside Julian Assange's War on Secrecy* by journalists Leigh and Harding (2011), Guardian editor-in-chief Alan Rusbridger attests to how Assange strategically started to reach out to journalists very early on. In August 2007, the Guardian published a story based on documents leaked to WikiLeaks relating to corruption by the regime of Arap Moi in Kenya (Rice, 2007). In subsequent years the connections with journalists were intensified and expanded, certainly after Nick Davies, another Guardian journalist, convinced Assange that the explosive US military and diplomatic information WikiLeaks had received 'would have more impact and meaning if he was willing to ally with one or two newspapers – however traditional and cowardly or compromised we might be in the eyes of some hackers' (Rusbridger, in Leigh & Harding, 2011, p. 17).

One of the characteristics of strong ties is that they are emotional and that also has a downside. As is apparent from the critical tone in Domscheit's book, the very close connections of the core-members within WikiLeaks became destructive at some point. After repeated clashes and conflicts with Assange, Domscheit-Berg was first suspended and subsequently quit the organisation in September 2010. Besides this, the man responsible for the technical side of things called 'The Architect' left too, taking with him all the code he wrote and the intricate and secure technical structure he had built. At the time of writing – early 2012 – WikiLeaks is still not accepting new leaks:

> At the moment WikiLeaks is not accepting new submissions due to re-engineering improvements the site to make it both more secure and more user-friendly. [...] We anticipate reopening the electronic drop box and live chat support in the near future. (http://wikileaks.ch/Submissions.html - retrieved on 01/02/2012)

Also the relationship between Assange and the journalists, with whom he had built strong links, would turn sour. Assange increasingly felt betrayed by them because of the way in which they reported, unfavourably according to him, on the allegations of sexual misconduct filed against him in Sweden (see Leigh & Harding, 2011; Keller, 2011).

Weak Ties

Anonymity is crucial for whistleblowers who often put their careers and sometimes even their physical integrity and/or freedom at risk by leaking sensitive hidden information. As Domscheit-Berg (2011: 37) points out, great efforts were made to make sure that even WikiLeaks itself did not know the identity of the whistleblower as leaked information was sent 'through so many detours, encryptions, and anonymizing procedures [...] that no one could trace where they came from'. For example, WikiLeaks did not know the identity of the person who leaked the Afghanistan and Iraq diaries as well as the diplomatic cable until U.S. private Bradley Manning was arrested on 26 May 2010 after bragging about his exploits in a chat room.

Given the secretive nature of the organisation and the tight control of information by Assange, the object of critique by Domscheit-Berg, it could be argued that the volunteers WikiLeaks relied upon for very particular and specific tasks have weak links with the organisation. They are mostly used in an instrumental way and unable to have any impact on the organisation beyond the specific task they have been given by Assange or others at the core of the organisation. If Domscheit-Berg is accurate even core-members were often left in the dark by Assange regarding certain actions or strategies pursued.

WikiLeaks also relied heavily on weak links in the wake of the publication of the Afghan and Iraq War diaries and the diplomatic cables and as the organisation increasingly came under attack by corporate and government actors. Through these weak links, WikiLeaks and Assange received a huge amount of publicity and garnered considerable public support. On 8 December 2011, the Australian Internet organization GetUp! posted a letter of support for Julian that attracted 45,000 signatures within 48 hours. Public figures such as the Pentagon papers leakers Daniel Elsberg, filmmaker Michael Moore, and author Naomi Wolf also spoke out in support of Assange and of WikiLeaks.

Latent Ties

The links between WikiLeaks and other information and communication activists, such as the Hacktivist collective Anonymous could be described as latent, in the sense that there are no apparent direct connections between both, but at strategic moments Anonymous aligned its struggle with WikiLeak's plight. The links between WikiLeaks and the decentralised hacker collective Anonymous date back from 2007 when WikiLeaks received unexpected help from Anonymous to publish and structure all the Church of Scientology material they had received. This US-based sect was the first target

of Anonymous and the hackers collective was all too happy to voluntarily prepare 'the site so that readers could find their way more easily through the deluge of documents' (Domscheit-Berg, 2011, p. 38).

After this episode the ties turned latent again, only to be reactivated when WikiLeaks was severely crippled through corporate repression after they leaked the US diplomatic cables. Anonymous subsequently revamped its 'Operation Payback' – initially targeted at the music industry, into 'Operation Avenge Assange' – a campaign of retaliation in defense of WikiLeaks and Assange. Coldblood, a self-proclaimed spokesperson of Anonymous issued the following statement attesting to this:

> Anonymous is supporting WikiLeaks not because we agree or disagree with the data that is being sent out, but we disagree with any from of censorship on the internet. If we let WikiLeaks fall without a fight then governments will think they can just take down any sites they wish or disagree with. (Coldblood, quoted in Halliday & Arthur, 2010)

While there never was a direct connection between Anonymous and WikiLeaks there were mutual sympathies and latent ties, which were activated at crucial points when their respective struggles aligned themselves.

Mediated Opportunities and Structural Constraints

As a theoretical construct, mediation is often critiqued for being conceptually fuzzy, too general, not analytical enough and furthermore overly media-centric (Lundby, 2009, p. 3). One of the main reasons for this is that mediation attempts to be all encompassing. It aims to conceptually grasp as well as complicate the interactions between various analytical dichotomies such as public versus private, producer of content versus the receiver, the symbolic versus the material and crucially structure versus agency. This indeed makes it fuzzy, but also apt at making sense of the increased pervasiveness and ubiquity of media and communication in our everyday life and in politics.

In social movement theory, the concept of opportunity structure is also contested as neglecting the symbolic, overemphasizing process over culture and structure over agency. Combining the inherently dialectic nature of mediation with the concept of opportunity structure might offer a potential way out of this paradigmatic conundrum, overcoming the stark contradiction between structure and agency and between process and culture. As Koopmans (1999) rightly argues, accounting for structures does not deny the potential for agency or even sudden change, it just makes the obvious point that 'not all of opportunity is agency, but that some of it is structured' (p. 102). Approaching the opportunity structure in such a more dialectical way enables us to account for both structural impediments to and opportunities for change.

The WikiLeaks case is analyzed in view of the discursive and networked opportunities it exploits, but also the particular structural constraints it has to contend with both at the symbolic level and the material.

Discursive Opportunities and Constraints

The discursive opportunity structure foremost relates to the frames that are being used and disseminated to justify a particular struggle, to propagate an alternative vision and to mobilize for direct action (Ferree, et al. 2002). As such, in the social movement literature the use of diagnostic (what is the problem), prognostic (what is to be done) and motivational (what can we do) frames are distinguished (Snow & Benford, 1988).

At the diagnostic level WikiLeaks inscribes itself in a broader movement of freedom of information activism, concerned with free access to information, as well as transparency and accountability within a democracy, to expose what those that represent us and govern in our name attempt to keep hidden. These frames are directed against well-known strategies of concealment and secrecy of corporations to protect their business interests and of governments to protect the 'national interest' (Florini, 2004), but they equally apply to the whole debate converning copyright (Cammaerts, 2011).

At a prognostic level, the advent of the information society in the 1990s and the digitalization of information have played a pivotal role in providing tactical opportunities for those advocating for a more open and transparent government. However, at the tactical level divisions within the freedom of information movement can be observed. While conventional transparency advocates operate within the confinements and rules of engagement of liberal democracy, radical freedom of information activists or 'the guerrilla front of the transparency movement' (Brooke, 2011, p. 17), argues that legal activism is not enough and adopts more radical tactics such as anonymous whistleblowing.

At the motivational level, discourse serves to 'suggest not merely that something can be done but that "we" can do something' (Gamson, 1992, p. 7). In this regard, WikiLeaks clearly demonstrated through their online platform that something could be done, establishing a safe haven for potential whistleblowers to securely post the information they wish to leak. In addition to this, WikiLeaks also did their utmost to make sure that the leaks they published received ample media resonance and thus reached beyond netizens.

Changing attitudes and discourse towards government transparency

Arguments of national security are often invoked to legitimate the need for secrecy and concealment in a democracy and this is especially the case in times of war – 'In war, truth is the first casualty', the Greek dramatist Aeschylus proclaimed. Margaret Thatcher's defense of limiting civic liberties at the height of the IRA-crisis can be seen in a similar light:

> We do sometimes have to sacrifice a little of the freedom we cherish in order to defend ourselves from those whose aim is to destroy the freedom altogether – and that is a decision we should not be afraid to take. [...] The only victory will be our victory: the victory of democracy and a free society. (Speech at the Lord Mayor's annual Banquet, 14/11/1988)

As this quote above exposes, the relationship between democracy as a model of governance and secrecy remains conceptually fraught and inherently contradictory. Hence, while the current policy discourse is often one of transparency and open government, the different classifications to denote the degree and nature of secrecy of documents and information – from 'confidential' via 'secret' to 'top secret' – remain firmly in place.

At the other end of the continuum we find those advocating for the transparency of government and corporate information. Transparency advocates base themselves on a Kantian imperative that considers lying to be morally wrong in all circumstances (Korsgaard, 1989) and on a strong belief that those in representative positions of power need to be fully accountable to those from whom they derive their power, to argue that secrecy is antithetical to democracy and a democratic society. It is the expression of mistrust of decision makers towards those that they rule (Stiglitz, 1999, p. 2).

In an attempt to address these concerns and critiques many States introduced Freedom of Information (FoI) laws providing legal guarantees for citizens to access government information. At least at a symbolic level, the introduction of FoI legislations represented a change in the way the provision of government information was organised. While before, information was provided to citizens on a 'need to know' basis, FoI laws turned this into a 'right to know' (Ackerman & Sandoval-Ballesteros, 2006, p. 93). To date almost 90 countries have enacted specific FoI legislations. However, despite the adoption of far-reaching FoI-laws in many countries, the degree of exceptions States can invoke to deny citizens their right to know and the number of loopholes is still considerable. This leads Kierkegaard (2009) to conclude that the abundance of opt-outs re-asserting the principle of secrecy leads to FoI laws being almost pointless.

Besides enabling legal requests from citizens for government information the principles of FoI also include adequate protections for so-called whistleblowers. Whistleblowing is a practice involving 'speaking out from within an organization to expose a social problem or, more generally, to dissent from dominant views or practices.' (Martin, 1999, p. 16). It is generally accepted, however, that the legal protections for whistleblowing are often inadequate and that those engaging in such practices take considerable risks.

The shoot-the-messenger syndrome is rife – '[i]nstead of their message being evaluated, the full power of the organization is turned against the whistleblower' (ibid: p. 19). Common counter-tactics of organizations include harassment, ostracism, bullying, reprimands, demotion and dismissal. This explains why many whistleblowers prefer to remain anonymous rather than seeking full publicity and why the more radical forms of information and transparency activism – such as WikiLeaks – have been gaining strength in recent years.

The Discursive War of Position

As it became apparent to Assange that 'the more important and the bigger the leak is, the less chance it has of being reported if it is being distributed to

everyone at once'[2], he started developing even stronger ties with a limited number of journalists in order to increase media resonance and exposure of the content WikiLeaks publishes. As a result, initially journalists of the New York Times, The Guardian and Der Spiegel were given exclusive access to the material relating to Afghanistan. This was subsequently expanded to Al Jazeera and Channel4 for the Iraq War Diaries and to El País and Le Monde for the US diplomatic cables. In an op-ed in an Australian newspaper, Assange (2010) called this tactic 'scientific journalism':

> We work with other media outlets to bring people the news, but also to prove it is true. Scientific journalism allows you to read a news story, then to click online to see the original document it is based on. That way you can judge for yourself: Is the story true? Did the journalist report it accurately?

As mentioned earlier, Assange reached out to the media very early on when he started WikiLeaks, acknowledging that in order to have a serious impact at a discursive level, information activism must resonate in the mainstream media. His solution was taking transparency warfare to the masses, quite literally as was shown with the release of the Collateral Murder-video[3] (April 2010), which was widely reported and showed images from an Apache helicopter shooting at journalists and unarmed Iraqi civilians. After that, the Afghanistan and Iraq war logs (July and October 2010) and the U.S. diplomatic cables (November 2010) caused even more international havoc, exposing the brutality of war and the cynicism of real-politik.

Such discursive attacks never go unchallenged by the forces that are the object of attack. The more popular WikiLeaks became, the more sensitive information was leaked through its secure platform, the more the organisation and its founder became the focus of security services and the target of legal challenges. Besides a scuppered attempt in 2008 by the Swiss bank Julius Bär to block WikiLeaks' domain name, the efforts to counter-attack and discredit WikiLeaks were stepped-up considerably after the leaking of the US diplomatic cables.

The U.S. Justice Department started investigating whether Assange could be personally indicted with violating the 1917 Espionage Act. U.S. Senator and chair of the Committee on Homeland Security and Governmental Affairs Joe Lieberman called upon Amazon to stop hosting WikiLeaks and Amazon duly complied. Some commentators started labeling Assange as an 'information anarchist' (see Crovitz, 2010) and Sarah Palin called for Assange 'to be hunted down like Osama Bin Laden' thereby positioning WikiLeaks within the terrorism frame. Larry Sanger, co-founder of Wikipedia, tweeted: 'I consider [WikiLeaks] enemies of the U.S.—not just the government, but the people'[4].

Matters were, however, to become much worse and much more divisive when Assange had to address accusations of sexual misconduct in Sweden and an international arrest warrant was issued (Leigh, et al., 2010). As mentioned earlier, the immense pressure on Assange and on WikiLeaks as an organisation ultimately led to a split at the core of the organisation as distrust amongst the core members grew and long-term internal conflicts boiled over. At a discursive level all this led that the emphasis of the debate rapidly shifted

from the actual content of the leaks to the personality of Assange, but also to the collateral damage and harm caused by the release of the classified material.

Material Opportunities and Constraints

One of the most pervasive slogans of the early hacker movement was 'Information wants to be free', pointing to its ethics of open access to information and (technical) knowledge. Computing power in combination with telecommunication networks have for many years been the tools par excellence for hackers. However, as Chadwick (2006) quite rightly reminds us 'the very idea of a single community of hackers that share a common culture has been difficult to sustain' (p. 130). That is why in this article the focus is more specifically on Hacktivism rather than hackers and hacking in general.

Hacktivism was first coined in 1998 by Omega, a hacker of the US hackers collective The Cult of the Dead Cow5, also known as cDc, to indicate the use of hacking for political change rather than personal gain (Delio, 2004). While hacktivism first related foremost to the use and development of software to protect human rights and privacy on the internet, its meaning soon broadened to technology enabled political activism beyond the internet.

As the use of the nickname Omega shows, communication resistance enacted by activists requires anonymity and the use of pseudonyms, which is technologically facilitated. Despite this, just as other forms of radical resistance, information and communication resistance invites state repression, corporate pressure and legal responses. However, the network does provide opportunities for hactivists to retaliate and fight back. First, the opportunities created by the changes from a paper-based government to an e-government will be highlighted.

The shift from a paper culture to a digital culture

The relatively swift introduction of ICTs in public administrations and in the 'business' of government during the 1990s and 2000s was mainly the result of a techno-optimist and celebratory institutional discourse surrounding the presumed benefits of the information society and the quest of governments to reduce the costs of running public administrations and services (Garnham, 2005). Besides this, the introduction of ICTs in public administrations was also part of a broader shift from a bureaucratic 'self-preservation' paradigm to a more consumer and service-oriented paradigm advocating an open transparent government and public administration (Mayer-Schönberger & Lazer, 2007).

Of particular concern here are the efforts of governments and public administrations to increase internal efficiency through the digitalization of internal communication flows and archives, the development of secure cross-departmental intranets, and the linking-up of disparate databases with the aim to reduce overall costs and making so-called Government-to-Government (G2G) communication more efficient (Chadwick, 2006). Besides this, as outlined above the practical implications of Freedom of Information laws

required governments to become more transparent externally and provide performant and user-friendly informational services to citizen (C) and businesses (B), so-called G2C and G2B services.

At the same time, this e-government digitalization process has made States much more vulnerable when it comes to keeping their secrets under wraps, certainly as diplomacy has also digitalized (Rana & Kurbalija, 2007). Information hactivists are acutely aware of the growing use of the internet and digital technologies by governments, which has created unprecedented opportunities to expose information 'that was not intended for distribution outside certain vetted channels' (Sterner, 2011, p. 5).

So while the leaking of sensitive and classified information is by no means a new phenomenon, the digitalization of records, memo's, minutes, reports and mail has certainly made it easier and has made classified information more vulnerable to leaking beyond the eyes of those for whom it was meant.

Technology-Enabled Anonymity

Since 1999, a group called Hactivismo – a special project under the umbrella of cDc – dedicates all its efforts to the development of anti-censorship software specifically geared towards protecting human rights, fostering activism, enabling dissent and preventing detection of communication by security forces. This exposes the instrumental side of communication resistance, assisting those that resist in the offline world. Hacktivismo describes its mission as such:

> To conduct and publish scientific research in the areas of information technology, communications and electronic media; and, to assist (where possible) non-governmental organizations, social justice groups and human rights entities in the use of advanced information technologies for the furtherance of their works. We also intend to have fun doing this. Turn it up. Way up[6].

While the cDc has always been political – it even fielded a US presidential candidate every election since 1992 – Hacktivismo signaled a new phase in hacktivist practices, positioning themselves 'at the forefront of the ongoing struggle for human rights in and out of cyberspace'[7]. Over the years Hactivismo has developed many applications that enable internet users to anonymize themselves when they are online. Three of these are of particular interest here: Torpark (web-browser), Torbird (email client) and Scatterchat (IM client). While Torpark will be addressed more in detail here, the other two software applications work along the same principle and use the same network and technique to conceal the identity of those communicating.

Torpark refers to 'Deer Park', the codename for Mozilla's open source browser Firefox 1.5 on which Torpark is based. It uses a global network of encrypted proxy-servers called Tor [8] and a technique called onion-routing which repeatedly encrypts data and then sends it through several intermediate routers masking the origin and the destination of the data. The US Navy

patented onion routing in 1998 and was initially set-up to secure government communication[9].

By using the onion routing technique, Torpark and other Tor-related applications enable individuals to use the same network to disguise their location and identity from law enforcers, but also from websites targeting advertising or companies monitoring your online search patterns. The main disadvantages of the Tor-network are that it slows down your connection considerably and especially that it is an open system that can potentially be attacked by third parties. In 2007 a new version of Torpark was released called XeroBank Browser, which provided access to the Xerobank anonymous network, run by a commercial operator called Xero Networks AG, founded in Saint Kitts & Nevis in the Caribbean. Xero Networks offers faster (broadband) anonymous connections and a more secure environment by denying third parties the right to snoop and monitor. Xero Networks thus offers an extra layer of protection so to speak.

The Empire Strikes Back

Besides a discursive backlash, WikiLeaks also had to contend with serious challenges at a material level of analysis. The strategy to expel WikiLeaks from the network was two-fold; on the one hand attempts were made to block access to the WikiLeaks content and on the other hand its ability to generate funds through donations was severely disrupted. At the level of content, both the physical hosting of the actual content as well as the linkage between IP-address and the domain names of WikiLeaks were targeted.

On 2 December 2010, four days after publishing the US diplomatic cables, Amazon terminated its contract with WikiLeaks. While US senator Joe Lieberman had urged US companies, naming Amazon in particular, to sever their links with WikiLeaks and Assange (Poulsen, 2010), Amazon denied that blocking access to the diplomatic cables was a result of state pressure, instead they claimed that WikiLeaks had breached their 'terms of service':

> It's clear that WikiLeaks doesn't own or otherwise control all the rights to this classified content. Further, it is not credible that the extraordinary volume of 250,000 classified documents that WikiLeaks is publishing could have been carefully redacted in such a way as to ensure that they weren't putting innocent people in jeopardy. (http://aws.amazon.com/message/65348/ - retrieved 01/06/2011)

In addition to this, on the same day, the US-based domain name provider EveryDNS Inc. suspended their service to WikiLeaks. They claimed the domain names of WikiLeaks were being attacked incessantly by so-called Distributed Denial of Service (DDOS) attacks, putting other users of their service at risk. As a result of all this, WikiLeaks was forced to move the hosting of their content to the French service provider OVH and use a Swiss DNS provider. In the section below other resistance strategies to counter this state and corporate clampdown will be discussed further.

As mentioned above, besides the efforts to close down access to the WikiLeaks' website, its financing was also targeted. After the Cablegate, end of November 2010, several banks and companies facilitating online donations and payments blocked accounts pertaining to WikiLeaks. In quick succession PayPal, Moneybookers, Visa, MasterCard, BankAmerica and the Swiss bank PostFinance closed, froze or restricted the accounts of WikiLeaks. Again, the justification used by these corporations to do this, was that WIkileaks had breached their terms and conditions. PayPal, for example, sent out a press-release on 3 December 2010, saying that they

> permanently restricted the account used by WikiLeaks due to a violation of the PayPal Acceptable Use Policy, which states that our payment service cannot be used for any activities that encourage, promote, facilitate or instruct others to engage in illegal activity.[10]

All this shows the vulnerability of radical activists when relying too much on the corporate structures that rule the internet and facilitate financial transactions online. While this is an illustration of the constraints of the networked opportunity structure, there are also plenty of opportunities the network provides to resist and to retaliate.

Networked Strategies of Contention

Activists typically enact a variety of strategies when dealing with mainstream political cultures. Rucht (2004) identified four such strategies when studying the history of protest movements, which I present here in a somewhat different order for narrative purposes – the development of alternatives to the mainstream, adaptation to the mainstream, attack of the mainstream and abstention from the mainstream. As will be shown in what follows, WikiLeaks and Assange in particular used all four of these strategies interchangeably.

Alternatives

At the outset WikiLeaks operated at the level of complete independence from the system, developing alternatives that completely bypass mainstream public spaces, positioning themselves as merely making information that was sent to them accessible through their website, unaltered and as they had received it. Gradually WikiLeaks built-up its name recognition and reputation as a maverick organisation releasing ever more explosive content. The long-term involvement of both Assange and Domscheit-Berg in the hackers-movement, respectively in Australia and Germany, played an important role in terms of building their social capital within the freedom of information movement.

However, the increased notoriety of WikiLeaks as an organisation amongst the likeminded did not necessarily translate in more attention for the actual content of the leaks in the mainstream media as a whole, nor did it wield more funding to keep the organisation and their networked infrastructure running. In November 2009 someone leaked 500.000 text messages relating to 9/11, mostly by US officials. They provided an account of the panic, fear and chaos that was prevalent that day. In the course of publishing these messages WikiLeaks discovered that that wealth of information did not yield much

publicity for the content in the first instance, nor for WikiLeaks as an organisation. In fact, they had also run out of money and it was decided to shut down WikiLeaks on 23 December 2009 as a kind of signal to the world and to garner (financial) support (Domscheit-Berg, 2011, p. 104).

Adaptation

When Wikileaks went back online in January 2010 an important lesson had been learned. WikiLeaks decided to change its strategy from relying on alternatives to adapt more to the media logic, even if that entailed relinquishing some of its principles. The collateral murder video is a good example of this. Instead of releasing the raw footage, WikiLeaks decided to edit the footage in order to increase its impact, subtitling what was said and adding a provocative quote of Orwell on the deceiving nature of political language. In doing so, WikiLeaks renaged on its promise to publish material as they received it and started assuming an editorial role and stance.

When they received the Afghan, Iraqi and diplomatic data, it became clear quite quickly that WikiLeaks would need help and resources in order to make sense of the millions of leaked documents and increase their impact in the global media. Allies were sought and found in the mainstream media to build an extensive database able to make connections and do searches (Leigh & Harding, 2011; Keller, 2011). These exclusive deals were designed to ensure that global mainstream media outlets would run long series of stories on the basis of the leaked documents, which ideally would be reinforced by other media across the world.

While this was successful to a large extent, the deluge of Wikileaks stories at some point has undoubtedly led to them becoming less newsworthy, leading to what was called WikiLeaks fatigue. Even with the active involvement of journalists and global media organisations, overload of WikiLeaks related reports was considered a problem. One of the main problems, Domscheit-Berg (2011) acknowledges, 'was the sheer volume of data. The collection of material was too large for people to enter into the debate simply' (p. 153).

Attack

The network 'allows clever workarounds and David-against-Goliath battles that can sometimes reward technical virtuosity and tactics over the brute force of state authority and capitalist logic' (Fenster, 2011, p. 15). As such, WikiLeaks, as well as loosely associated actors, enacted several networked resistance strategies to counter the efforts of state and corporate actors to close down its operations. Such attack strategies are an illustration of the constitutive role that communication resistance can play in becoming direct action rather than just facilitating it.

On 30 July 2010, four days after releasing the Afghan War Diaries, WikiLeaks distributed a 1.4 Gb encrypted file called 'insurance.aes256'. It was preemptive move against the various legal and extra-legal attacks it was expecting. The file was first given to some trusted parties on USB-sticks, but later on it was also distributed worldwide through the BitTorrent peer2peer network[11]. It is

unknown what the file exactly contains, but the idea would be that if anything happened to WikiLeaks/Assange, the password for this file would be made publicly available allowing anyone who has downloaded the file on their computer to unlock it.

When Amazon ousted WikiLeaks and EveryDNS ceased to link their domain name to their IP address, they simply moved their content and DNS service to European providers. A tweet from WikiLeaks on 1 December 2010 read: 'Free speech the land of the free – fine our $ are now spent to employ people in Europe'[12]. In the aftermath of this, several mirror sites sprung up all over the internet, making sure the content of WikiLeaks remained accessible[13].

The repression against WikiLeaks also activated latent ties with the hacktivist collective Anonymous, who through coordinated Distributed Denial of Service (DDoS) attacks targeted the websites of respectively PostFinance (6/12/2010), EveryDNS (7/12/2010), MasterCard (8/12/2010), Visa (8/12/2010), PayPal (9/12/2010) and MoneyBookers (10/12/2010). Amazon was also targeted, but that particular attack had to be aborted because the 'hive' of computers engaged in the operation was not 'big enough to attack Amazon' (Tweet on #AnonOpsNet, 9/12/2010). Besides corporate actors, Anonymous also attacked political actors such as Sarah Palin's PAC (8/12/2010) and two days later an affiliate site conservatives4palin.com. Joe Lieberman was also a prime target and his Senate website was briefly disrupted[14].

More controversial, certainly from within the Hacker movement, were the attacks on the Swedish Prosecution Authority on 7 December 2010, followed by an attack the next day on the lawyers' firm *Borgstrom and Bodström* which represents the two women accusing Assange of sexual molestation. The attacks on the Swedish prosecutor's office and the lawyer-firm was, according to those within the hacker movement who wanted to separate WikiLeaks as a project and an activist organisation from the personality and private issues of its eccentric and autocratic founder, highly problematic (Domscheit-Berg, 2011, p. 207). As explained earlier, the case of WikiLeaks also brings to bare the problems of collapsing the political and the personal and the conflicts this can potentially produce internally and with latent actors.

Abstention

Given the opacity of WikiLeaks as an organisation, some degree of temporal abstention also features prominently in the strategies of WikiLeaks; engaging with and adapting to mainstream logics, but at other times disengaging from it and abstaining from interaction. As Guardian editor-in-chief Rusbridger recalls: 'Assange was, at the best of times, difficult to contact, switching mobile phones, email addresses and encrypted chat rooms as often as he changed his location' (in Leigh & Harding, 2011, p. 17). Also Domscheit-Berg (2011) accounts of numerous periods in which Assange was unreachable even for core-members of the organisation.

After the clampdown following the release of the diplomatic cables, Assange and WikiLeaks increasingly abstained fully from engagement with mainstream culture or society at large. As mentioned earlier WikiLeaks

disabled their online submission system and Assange himself largely disappeared from the mainstream public space, concentrating on the court-case against him deciding on his extradition to Sweden.

Conclusions

At the level of networks, the WikiLeaks case exemplifies how the development of strong offline ties is combined with the strength of weak mediated ties as well as with the activation of latent ties at strategic moments. However, the complication when analyzing WikiLeaks and its networks consists in the difficulty to distinguish WikiLeaks as an organisation from its main spokesperson and founder Assange. This led to conflictual tensions with detrimental effects on the strong ties with core-members and journalists, as well as splitting latent sympathizers.

Despite this, WikiLeaks presents itself as a fascinating case to understand the dynamics of mediated resistance and its consequences on power. Benkler (2011) concludes that WikiLeaks represents a 'vivid instance of the ways in which the networked society has disrupted traditional pathways for the exercise of power and created new dimensions of power and new degrees of freedom' (p. 750). Both at a discursive level of analysis as well as a material one, opportunities were seized to further the anti-war and pro-transparency discourse, to increase the impact of the leaks, to protect the identity of activists and whistleblowers.

However, as pointed out in the analysis the empire always tends to strike back and this time with a vengeance. WikiLeaks and Assange were positioned within the terrorism frame and serious attempts were made to close down its operations, exposing the vulnerability of radical activists when they are dependent on market-based platforms for hosting content and for funding purposes. Furthermore, the abundance of information and of WikiLeaks related reporting at some point revealed to be problematic in its own right, as WikiLeaks fatigue set in. It is therefore debatable whether WikiLeaks really managed to disrupt the traditional pathways of power in the long run as suggested by Benkler.

WikiLeaks as well as other related actors, such as Anonymous, employ a variety of strategies in their relations with mainstream political culture. The development of an alternative space for the posting of leaked information and its growing social capital amongst the hacker communities were instrumental to the rise of WikiLeaks and arguably led to more and more documents being leaked through its platform. However, WikiLeaks increasingly started assuming an editorial role and adapting to the media logic by involving mainstream media actors and granting them exclusivity in order to increase media resonance. This came at a cost, namely loosing control of the data leaked to its site thereby also undermining its credibility and social capital. When WikiLeaks was crippled by corporate repression, a strategy of attack became needed. Latent ties were instrumental in this regard, leading to Anonymous retaliating and flexing its counter-power. However, it has to be

kept in mind though that despite the highly spectacular and symbolic nature of these attacks, the actual damage and disruption they caused was minimal.

Furthermore, for the time being at least, it seems that the forces out to damage and silence WikiLeaks/Assange are prevailing and the culture of secrecy and information control restored. However, this is precisely the nature of the mediation opportunity structure for information and communication resistance; opportunities open up or are created, which are subsequently closed down after which new ones emerge.

References:

Ackerman, J. M. and Sandoval-Ballesteros, I. E. (2006). The Global Explosion of Freedom of Information Laws. *Administrative Law Review,* 58(1), 85-130.

Arquilla, J. and Ronfeld, D. (2001). *Networks and Netwars: The Future of Terror, Crime and Militancy*. Santa Monica: RAND.

Assange, J. (2010). Don't shoot messenger for revealing uncomfortable truths. *The Australian*, 8 December: http://www.theaustralian.com.au/in-depth/wikileaks/dont-shoot-messenger-for-revealing-uncomfortable-truths/story-fn775xjq-1225967241332 [Last Consulted on 28 May 2013]

Assange, J. (2011). A Q&A with Julian Assange (part I): on the Arab Spring, phone hacking, and WikiLeaks' ethics. *Frontline Club*, 11 May: http://www.frontlineclub.com/a_qa_with_julian_assange_part_i_on_the_arab_spring_phone_hacking_and_wikileaks_ethics/ [Last Consulted on 28 May 2013]

Benkler, Y. (2011). Networks of Power, Degrees of Freedom. *International Journal of Communication,* 5, 721-55.

Brooke, H. (2011). Fess up - or face a future of leaks. *British Journalism Review,* 22(1), 17-9.

Burns, J. F. and Somaiya, R. (2010). WikiLeaks Founder on the Run, Trailed by Notoriety. *New York Times*, 23 October: http://www.nytimes.com/2010/10/24/world/24assange.html?pagewanted=all [Last Consulted on 28 May 2013]

Cammaerts, B. (2011). Disruptive Sharing in a Digital Age: Rejecting Neoliberalism? *Continuum: Journal of Media and Cultural Studies,* 25(1), 47-62.

Chadwick, A. (2006). *Internet Politics: States, Citizens, and New Communication Technologies*, Oxford: Oxford University Press.

Collins, B. S. and Mansell R. (2005). Cyber Trust and Crime Prevention. In R. Mansell & B. S. Collins (Eds.), *Trust and Crime in the Information Society*. Cheltenham: Edward Elgar Publishers, pp. 11-55.

Conway, M. (2007). Cyberterrorism: Hype and Reality. In L. Armistead (Ed.), *Information Warfare: Separating Hype From Reality*. Washington, DC: Potomac Books, pp. 73-94.

Crovitz, G. L. (2010). 'Julian Assange, Information Anarchist', The Wall Street Journal, 6 December: http://online.wsj.com/article/SB10001424052748703989004575653113548361870.html [Last Consulted on 28 May 2013]

della Porta, D. and Diani, M. (2006). *Social Movements: an introduction* – 2nd Edition. Oxford: Blackwell Publishing.

Domscheit-Berg, D. (2011). *Inside WikiLeaks: My Time with Julian Assange at the World's Most Dangerous Website*. New York: Crown.

Fenster, M. (2011). Disclosure's Effects: WikiLeaks and Transparency. *SSRN Working Paper Series* 28 March: pp. 1-52: http://ssrn.com/abstract=1797945 [Last Consulted on 28 May 2013]

Ferree, M. M., Gamson, W. A., Gerhards, J. and Rucht, D. (2002). *Shaping Abortion Discourse: Democracy and the Public Sphere in Germany and the United States.* Cambridge: Cambridge University Press.

Florini, A. (2003). *The Coming Democracy: New Rules for Running a New World.* Wahsington, DC: Island Press.

Gamson, W. A. (1992). *Talking Politics.* Cambridge: Cambridge University Press.

Garnham, N. (2005). The information society debate revisited. In J. Curran and M. Gurevitch (Eds.), *Mass Media and Society* - 4th Edition, London: Hodder Arnold, pp. 287-302.

Halliday, J., & Arthur, C. (2010). WikiLeaks: Who are the hackers behind Operation Payback? *The Guardian*: http://www.guardian.co.uk/media/2010/dec/08/anonymous-4chan-wikileaks-mastercard-paypal [Last Consulted on 28 May 2013]

Haythornthwaite, C. (2005). Social Networks And Internet Connectivity Effects, *Information, Communication & Society,* 8(2), 125-47.

Jordan, T. (2008). *Hacking: Digital Media and Technological Determinism.* Cambridge: Polity Press.

Keller, B. (2011). The boy who kicked the hornet's nest. In A. Star (Ed.), *Open Secrets: WikiLeaks, War and American Diplomacy.* New York: New York Times, pp. 6-26.

Kierkegaard, S. (2009). Open access to public documents – More secrecy, less transparency! *Computer Law & Security Review,* 25, 3-27.

Koopmans, R. (1999). Political. Opportunity. Structure. Some Splitting to Balance the Lumping, *Sociological Forum,* 14(1), 93-105.

Korsgaard, C. M. (1989). The Right to Lie: Kant on Dealing with Evil. *Philosophy & Public Affairs,* 15(4), 325-49.

Leigh, D. & Harding, L. (2011). *WikiLeaks: Inside Julian Assange's War on Secrecy.* London: Guardian Books.

Leigh, D., Harding, L., Hirsch, A., & MacAskill, E. (2010). WikiLeaks: Interpol issues wanted notice for Julian Assange. *The Guardian*, 30 November: http://www.guardian.co.uk/media/2010/nov/30/interpol-wanted-notice-julian-assange [Last Consulted on 28 May 2013]

Livingstone, S. (2007). On the material and the symbolic: Silverstone's double articulation of research traditions in new media studies. *New Media and Society,* 9(1), 16-24.

Ludlow, P. (2010). 'WikiLeaks and Hacktivist Culture'. *The Nation*, 4 October: 25-6.

Lundby, K. (2009). Introduction: "Mediatization" as Key. In K. Lundby (ed.) *Mediatization: concept, changes, consequences.* New York: Peter Lang, pp. 1-20.

Martin, B. (1999). Whistleblowing and Nonviolence. *Peace & Change,* 24(1), 15-28.

Mayer-Schönberger, V., & Lazer, D. (2007). *Governance and information technology: from electronic government to information government.* Cambridge, MA: MITpress.

McMillan, Robert (2010). FBI raids ISP in Anonymous DDoS investigation. *Computer World*, 30 December. See: http://www.computerworld.com/s/article/9202838/FBI_raids_ISP_in_Anonymous_DDoS_investigation [Last Consulted on 28 May 2013]

Poulsen, K. (2010). Lieberman Introduces Anti-WikiLeaks Legislation. *Wired*, 2 December: http://www.wired.com/threatlevel/2010/12/shield/ [Last Consulted on 28 May 2013]

Rana, K. S., & Kurbalija, J. (eds) (2007). *Foreign Ministries: Managing Diplomatic Networks and Optimizing Value.* Geneva: DiploFoundation.

Rice, X. (2007). 'The looting of Kenya'. The Guardian, 31 August: http://www.guardian.co.uk/world/2007/aug/31/kenya.topstories3 [Last Consulted on 28 May 2013]

Rucht, D. (2004). The Quadruple "A": Media Strategies of Protest Movements Since the 1960s. In W. van de Donk, B. D. Loader, P. G. Nixon & D. Rucht, (eds.) *Cyberprotest: New Media, Citizens, and Social Movements*. London: Routledge, pp. 29-58.

Snow, D. A., & Benford, R. D. (1988). Ideology, frame resonance, and participant mobilization. *International Social Movement Research,* 1, 197-217.

Sterner, E. (2011). WikiLeaks and Cyberspace Cultures in Conflict. *Marshall Institute Policy Outlook*. February: http://www.marshall.org/pdf/materials/931.pdf [Last Consulted on 28 May 2013]

Stiglitz, J. (1999). On Liberty, the Right to Know, and Public Discourse: The Role of Transparency in Public Life. Oxford Amnesty Lecture. 27 January: http://siteresources.worldbank.org/NEWS/Resources/oxford-amnesty.pdf [Last Consulted on 28 May 2013]

Tarrow, S. (1994). *Power in Movement: Social Movements, Collective Action and Mass Politics in the Modern State*. Cambridge: Cambridge University Press.

About the Author:

Bart Cammaerts is a senior lecturer at the Media and Communication Department of the London School of Economics and Political Science. His research centers around the relationship between media as well as communication technologies and activism with particular focus on multi-stakeholder policy processes, media strategies of activists, representation of protest, alternative media cultures and issues relating to media power, resistance and public-ness. He is former chair of the Communication and Democracy section of ECREA and vice-chair of the Communication Policy and Technology section of IAMCR.

Contact-Details:
LSE, Media and Communication Department, Houghton Street, London WC2A 2AE, UK.
E-mail:
b.cammaerts@lse.ac.uk

Notes:

1 See Domscheit-Berg (2011) for a more comprehensive overview of leaks

2 quote from a public talk at Frontline Club, London, 26th July 2010

3 See: http://www.youtube.com/watch?v=5rXPrfnU3G0 [Last Consulted on 28 May 2013]

4 See: http://www.larrysanger.org/wikileaks.html [Last Consulted on 28 May 2013]

5 Founded in 1984 in Lubbock, Texas, see: http://www.cultdeadcow.com/ [Last Consulted on 28 May 2013]

6 See: http://www.hacktivismo.com/about/index.php [Last Consulted on 28 May 2013]

7 See: http://w3.cultdeadcow.com/cms/about.html [Last Consulted on 28 May 2013]

8 See: https://www.torproject.org/ [Last Consulted on 28 May 2013]

9 US Patent No. 6266704 - Onion routing network for securely moving data through communication networks.

10 See: https://www.thepaypalblog.com/2010/12/paypal-statement-regarding-wikileaks/ [Last Consulted on 28 May 2013]

---

11 See:
http://thepiratebay.org/torrent/5741985/INSURANCE.AES256_WIKILEAKS.SECRET.DOCUMENT.2010.08.06 [Last Consulted on 28 May 2013]

12 See: http://twitter.com/#!/wikileaks/status/10058229002272768 [Last Consulted on 28 May 2013]

13 for an overview of official mirror-sites see: http://wikileaks.info/ [Last Consulted on 28 May 2013]

14 It has to be noted that most of these DDoS attacks resulted in rather limited downtime for most of the sites that were targeted. For example, Lieberman's senate site was down for a total of 12 minutes, Sarah Palin PAC-site for 25 minutes, Paypal for 33 minutes, Mastercard for 1 hour 17 minutes. The attack on the Swiss bank Postbank was more successful as their e-banking services were down for a total of 33 hours. (Source: http://pandalabs.pandasecurity.com/tis-the-season-of-ddos-wikileaks-editio/ - Last Consulted on 28 May 2013)