You have no sovereignty where we gather

–

Wikileaks and Freedom, Autonomy and Sovereignty in the cloud

Bodó Balázs, PhD (Budapest University of Technology and Economics)

Working paper (draft), March, 2011

Abstract

Wikileaks represents a new type of (h)activism, which shifts the source of potential threat from a few, dangerous hackers and a larger group of mostly harmless activists -- both outsiders to an organization -- to those who are on the inside. For insiders trying to smuggle information out, anonymity is a necessary condition for participation. Wikileaks has demonstrated that the access to anonymity can be democratized, made simple and user friendly.

Being Anonymous in the context of Wikileaks has a double promise: it promises to liberate the subject from the existing power structures, and in the same time it allows the exposure of these structures by opening up a space to confront them. The Wikileaks coerced transparency, however, is nothing more than the extension of the Foucauldian disciplinary power to the very body of state and government. While anonymity removes the individual from existing power relations, the act of surveillance puts her right back to the middle.

The ability to place the state under surveillance limits and ultimately renders present day sovereignty obsolete. It can also be argued that it fosters the emergence of a new sovereign in itself. I believe that Wikileaks (or rather, the logic of it) is a new sovereign in the global political / economic sphere. But as it stands now, Wikileakistan shares too much with the powers it wishes to counter. The hidden power structures and the inner workings of these states within the state are exposed by another *imperium in imperio*, a secretive organization, whose agenda is far from transparent, whose members, resources are unknown, holding back an indefinite amount of information both on itself and on its opponents.

I argue that it is not more secretive, one sided transparency which will subvert and negate the control and discipline of secretive, one sided transparency, it is anonymity. The subject's position of being *"a multiplicity that can be numbered and supervised",* its state of living in a *"sequestered and observed solitude"* (Foucault 1979) can only be subverted if there is a place to hide from surveillance. I argue that maybe less, and not more transparency is the path that leads to the aims of Wikileaks.

"We have to be very attentive and united at a state level to fight against what is a threat to democratic authority and sovereignty," - French government spokesman Francois Baroin speaking out against wikileaks releasing US diplomatic cables.

„Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."- A Declaration of the Independence of Cyberspace, John Perry Barlow

Intro

In 2010, an organization called Wikileaks started to publish hundreds of thousands of secret US diplomatic cables and military documents, acquired from anonymous whistleblowers. The publication of these documents marks the beginning of a new era. While all the critical information within these organizations is already digital, never has the firewall between a secret and a public knowledge been thinner. Sharing secrets and in the same time preserving anonymity seems to be easier than ever. And as the continuous accessibility of Wikileaks so far has proved, even the most powerful sovereign in the world can do little to contain a leak after it has happened. State sovereignty and corporate autonomy needs to be rethought.

But not only *their* self-determination is in question. Wikileaks itself has also come under attack: their access to the global payment system was cut, their hosting provider stopped serving them and their access to the global Domain Name System was also curtailed, despite the fact that no official charges were made against the organization. These steps have so far been inadequate to make Wikileaks disappear or to stop the dissemination of the confidential materials. But the questions still linger: what are the critical infrastructures that are absolutely necessary for any digital, networked organization to survive? Are there any real gatekeepers on the web, and if there are, who are they, and how powerful they are? How effective is their control over the critical infostructures? To what extent can any organization expect to be sovereign in the cloud?

„You have no sovereignty where we gather." John Perry Barlow's words (Barlow 1996) that declared the independence of cyberspace now mark a full-blown cyber-war between states, corporations and ad-hoc, informal, hacktivist networks over the issues of sovereignty, autonomy, self-determination on both sides of what has been the cyber/real divide. But that distinction does not have any meaning anymore. Cyberspace is not another, distant, secluded space which Barlow envisioned. The declaration of the cyberspace is not the foundation of a sovereign in a far away land. Cyberspace is in the very heart of traditional institutions: the state, economic enterprises, society. And the question now is whether cyberspace can be inserted into the societal order, which - at least in principle - rests on mutual checks and balances, on an equilibrium that ensures that no power is left unchecked. Is it true that states have no sovereignty in cyberspace? And what happens when the citizens of the cyberspace start to gather *inside* the state, inside the corporations, easily crossing

that never-existent border between cyberspace and the “real world”? What is left of the sovereignty of the state, the autonomy of our traditional institutions when *they start to gather [and? to?] put these institutions under constant surveillance*?

The outcome of this conflict greatly depends on the role everyday citizens will play in this power universe. The digital traces of our online being serve as the most important raw material in the digital economy. Also, (digital) transparency is the key concept in the Foucauldian understanding of power, as it serves to maintain and reproduce power-relations within society. On the other hand, these individually impotent and powerless users can quickly team up into informal, anonymous, ad-hoc action networks that from time-to-time make a powerful impact. Wikileaks is the most recent and most potent tool in the hands of these crowds as it enables resistance to power both by the anonymity it offers and by the leaks which force transparency upon the state. *The real question is whether Wikileaks can be a true emancipatory force, which will lead anonymous crowds to a self-aware use of these powers and to fulfill their actual potential?*

Does Wikileaks mark the rise of a new sovereign in our world? A new world power which lacks standing armies, natural resources, the strategic geopolitical location, and the financial might that characterized world powers before? A new sovereign, which draws its power from both the ability to disrupt the information flows, and the ability to provide anonymity to its users? A new power which is sovereign because in the fragmented infrastructure landscape of the internet, it can always find refuge from where it can safely operate? A power which is organized unlike any other power so far, because it exists beyond the formal structures of law, economy and society?

Soon we will find out.

A new era of hacktivism

Wikileaks-enabled activism is quite different from the types of cyber activism and hacktivism that were prominent in the last decade. The latter, let’s call it hacktivism 1.0, *“breaks down into two broad streams of actions: 1. Mass virtual direct actions, which use cyberspatial technologies of limited potential in order to re-embody virtual actions, [and 2.] digitally correct actions, which defend and extend the peculiar powers cyberspace creates. […]Whereas mass action hacktivists look to networks to do things for them, to be a place in which protest can occur just as roads are places in which demonstrations can occur, digitally correct hacktivists attempt to form the nature of the roads and passages of cyberspace. In doing this they generate actions directly focused on the codes that make cyberspace the place it is”* (Jordan and Taylor 2004). Hacktivism 1.0 offers few opportunities for political action. They can be complex technological stunts, committed by highly skilled computer programmers. The results of this type of activism are either the disruption of the infostructure of the target organization or some specialized software tool to aid activists. Such actions are costly and time consuming, therefore relatively rare. On the other hand, hacktivism offers individuals the chance to participate in electronic civil disobedience, like virtual sit-ins, where, along with thousands of others one can try to overload the public web services of the target organizations. In this sense electronic disobedience is closely related to the earlier, non-electronic civil disobedience movements. These attacks – Distributed Denial of Service (DDoS) attacks as they are called now –

require no technical skills, and beyond making a website inaccessible for the time of the attack, they yield little more than the attention generated by the news of the attack. Hacktivism 1.0 is torn between highly effective but rare instances of hacking, and relatively frequent cyber-protests with little more than symbolical value.

Wikileaks marks the beginning of hacktivism 2.0.[1] Wikileaks is first and foremost an infostructure provider, with the immense potential to empower mass-scale cyber-activism. Wikileaks offers three crucial factors through which the effectiveness of hacker attack can be merged with the ease and openness of mass actions. First, it offers a highly resistant, autonomous content distribution network, which so far has been able to survive even the most aggressive attacks against its infrastructure.[2] Second, it has all the attention of the world, including key media organizations which participate in the verification[3] and publication of the disclosed information. [4] And what is the most important: it promises anonymity.

Hacktivism 1.0 was the activism of *outsiders*. Its organizing principle was to get outsiders into the territory of the other. Wikileaks, on the other hand, is an infostructure developed to be used by *insiders.* Its sole purpose is to help people *get information out* from an organization. Wikileaks shifts the source of potential threat from a few, dangerous hackers and a larger group of mostly harmless activists -- both outsiders to an organization -- to those who are on the inside. For mass protesters and cyber activists anonymity is a nice, but certainly not an essential feature. For insiders trying to smuggle information out, anonymity is a necessary condition for participation. Wikileaks has demonstrated that the access to such features can be democratized, made simple and user friendly. Easy anonymity also radically transforms who the activist may be. It turns a monolithic, crystal clear identity defined solely through opposition, into something more complex, multilayered, and hybrid by allowing the cultivation of multiple identities, multiple loyalties. It allows those to enter the activist scene who do not want to define themselves – at least not publicly – as activist, radical or oppositional. The promise – or rather, the condition -- of Wikileaks is that one can be on the inside and on the outside at the same time. Through anonymity the mutually exclusive categories of inside/outside, cooption/resistance, activism/passivity, power/subjection can be overridden and collapsed.

[1] I share Malcolm Galdwell's opinion on Facebook and Twitter as an ineffective tool for resistance and achieving social change. (Gladwell 2010) These tools are still for outsiders, and unlike Wikileaks they separate the place of impact from the place of resistance. „[I]t is simply a form of organizing which favors the weak-tie connections that give us access to information over the strong-tie connections that help us persevere in the face of danger. It shifts our energies from organizations that promote strategic and disciplined activity and toward those which promote resilience and adaptability. It makes it easier for activists to express themselves, and harder for that expression to have any impact. The instruments of social media are well suited to making the existing social order more efficient. They are not a natural enemy of the status quo."

[2] It would be interesting to learn how the internal organization and governance of Wikileaks helps them to survive the attacks from the outside. However, at the time of writing this, little is known about how Wikileaks manages its defense and ensures its survival.

[3] The verification of leaked information is crucial in the success of Wikileaks. No wonder that one of the tactics proposed by intelligence agencies to counter Wikileaks was to flood them with false information.

[4] See a critique of the relationship of Wikileaks on the mainstream media at (Chossudovsky 2010).

Anonymous

Anonymous is a name frequently appearing in articles about Wikileaks. It refers to a group of hacktivists (from the 1.0 type), who organized mass cyber-attacks against companies that severed their ties with Wikileaks in the tumultuous last weeks of 2010. According to their self-description: *“Anonymous is not a person, nor is it a group, movement or cause: Anonymous is a collective of people with too much time on their hands, a commune of human thought and useless imagery. A gathering of sheep and fools, assholes and trolls, and normal everyday netizens. An anonymous collective, left to its own devices, quickly builds its own society out of rage and hate. […]They have no leader, no pretentious douchebag president or group thereof to set in stone what Anonymous is and is not about. This makes them impossible to control or organize. Not really a collective at all - more like a stampede of coked-up lemmings. […] Anonymous is not a single person, but rather, represents the collective whole of the internet. As individuals, they can be intelligent, rational, emotional and empathetic. As a mass, a group, they are devoid of humanity and mercy.” (Encyclopedia Dramatica 2011)*

This type of Anonymous (let’s call it Anonymous 1.0) is the fuel of (h)acktivism 1.0. They are a group of outsiders who are rallied against something. They are on the outside, trying to get in, but if they get in, they have little more in their minds than to wreak havoc. In the last months of 2010 Anonymous was credited for launching DDoS attacks against those companies that severed their business relationship with Wikileaks, including Paypal, Mastercard, Visa, as well as OpenDns and Amazon. These attacks gained little more than some press attention. Their effectiveness in terms of disrupting the everyday operations of these companies, or inducing a shift in their policies was nil.

There is, however, another, much more important Anonymous (Anonymous 2.0) in the Wikileaks story that needs to be discussed: those powerful individuals in privileged positions within the existing power structures, who now can safely subvert the very power structures that they define (and that define them). If Anonymous is to be feared, it is not because some rascals with short attention span download a crudely written software tool to attack websites, but because of those, for whom such anonymity lowers the costs of exposing and confronting power from within. Lowering the cost of safe opposition is exactly what Wikileaks is for.

Being Anonymous in the context of Wikileaks has a double function: it liberates the subject from the existing power structures, and in the same time it allows the exposure of these structures by opening up a space to confront them.

Anonymity offers the chance for the individual to – at least partially – remove herself from the pre-existing discursive determinations and power relations and consider alternatives. *“If governmental rationalities operate through the nomination and specification of a positive identity through a series of constitutive exclusions, rarefactions and restrictions, then the practices of freedom are enabled by withholding the knowledge of oneself, resisting the injunction to a ‘confessional’ self-expression, declining the incitement to active participation in the governmentally sanctioned discourse. Anonymity may then serve ‘to encourage freedom by increasing the scope of actions not susceptible to official observation, records and interpretation’”* (Prozorov 2007, citations ommitted). Anonymity is important because it liberates insiders.

Being Anonymous is an identity play, and as an identity play, it is a loyalty play. As an identifiable member of the society, the individual is bound by formal and informal attachments and hierarchies, the breaches of which are severely and instantly punished. Being Anonymous means that one's identity and loyalty is up for grabs, it is fluid, it is independent, it is freed from it social base. Wikileaks, being the key anonymity-providing infostructure, supports new loyalties that are detached from the corrupted and failing national identities, the debilitating chorus of corporate anthems, historical determination and the normalizing judgment of Facebook peers. *"People are asked to identify personally with organisations who can either no longer carry historical projects worthy of major sacrifices or expressly regard their employees as nothing but expendable, short−term resources. This […] creates the cognitive dissonance that justifies, perhaps even demands, the leaker to violate procedure and actively damage the organisation of which he, or she, has been at some point a well−acculturated member (this is the difference to the spy). This dissonance creates the motivational energy to move from the potential to the actual."* (Stalder 2010) When this happens, one's 'proper' identity, one's real name turns into a mere pseudonym that serves to hide one's 'real' identity, one's true loyalties.

Wikileaks, the same space which allows the individual to liberate himself promises him the chance to liberate others. *It is in fact designed in a way that it only liberates those who are willing to 'liberate' others.* The big Wikileaks promise is that the exposure of how power is structured, organized, the exposure of how *"the great systems of exclusion which forge discourse - forbidden speech, the division of madness and the will to truth"* (Foucault 1981) operate will break these systems down and force them to change for the better.

This claim is, however, unfounded. The Wikileaks coerced transparency is nothing more than the extension of the Foucauldian disciplinary power to the very body of state and government. While anonymity removes the individual from existing power relations, the act of surveillance puts her right back to the middle.

Transparency

Eben Moglen, in his „Freedom in the cloud" talk (Moglen 2010) outlined a grim vision of individual freedoms in the cloud age. He argued that individual freedoms are severely limited when Facebook-, and Google-like central entities hold all the information about us and users have no access to, or chance to control that information and limit the access of others to it. He argued that by trusting commercial third parties to provide us with free services in exchange for our personal data, we surrender all the information about who we are and how we behave in the digital universe. We are disempowered by being spied upon, we are disempowered by our lack of information-autonomy, we are disempowered by voluntarily surrendering ourselves to the invisible observer in this digital Panopticon.

By putting Moglen's arguments parallel to the Wikileaks story we need to ask ourselves: in what way are the two transparencies different? Are we expecting the Wikileaks-induced transparency to do to corporations and governments what we are afraid of being done to us? Does transparency on the state, corporate and on the individual level serve the same goal: pure, internalized control?

Assange's quest for a better government suggests that in some sense the answer is yes. A well mannered and well-behaving, ethical, productive and accountable government created by the Wikileaks transparency[5] is very similar to the benefits Bentham assigned to his Panopticon design, as cited by Foucault: *"Morals reformed – health preserved – industry invigorated – instruction diffused – public burthens lightened – Economy seated, as it were, upon a rock – the gordian knot of the Poor-Laws not cut, but untied – all by a simple idea in architecture!"*

But it would be a misunderstanding to equate the state with power, the secrets with how control operates. Also, it is a misunderstanding to expect better governance from transparency. Nowhere is it said, that the discipline of the Panopticon would in any way result in any of those ideals that Assange is longing for. It is true that the Panopticon produces more efficient, more productive, more obedient, and more controlled subjects, but this has nothing to do with the state, the society, or power turning more just, enlightened, ethical or truthful. Even if the chain of events would stop at Wikileaks, there would be little reason to believe that *"[t]he public scrutiny of otherwise unaccountable and secretive institutions forces them to consider the ethical implications of their actions"* (wikileaks.org 2008). The only apparent and possible outcome of panopticism is more panopticism. The consideration of the ethical implications of one's actions is nowhere guaranteed.

The way the US state apparatus has reacted to Wikileaks clearly illustrates this point. In a memorandum on January 3rd, 2011, the National Counterintelligence Executive and the Director of the Information Security Oversight Office detailed the procedures by which they hope to prevent any further leaks. The document is a 14-page long checklist covering all aspects of keeping secrets: "the measures in place to determine appropriate access for employees to classified information"; the existence of counterintelligence programs; the use of back-up media; "a trend analysis of indicators and activities of the employee population which may indicate risky habits or cultural and societal differences other than those expected for current employees for security clearances" and the *"use [of] psychiatrist and sociologist to measure [the r]elative happiness as a means to gauge trustworthiness [, and the d]espondence and grumpiness as a means to gauge waning trustworthiness"* (Lew 2011).

This document is the blueprint of an internal total transparency program that is designed to maximize the control over the state apparatus in order to detect potential leakers and prevent information breaches. The state reacted to the transparency of Wikileaks by creating a transparency of its own. This is the classic example of internalization: the state, under surveillance has internalized the expectations and now is busy learning how to make sure that what is not to be shown stays truly hidden. Secrets to outsiders can only be protected through total transparency on the inside. This is the problem with total control: it does not annihilate undesired behavior, it does not mute and reform inappropriate and prohibited desires, it only suppresses them, and fosters secrecy and deceit. Transparency will not break the logic of power based on panopticism: *"The panoptic schema, without disappearing as such or losing any of its properties, was destined to spread throughout the social body; its vocation was to become a generalized function. […] While, on the one hand, the*

[5] The Wikileaks mission statement clearly defines its aims: "Publishing improves transparency, and this transparency creates a better society for all people. Better scrutiny leads to reduced corruption and stronger democracies in all society's institutions, including government, corporations and other organisations. A healthy, vibrant and inquisitive journalistic media plays a vital role in achieving these goals. We are part of that media" (wikileaks.ch 2010).

disciplinary establishments increase, their mechanisms have a certain tendency to become 'de-institutionalized', to emerge from the closed fortresses in which they once functioned and to circulate in a 'free' state; the massive, compact disciplines are broken down into flexible methods of control, which may be transferred and adapted. […]'Discipline' may be identified neither with an institution nor with an apparatus; it is a type of power, a modality for its exercise, comprising a whole set of instruments, techniques, procedures, levels of application, targets; it is a 'physics' or an 'anatomy' of power, a technology.[…] On the whole, therefore, one can speak of the formation of a disciplinary society in this movement that stretches from the enclosed disciplines, a sort of social 'quarantine', to an indefinitely generalizable mechanism of 'panopticism'" (Foucault 1979). The transparency of Wikileaks does not counter this process, it reinforces it. By putting the locus of sovereign power under surveillance it simply draws the state under this form of control, putting the last missing piece of the puzzle to its place. Wikileaks in same sense only propagates the control it wishes to subvert. It only helps the logic of panopticism to fold and close upon itself.

Sovereignty

Sovereignty, in its strictest definition is the supreme authority within a territory. The three components of sovereignty: being supreme, having authority and territoriality have all been transformed by the rapid rise of supranational, supra-governmental political, economic, legal institutions, the formation and the consolidation of global networks of information, telecommunications, finance, logistics, extraterritorial corporations, and (private) justice systems. Since such external authorities limit or determine state actions in the fields of finance, economics, social policy, foreign and internal politics, military, or human rights, globalization was seen as a threat to the traditional concept of post-Westphalian sovereignty. Such external authorities made state sovereignty to be less and less absolute. But as Saskia Sassen argues, the interplay between sovereignty and globalization is more complex than that. "*The strategic spaces where many global processes take place are often national; the mechanisms through which the new legal forms necessary for globalization are implemented are often part of state institutions; the infrastructure that makes possible the hyper-mobility of financial capital at the global scale is situated in various national territories. Sovereignty remains a feature of the system, but it is now located in a multiplicity of institutional arenas: the new emergent transnational private legal regimes, new supranational organizations (such as the WTO and the institutions of the European Union), and the various international human rights codes"*(Sassen 1996). The institutions that override sovereignty build upon the land and the institutions of nation-states. But Sassen's observations about the transformation, rather than the diminishment of national sovereignty only hold true because the supranational frameworks are always legitimized and authorized in one way or another by the sovereign states[6], and some key elements of sovereignty are kept intact.

[6] This is of course an oversimplified, naive interpretation: the Wikileaks cables reveal some of the coercive tactics used in international diplomacy. But even if such tactics could amount to blackmail and plain coercion, the actual supranational institutional framework is always there to mask these actions and legitimize the outcome.

Wikileaks poses a new, so far unprecedented threat to sovereignty. Its power rests on three pillars: on the immunity to intervention, on the authority its supporters vest in it, and on its ability to interfere with the internal affairs of others.

As the ineffective actions against its infrastructures have shown, Wikileaks is immune from technological, financial, infrastructural, and legal interventions. There have been several attempts to cut Wikileaks of the financial network, weaken its physical infrastructure or curtail its accessibility. None of these efforts could render Wikileaks inaccessible, and there is no sign of a more effective method to erase a service from the web other than those already used. States and governments, just like corporations, are as defenseless and exposed to Wikileakistan as much the entertainment industry is exposed to Kazaastan and Torrentia.[7] I do not wish to underestimate the intellectual power behind the Wikileaks infrastructure, but from a government perspective one of the most frightening aspects of the whole Wikileaks affair is that it is so easy to set up a network that is so difficult to take down or to engage with. At the moment it seems Wikileaks cannot be woven into the complex web of institutional inter-dependencies. *„In light of this redistribution of power, what would the solution for conventional/"atomic" power's reassertion of hegemony? This would be to contain the rise of informatic power by containing its means of distribution. This would be by the means of national firewalling, and trunk-line disconnection or limited Internet disabling, disrupting infopower, but also crippling the flow of digitized material capital as well. This is problematic at best, as conventional power and informatic power are in symbiotic, the latter being more nimble and a step ahead of the former, and to attack a symbiote always means to cripple its partner as well. The logical result of such actions would be the elimination of net neutrality (the free and open flow of data across the Internet) or even the severance of typologies and flows of information across the networks. The symbiotic effect is that conventional power/capital is also hobbled, as the physical is dependent on the same flows of information across the distributed nets, disabling itself in the process. It is for this reason that it cannot engage in this means of retaliation, as it would be the digital suicide of the First World nation-state."* (Lichty 2010) As long as Wikileaks exists on thousands of mirrors and in thousands of copies circulating on p2p networks, the debate on whether Wikileaks is a terrorist organization[8] or a group of freedom fighters, and whether such a quest for total transparency is misguided[9] or a necessary step in the development of information society remains

[7] The parallels with the p2p technology and the music industry are more than apparent. Despite the tens of thousands of legal actions against individual downloaders, technology developers, service operators, despite co-opting some ISPs, despite the immense lobbying efforts and the continuous push for more stringent regulation, the music industry could not suppress unauthorized file sharing, and eventually had to come to terms with the loss of tight market control. Only now, more than ten years after the first conflict, the industry starts to realize that file-sharing can be regarded as an asset. It can be used for market research, it is an effective distribution channel, it can be used to serve certain target groups, it can be marketed and its users can be converted to paying customers. The industry will probably never control file-sharing, but if it changes its practices, it can harness some of its resources. (Bodó 2011) I see no reason to think that the relationship of Wikileaks to states would be any different.

[8] The US Department of Defense defines terrorism as "The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological" (http://www.dtic.mil/doctrine/dod_dictionary/data/t/7591.html)

[9] We heard arguments that secrecy is a necessary component in conducting state affairs as well as international diplomacy. The state cannot and should not bear the burden of total transparency, because without some level of privacy, the state cannot fulfill its functions. Lawrence Lessig argued in the pages of The New Republic that some facts deserve privacy, because the public has a short attention span and is, in some

academic. Until the point where it can be proved that Wikileaks can be controlled – and if that happens, it ceases to exist altogether - Wikileaks is free to follow its own agenda and as a consequence is the utmost authority of the information era.

The second source of Wikileaks' power is the authority its supporters vest in it. States do not enjoy the supreme and ultimate authority over their territory anymore, because their citizens as the source of that authority now enjoy multiple citizenships -- one being that of Wikileakistan --, and have the potential to act upon multiple loyalties.[10] If citizens and corporate employees decide to break the laws of the land and follow the laws of their conscience and leak the secrets entrusted upon them to Wikileaks, it means that in the given situation they deny the supreme authority from the state and subscribe to the abstract ideals of Wikileakistan in order to preserve what loyalty they feel towards the 'nation', the 'country', the 'constitution', the 'democratic ideals' or any other notion which they think Wikileaks represents and which they hope to regain by turning to it. If Wikileaks would be Wikileakistan, another territory-bound sovereign, there would not be any problems: it could be bombarded or sanctioned into submission. But that lawless fringe, that barbaric kingdom, that pirate utopia is not somewhere else. It is exactly where we are. Confrontational, non-conciliatory action against such idealists hardly yields anything else but more disenchantment, alienation and ultimately disloyalty. By turning against such double citizens the state turns against, and ultimately eliminates itself.

Third, immunity and authority is now coupled with an unparalleled might to interfere with the internal affairs of states and corporations alike. External sovereignty is exercised *"with respect to outsiders, who may not interfere with the sovereign's governance."* (Philpott 2010) Wikileaks poses a different kind of threat to the external sovereignty than the internet, in general. (Boyle 1997) It seems possible to exercise authority with an aterritorial entity like the internet in place, but it does not seem possible to exercise *any* authority if the sovereign cannot control its internal processes, data and communication. Within the core of any sovereignty there is the ultimate capability to control the internal communications, information collection and interpretation processes. Assange describes the effects of exposing internal communications in his essay dating back to 2006: *"The more secretive or unjust an organization is, the more leaks induce fear and paranoia in its leadership and planning coterie. This must result in minimization of efficient internal communications mechanisms (an increase in cognitive "secrecy tax") and consequent system-wide cognitive decline resulting in decreased ability to hold onto power as the environment demands adaption. Hence in a world where leaking is easy, secretive or unjust systems are nonlinearly hit relative to open, just systems. Since unjust systems, by their nature induce opponents, and in many places barely have the upper hand, mass leaking leaves them exquisitely vulnerable to those who seek to replace them with more open forms of governance."*(Assange 2006)

sense ignorant, and therefore is doomed to oversimplify, misunderstand, and/or misinterpret complex phenomena, if they are simply laid bare in front of it. (Lessig 2010)

[10] It is believed that a low level US military analyst, Private Bradley Manning leaked classified information to Wikileaks. The source of this information is the log of unknown authenticity, of an online discussion, recorded and released by another whistleblower Adrian Lamo. Manning summed up his motivations in the discussion: "Manning: its sad […]i mean what if i were someone more malicious i could've sold to russia or china, and made bank?/Q: why didn't you?/Manning: because it's public data. […] it belongs in the public domain. information should be free. it belongs in the public domain. because another state would just take advantage of the information… try and get some edge. […]im not sure whether i'd be considered a type of "hacker", "cracker", "hacktivist", "leaker" or what … im just me… really." (The Guardian 2010)

The ability to place the state under surveillance limits and ultimately renders present day sovereignty obsolete.

It can also be argued that it fosters the emergence of a new sovereign in itself. I believe that Wikileaks (or rather, the logic of it) is a new sovereign in the global political / economic sphere. If everyday citizens have an autonomous zone (Bey 1991), a safe haven, hiding in the discontinuities of cyberspace, from where they can oversee and control the state apparatus; if such an organization is safe from interventions and can continuously enjoy the ethical and ideological support if its "citizens"; if the information it distributes cannot be filtered by any country, then such an organization is a new sovereign, not in cyberspace but in the real world, even though it lacks the territorial dimension.

But as it stands now, Wikileakistan shares too much with the powers it wishes to counter. As The Economist's commentator put it: *„To get at the value of WikiLeaks, I think it's important to distinguish between the government—the temporary, elected authors of national policy—and the state—the permanent bureaucratic and military apparatus superficially but not fully controlled by the reigning government. The careerists scattered about the world in America's intelligence agencies, military, and consular offices largely operate behind a veil of secrecy executing policy which is itself largely secret. American citizens mostly have no idea what they are doing, or whether what they are doing is working out well. The actually-existing structure and strategy of the American empire remains a near-total mystery to those who foot the bill and whose children fight its wars. And that is the way the elite of America's unelected permanent state, perhaps the most powerful class of people on Earth, like it."(W. 2010)* This is against what Wikileaks has risen. But the hidden power structures and the inner workings of these states within the state are exposed by another *imperium in imperio*, a secretive organization, whose agenda is far from transparent, whose members, resources are unknown, holding back an indefinite amount of information both on itself and on its opponents. The mantra of Wikileaks supporters and the mantra of state and corporate executives are shockingly identical: "We share no information on ourselves; we gather information on everyone else. Only our secrets are valid secrets." The Eye of Providence on the reverse side of the Great Seal of the United States, surrounded by the words Annuit Cœptis (He approves our undertakings), and Novus Ordo Seclorum, (New Order of the Ages) could very well be the seal of Wikileaks as well.

This leads to the question of who the parties in this conflict are. Is it the state against Wikileaks? Or maybe what we are seeing now is a battle between different secretive organizations for the control of the state and through it, the body politic? With Wikileaks the state has finally entered the Panopticon. But within, the freedom of those who are under surveillance is lost, whether they be individuals or states.

It is not more secretive, one sided transparency which will subvert and negate the control and discipline of secretive, one sided transparency, it is anonymity. The subject's position of being *"a multiplicity that can be numbered and supervised",* its state of living in a *"sequestered and observed solitude"* (Foucault 1979) can only be subverted if there is a place to hide from surveillance. There are two types of Anonymity, that of the observer, and that of the subject, both immensely empowering. The true potential of the cyberspace is not that it enables anonymous observation of the state power, but that it offers its citizens the chance to hide from observation. In other words the identity-protecting side of technology has more emancipatory power than its capability to obtain and expose secrets. Maybe less, and not more transparency is the path that leads to the aims of Wikileaks.

We have also seen how Anonymous can turn into a "stampede of coked-up lemmings". But how to be truly free in the age of ubiquitous surveillance? Is it enough if we put the observers under surveillance? Maybe we need to leave the oppositional power relationships behind, and be what Anonymous really means: invisible. Invisible in its strictest sense: being beyond the determinations that define the identity and the discourse. Because, as Pozorov (2007) so aptly said: *"freedom is not a guarantee for the fulfilment of any desire but rather the condition of possibility of its pursuit."* Wikileaks, the latest manifestation of cyberspace offers this freedom for individuals, but its proposition on how to act upon it is disturbingly similar to what it defined itself against in its Declaration of Independence. I salute Wikileaks as the first – and potentially only - truly independent sovereign of the information age. "May it be more humane and fair than the world […] governments have made before." (Barlow 1996)

References

Assange, J. (2006). "The non linear effects of leaks on unjust systems of governance." iq.org. Retrieved January 11, 2011, from http://web.archive.org/web/20071020051936/http://iq.org/#Thenonlineareffectsofleaksonunjustsystemsofgovernance.

Barlow, J. P. (1996). "A Declaration of the Independence of Cyberspace." eff.org. Retrieved January 18, 2011, from https://projects.eff.org/~barlow/Declaration-Final.html.

Bey, H. (1991). T.A.Z. : the temporary autonomous zone, ontological anarchy, poetic terrorism. Brooklyn, NY, Autonomedia.

Bodó, B. (2011). A szerzői jog kalózai. Budapest, Typotex.

Boyle, J. (1997). "Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors." University of Cincinnati Law Review **66**: 177-1411.

Chossudovsky, M. (2010). "Who is Behind Wikileaks?" Global Research. Retrieved January18, 2011, from http://www.globalresearch.ca/index.php?context=va&aid=22389.

Collins, N. (2010). "WikiLeaks: guilty parties 'should face death penalty'." The Telegraph. Retrieved January11, 2011, from http://www.telegraph.co.uk/news/worldnews/wikileaks/8172916/WikiLeaks-guilty-parties-should-face-death-penalty.html.

Curran, J. (1991). "Mass media and democracy: A reappraisal." Mass media and society: 82-117.

Der Derian, J. (2009). Virtuous war: mapping the military-industrial-media-entertainment network, Routledge.

Encyclopedia Dramatica (2011). "Anonymous." Encyclopedia Dramatica. Retrieved January 11, 2011, from http://encyclopediadramatica.com/Anonymous.

Fildes, J. (2010). "What is Wikileaks?" BBC News. Retrieved January 11, 2011, from http://www.bbc.co.uk/news/technology-10757263.

Foucault, M. (1979). Discipline and punish: the birth of the prison. New York, Vintage Books.

Foucault, M. (1981). The order of discourse. Untying the text: A post-structuralist reader. R. Young, Routledge.

Gladwell, M. (2010). Small Change. The New Yorker. New York, NY, Condé Nast. **October 4, 2010**.

Harding, L. (2010). "Julian Assange should be awarded Nobel peace prize, suggests Russia." The Guardian. Retrieved January 11, 2011, from http://www.guardian.co.uk/media/2010/dec/09/julian-assange-nobel-peace-prize.

Jordan, T. and P. Taylor (2004). Hactivism and Cyberwars - Rebels with a Cause? London, Routledge.

Lessig, L. (2010). "Against Transparency." The New Republic. Retrieved January 10, 2011, from http://www.tnr.com/article/books-and-arts/against-transparency.

Lew, J. J. (2011). Initial Assessments of Safeguarding and Counterintelligence Postures for Classified National Security Information in Automated Systems EXECUTIVE OFFICE OF THE PRESIDENT OFFICE OF MANAGEMENT AND BUDGET. Washington, DC.

Lichty, P. (2010). "Digital Anarchy and Wikileaks. (Or, Skynet doesn't look anything like we thought it did.)." Retrieved January 10, 2011, from http://patricklichty.wordpress.com/2010/12/11/digital-anarchy-and-wikileaks-or-skynet-doesn%E2%80%99t-look-anything-like-we-thought-it-did/.

Moglen, E. (2010). Freedom in the Cloud: Software Freedom, Privacy and Security for Web 2.0 and Cloud Computing. New York, NY, New York Greater Metropolitan Area chapter of the Internet Society.

Philpott, D. (2010). Sovereignty. Stanford Encyclopedia of Philosophy. E. N. Zalta.

Prozorov, S. (2007). Foucault, freedom and sovereignty. Hampshire, Ashgate.

Rosen, J. (2010). "The Afghanistan War Logs Released by Wikileaks, the World's First Stateless News Organization." pressthink. Retrieved January 11, 2011, from http://archive.pressthink.org/2010/07/26/wikileaks_afghan.html.

Sassen, S. (1996). Losing control? : sovereignty in an age of globalization. New York, Columbia University Press.

Stalder, F. (2010). "Contain this! Leaks, whistle-blowers and the networked news ecology." eurozine.com. Retrieved January 18, 2011, from http://www.eurozine.com/articles/2010-11-29-stalder-en.html.

The Guardian (2010). "Bradley Manning, in his own words: 'This belongs in the public domain'." The Guardian. Retrieved January 11, 2011, from http://www.guardian.co.uk/world/2010/dec/01/us-leaks-bradley-manning-logs.

Virilio, P. (1995). The art of the motor, Univ Of Minnesota Press.

W., W. (2010). "In defence of WikiLeaks." The Economist. Retrieved January 11, 2011, from http://www.economist.com/blogs/democracyinamerica/2010/11/overseeing_state_secrecy.

wikileaks.ch (2010). "About - 1.3 Why the media (and particularly Wiki leaks) is important." Retrieved January 14, 2011, from http://wikileaks.ch/About.html.

wikileaks.org (2008). "Wikileaks:About." Retrieved January 10, 2011, from http://web.archive.org/web/20080504122032/wikileaks.org/wiki/Wikileaks:About.