Leaking Superpower: WikiLeaks and the contradictions of democracy

Jan Nederveen Pieterse

To cite this article: Jan Nederveen Pieterse (2012) Leaking Superpower: WikiLeaks and the contradictions of democracy, Third World Quarterly, 33:10, 1909-1924, DOI: 10.1080/01436597.2012.728324

To link to this article: https://doi.org/10.1080/01436597.2012.728324

Published online: 26 Oct 2012.
Leaking Superpower: WikiLeaks and the contradictions of democracy

JAN NEDERVEEN PIETERSE

ABSTRACT While US government agencies endorse and support the democratic potential of the internet and social media overseas, the criticisms of the WikiLeaks disclosures of US diplomatic cables reveal the bias in relation to transparency and democracy. This poses a wider problem of connectivity combined with hegemony. This paper discusses what the criticisms of the WikiLeaks disclosures reveal. After discussing the enthusiasm about ‘hyper-connectivity’, the paper turns to the WikiLeaks disclosures, and next spells out global ramifications of the leaked cables, the problems of transparency and hegemony, frictions between democracy and democratisation, and the role of banks blocking donations to WikiLeaks.

In recent years the US state department has been an active proponent of open media and the internet as ways to establish or strengthen democracy. It has supported media and internet activists in the ‘colour revolutions’ in the Caucasus and the Balkans and supported and trained social media and internet activists in the Arab world, Egypt, Iran and China. During the GW Bush administration secretary of state Condoleezza Rice introduced internet techies into outreach and diplomacy in the Middle East; internet freedom was part of the Bush administration’s Freedom Agenda. This approach continued under the next administration. According to President Obama in a speech in Shanghai in 2009, ‘I think that the more freely information flows, the stronger the society becomes, because then citizens of countries around the world can hold their own governments accountable’. In January 2010 Secretary of State Hillary Clinton gave a speech on internet freedom praising the way ‘the spread of information networks is forming a new nervous system for our planet’.

Just two weeks before WikiLeaks released its diplomatic cables Alec Ross, a leading proponent of all things digital at the state department delivered an excitable speech at an internet conference in Chile. The title was the ‘battle between open and closed societies’; Mr Ross argued that openness always wins. Yet barely six minutes in he managed to infuriate his Latin American audience...
by saying that the network ‘was the Che Guevara of the 21st century’. ‘Will you try to kill it too?’ inquired someone in the audience. 

While US government agencies endorse the democratic potential of the internet and social media, the official reactions to the WikiLeaks disclosures of US diplomatic cables (Cablegate) and the criticisms in the US media reveal bias in relation to transparency and democracy. This poses the problem of hegemonic connectivity and inconsistency in relation to transparency. This paper discusses what the criticisms of the WikiLeaks disclosures reveal. The first section discusses the general enthusiasm about ‘hyper-connectivity’ and democracy, the second turns to the WikiLeaks disclosures, the third addresses the global ramifications of the leaked cables, while further sections spell out the problems of transparency and hegemony, frictions between democracy and democritisation and, finally, the role of banks blocking donations to WikiLeaks.

Hyper-connectivity

According to Thomas Friedman, with ‘cloud computing, robotics, 3G wireless connectivity, Skype, Facebook, Google, LinkedIn, Twitter, the iPad, and cheap Internet-enabled smartphones, the world has gone from connected to hyper-connected’. Hyper-connectivity and the merger of globalisation and IT enable productivity gains as well as social protests from the Arab Spring to the Israeli tent movement, flash mobs in London, and the ‘globalization of anger’. This comes with the usual Friedman hyperbole: ‘This globalization/IT revolution is also “super-empowering” individuals, enabling them to challenge hierarchies and traditional authority figures—from business to science to government’.

Hyper-connectivity intersects with many force fields: economic, political, social and cultural. One of the frontiers is ‘liberation technology’ which ranges from hacking to whistleblowing, leaking and ‘clicktivism’. From Tahrir Square to Tiananmen Square new connectivity holds democratic potential. In China Sina Weibo’s micro-blog or twitter service (launched in 2009, registered users 230 million in 2011 and rising) and the search engine Baidu’s social media service expose corrupt local bosses; the government’s attempt to use and co-opt these services comes across in this comment in China Daily: ‘public opinion pressure conveyed by weibo is helpful in cracking down on corruption and supervising the administration of local governments’. Activists in Hong Kong and China teach Chinese activists to ‘jump firewalls’ and stay a step ahead of government censorship by continually upgrading software and becoming ‘clicktivists’. In Russia phone cameras and YouTube videos revealed ballot box stuffing in the 2011 elections and sparked riots and demonstrations. A comment noted: ‘The top-down model of “political technology”, the method of managing political life in Russia, is exhausted’.

Authoritarian governments turning to the internet and social media have also become standard fare, their activities ranging from internet surveillance and censorship to cyber-attacks on websites (as in Saudi Arabia, Burma, 1910
Belorussia, Kazakhstan) and blocking access to social media or jamming airwaves (Egypt, Iran, Russia) to paying micro-bloggers to spread positive information about the government, as in China.

US government agencies, the State Department, the Pentagon and the National Endowment for Democracy endorse and seek to instrumentalise hyper-connectivity and co-opt it in the arena of cyber-politics or ‘internet statecraft’. The combination of hyper-connectivity and hegemony produces new frontiers of power and emancipation, with US government agencies engaged in defensive and offensive cyber-war efforts and cyber-garments as the hegemon’s new clothes. In 2011 the USA designated cyberspace the fifth military domain, along with land, sea, air and space. The US deployment of the Stuxnet virus targeting Natanz, Iran’s uranium enrichment facility has been as ominous as the Flame computer malware virus that has been wreaking havoc in the Middle East.

In response to efforts to control information flows in Iran, North Korea, Egypt, Syria, Libya, Sudan, Saudi Arabia and other countries, the US State Department finances the creation of stealth wireless networks that would enable activists to communicate outside the reach of governments. By the end of 2011 it had spent some $70 million on circumvention efforts and related technologies, including ‘shadow’ internet and mobile phone systems that dissidents can use to undermine repressive governments; use of ‘mesh network’ technology that can transform devices like mobile phones or personal computers to create an invisible wireless web without a centralised hub; the ‘Internet in a suitcase’ project of the Open Technology Initiative at the New America Foundation; use of Bluetooth to beam information directly from one cell phone to another; the Palisades project, a $50 million collaboration of the Pentagon and State Department to build a ‘shadow’ mobile phone system in Afghanistan, where repressive forces (read: Taliban) exert control over the official network, relying in part on cell towers placed on protected US bases, with Kandahar airbase as a data collection point; and burying Chinese cell phones ‘on hillsides for people to dig up at night’ in Dandong and the surrounding Jilin Province, as ‘natural gathering points for cross-border cellphone communication and for meeting sources’ for use in North Korea and able to pick up signals from towers in China. This involves combinations of technology that the USA is developing and tools ‘created by hackers in a so-called liberation-technology movement sweeping the globe’.

WikiLeaks and Cablegate

In November 2010 WikiLeaks began publishing leaked US embassy cables totalling 251,287 documents dating from 1966 to the end of February 2010 and containing confidential communications between 274 embassies in countries throughout the world and the State Department in Washington, DC. Over 15,000 were classified secret and over 100,000 were confidential. In the words of WikiLeaks they represent ‘the largest set of confidential documents ever released into the public domain’. Major newspapers in five countries (the Guardian, New York Times, Le Monde, El Pais and Der
Spiegel), as well as media in countries outside the West, cooperated by releasing selected and redacted documents from the WikiLeaks cables.\textsuperscript{14} Washington’s initial official response to the disclosures was that they were a major breach of security and classified information. The rules of openness did not apply in this case, according to the secretary of state, because the information was ‘stolen’. In the second round, once the material had circulated widely and in major newspapers, the response in official and establishment circles was to poo-pooh and trivialise the disclosures as minor and unimportant, nothing new. They show, according to op-ed columnists, that American diplomats hold realistic assessments of conditions abroad, that they write well, and so forth. Many American responses, also in some left leaning media, have been either hostile or dismissive. Thus, according to Christian Caryl in the \textit{New York Review of Books}, the disclosures seem ‘to boil down to a policy of disclosure for disclosure’s sake…I don’t see coherently articulated morality, or immorality, at work here at all; what I see is an amoral, technocratic void’.\textsuperscript{15} According to Slavoj Žižek,

The only surprising thing about the WikiLeaks revelations is that they contain no surprises. Didn’t we learn exactly what we expected to learn? The real disturbance was at the level of appearances: we can no longer pretend we don’t know what everyone knows we know. This is the paradox of public space: even if everyone knows an unpleasant fact, saying it in public changes everything…Truth liberates, yes, but not \textit{this} truth. Of course one cannot trust the façade, the official documents, but neither do we find truth in the gossip shared behind that façade.\textsuperscript{16}

The disclosure of US diplomatic cables exposes contradictions at the new frontiers of information. In mainstream media, particularly in the USA, the responses to the WikiLeaks disclosures ranged from trivialisation to indignation—decrying them as vandalism or as acts of cyber-terrorism. These responses both reveal and paper over deeper contradictions. In the words of Alan Rusbridger, editor of the \textit{Guardian}, ‘It was astonishing to sit in London reading of reasonably mainstream American figures calling for the assassination of Assange for what he had unleashed. It was surprising to see the widespread reluctance among American journalists to support the general ideal and work of WikiLeaks.’\textsuperscript{17} Indeed, there is an astonishing gap between cyber-boosterism and hyperbolic enthusiasm for new technologies such as social media (as in notions of a ‘Facebook revolution’, etc) and the lack of enthusiasm when such media are being aimed at the USA, as in the case of WikiLeaks. Exposing politically correct targets—such as Iran, China, Syria—is held to an entirely different standard than exposing the hegemon.

US agencies routinely tap internet and mobile phone networks across the world for intelligence gathering and to stealthily obtain biometric information on UN diplomats (as WikiLeaks reveals) and thus steal information. The difference is that WikiLeaks is a non-state actor and the information is released into the public domain; the former is deemed theft, the latter vandalism.

Part of hyper-connectivity is the desegregation of audiences (cartoons satirising Islam intended for a Danish public reach Riyadh and Istanbul,
radio conversation in Berlin echoes in Islamabad, etc). Following the intelligence failures of 9/11 the US government desegregated information circuits and merged defence, diplomatic and intelligence information pools, which enabled defence personnel to access embassy cables and, allegedly, pass them on to WikiLeaks. So US government actions made the WikiLeaks disclosures possible. The root tension between hyper-connectivity and hegemony is that hyper-connectivity is multidirectional and cannot easily be harnessed, dictated or controlled.

As several discussions point out, at issue are questions of whistleblowing and civil disobedience. Viewing WikiLeaks disclosures as acts of civil disobedience is appropriate, but first poses the problem of obedience: the culture of conformity that is deeply ingrained in mainstream media. ‘Journalism these days amounts to little more than outsourced PR remixing’, notes Geert Lovink. Commentators fall over the messenger and gloss over the message. This presents several options: US war crimes (killings of civilians and their cover-up in Iraq and Afghanistan) are taken for granted—hence disclosing them is trivial. Or the disclosures are inopportune—which implies that the public is assumed to be complicit with impunity—or are taken as a breach of trust—which implies that impunity is the standard and its breach is more important than the actual information disclosed.

By any account the mainstream media responses are both revealing and deeply troubling. What are at issue are the political culture and the politics of impunity. Because it involves mainstream media and appeals to public sensibilities this double standard may be termed hegemonic populism. The notion that the cables contain ‘no surprises’ is beside the point; the point is that they confirm and document hegemonic operations, political complicity and war crimes, so their status changes from allegation and hearsay to actionable offences or, at a minimum, information that carries political consequences. It stands to reason that the political ripple effects are greater and weightier in the target zones of hegemony than on the home front where institutions act as buffers and a jaded public has been inured to impunity.

Global ramifications

Outside the West, in countries such as in Tunisia, Libya, the Arab world, Pakistan, India, Haiti, Thailand, Nigeria and Zimbabwe, the disclosures democratise access to information, undermine the legitimacy of rulers and hold significant political ramifications. This has barely been touched on in Western media and perspectives. The cables expose the complicity of governments and rulers in American schemes, notably in the Arab world, to a degree that, as Philip Stephens notes, is ‘startling’. In Tunisia WikiLeaks disclosures contributed to the ‘Jasmine Revolution’: “‘There were a lot of specific details in the cables that the public had not been exposed to before the release. There is no question that WikiLeaks added substantial evidence to the story that people already knew,” said Shibley Telhami. This is a recurrent theme:
The constant connections made between WikiLeaks and the Tunisian uprising are not just a coincidence. Barka, a prominent member of a Tunisian association for female equality, told us that ‘the WikiLeaks revelations circulated very well in Tunisia in January [2011]’. She also confirmed that local newspapers were publishing Cablegate analysis at the beginning of the year, prior to the revolution. She considers that the airing of the material on the mainstream media, revealing just how rotten Ben Ali’s crony-capitalist system was, played a significant role in politically engaging the youth of the country.23

In Libya Gaddafi railed against WikiLeaks and blamed the Tunisian uprising on it: ‘Qaddafi claims cables leaked by WikiLeaks detailing the spending habits of Ben Ali and his family were planted by ambassadors to push along the Tunisian uprising.’24 There are clear connections, then, between WikiLeaks and Tunisia’s ‘Dignity Revolution’ that sparked the Arab Spring, which, in turn, influenced Occupy Wall Street and other social movements. Thus WikiLeaks is a significant link in the chain of events that sparked a ‘new culture of popular resistance’25 and turned 2011 into a year of popular uprisings from the Arab world to the West and everywhere else.

The country most discussed in the cables is Iraq (with 15,365 documents). In Iraq WikiLeaks information on US armed forces killing civilians and seeking to cover up the deaths has seriously undermined the legitimacy of the US military presence. It has been a contributing factor in the Iraqi government’s decision not to grant permission for an extended stay to the US military. Thus the disclosures contributed to the effective end of the Iraq war by the end of 2011.

According to Chomsky, the ‘WikiLeaks cables reveal a profound hatred for democracy on the part of our political leadership’.26 Cables from the Arab world reported (and filtered) Arab leaders’ view that the major threat in the region was Iran and its potential nuclear capabilities—in stark contrast to views of the Arab population, 80% of whom see Israel and the USA as the main threats to peace and stability, as many opinion polls show. But this the cables don’t report. With regard to Israel’s siege of Gaza the cables show bias of the usual kind, in sync with general American media narratives, again disregarding the views of the Arab population.

The incursions of the US military into Pakistan’s autonomous regions (usually called ‘tribal areas’ in Western media) in pursuit of al-Qaeda and Afghan Taliban, and its drone attacks killing civilians have been condemned time and again by the Pakistani government—just as in Afghanistan the Karzai government continues to condemn similar bombings, night raids and attacks killing civilians. In Pakistan many tacitly assume the government condemnations of US incursions are perfunctory and, in fact, the attacks are being carried out with government sanction—which cannot be conceded publicly. WikiLeaks disclosures of diplomatic cables have confirmed this complicity. This has played into the hands of pro-Islamist forces, reinforcing their anti-government campaigns. The rationale is: if you hit us in the autonomous regions, we will hit you in Islamabad, Lahore and Karachi. It has generally reinforced already high anti-American sentiment in Pakistan. It
also strengthens Pakistan’s democratic forces, who seek futures that are
dominated neither by an overseas superpower nor by Islamist extremists.

A similar equation applies in Yemen: ‘The government of Yemen is happy
to see Washington use its drones to bomb al-Qaeda insurgents in the country.
On the other hand, the US must hold firmly to the public fiction that the
attacks are carried out by Yemeni forces’.27 Here the disclosures added to the
slipping of the Saleh government’s hold.

In India the Hindu newspaper accessed over 5000 diplomatic cables
through an arrangement with WikiLeaks and their disclosure created a major
uproar. They show that the ruling Congress Party had access to over US$1
million in funds to bribe MPs in order to survive the crucial confidence vote
over the US–India nuclear deal in July 2008.28 They also indicate that
Indians have the largest amount of black money in Swiss banks, which
confirms the momentous scope of India’s underground economy.29

WikiLeaks released several names of Indians with deposits in Swiss account
and threatens to release more unless the Indian government takes action.

In Thailand the disclosures have had a special impact because they reveal
the reflections of outside observers, ie US ambassadors, who were not con-
strained by the lèse majesté law that keeps Thailand’s ‘network monarchy’
outside public view and accountability. Thus a major power centre, hitherto
sheltered by an antiquarian law, suddenly stands exposed. In addition, they
concern a period of unprecedented violence and upheaval from 2009 to 2011,
including the clashes between the pro-monarchy ‘yellow shirts’ and the
opposing ‘red shirts’.30 Adherents of the erstwhile government cast the dis-
closures—spread on the internet 10 days before the elections of July 2011—as
part of a conspiracy to overthrow the Thai establishment and monarchy,
igniting forces similar to those of the Arab Spring and playing into the hands
of the Pheu Thai party led by Thaksin Shinawatra’s sister, which achieved a
landslide election victory on 3 July. According to a conservative pro-
monarchy commentator, ‘The timing of the leak was carefully orchestrated
with other events to show the world that Thailand is a backward country
ruled by an elite class that has no respect for freedom and democracy’.31 Here
the disclosures punctured the hold of the Thai monarchy.

In Zimbabwe the cables disclosed not only widespread disaffection with the
rule of Robert Mugabe, which is well known, but also major rifts within the
ruling Zanu PF party and government. In Suriname American diplomatic
cables of 2006 document in detail the close involvement of Desi Bouterse with
the Latin American cocaine trade as recently as five years ago. Released by
WikiLeaks in 2011, the cables caused political embarrassment in Paramaribo,
where Bouterse is now president.32

In Haiti, according to the Nation, a US paper, the disclosed cables covering
almost seven years, from 2003 to 2010, show ‘Washington’s obsession with
keeping Aristide out of Haiti and the hemisphere; the microscope it trained
on rebellious neighborhoods like Bel Air and Cité Soleil; and its tight
supervision of Haiti’s police and of the United Nations’ 9000-person military
occupation known as the UN Stabilization Mission in Haiti. . .What emerges
is an extraordinary portrait of Washington’s aggressive management of Latin
Part of WikiLeaks’ agenda to promote transparency in government is cooperation with media outlets in developing countries—more than 50 such cooperation agreements exist to date—and providing them with US Embassy materials relevant to the country. The disclosures provide evidence and documentation of what was previously only assumption and hearsay, which holds political as well as possible legal implications. While developing countries are part of the arena in which WikiLeaks operates, most Western reactions and criticisms only consider their ramifications in the West.

**Transparency and hegemony**

How then do we read the new frontiers of asymmetric information warfare? According to a former CIA agent, ‘while the drift of much of the ensuing commentary has been that there is not much new in the 250 000 leaked cables, the truth is that the damage to American credibility and diplomacy is incalculable. Amid all the WikiLeaks’ admirers’ trumpeting of the virtues of transparency, we risk forgetting the worth of diplomatic “back channels”—a strictly private way of communicating with the president of the United States’.35

Foreign affairs has traditionally been a preserve of elites. During past decades this monopoly has been broken by the large-scale entry of non-state actors such as NGOs, trade unions and people-to-people networks. In international relations this has given rise to the term ‘postinternational politics’. Social media and WikiLeaks are part of this cross-border communications field, just like Médecins Sans Frontières, Amnesty International and Human Rights Watch. Complaints of NGO interference by the monopoly holders have gradually died down; similarly, WikiLeaks will become part of the landscape. In time the complaints of the old information monopolists will become routine and boring. The major international NGOs, if they are service-delivery organisations, usually take a step back from overt political criticism and involvement and, if they are transnational advocacy NGOs (TANGOs), they may refrain from criticising donor countries. WikiLeaks differs from the major international NGOs by its counter-hegemonic approach.

The setting of this discussion is the information arena, the framing of narratives and ‘hearts and minds’ support. At issue are diverse readings of transparency, openness and democracy. Some US government agencies have embraced openness and adopt an agenda similar to that of George Soros’ Open Society Foundation. To some extent the premise is, if you can’t beat them, join them. Be on the side of Google, Facebook, Twitter, Apple and social media technologies. This is in line with general American and US government innovation rhetoric, and with the views of technologically progressive forces in Silicon Valley, Wall Street and Hollywood, many of which support the Democratic Party and the Obama administration. It also ties in with the long record of US agencies, such as the bipartisan National Endowment for Democracy (NED), in support of democracy and human
rights. Hence the use of cyber-technology is ‘a new front in a longstanding diplomatic push to defend free speech and nurture democracy. For decades, the United States has sent radio broadcasts into autocratic countries through Voice of America and other means. More recently, Washington has supported the development of software that preserves the anonymity of users in places like China, and training for citizens who want to pass information along the government-owned Internet without getting caught’.38

WikiLeaks exposes the tensions between democratic and hegemonic transparency. Hegemonic transparency is top-down transparency, transparency for ‘others’, a panopticon world, as in authoritarian rule and in Orwell’s 1984. Totalitarian governments such as the Soviet regime pursued the fiction of a transparent, legible society that, by being illuminated through intelligence monitoring, becomes opaque to itself.39 Contemporary surveillance technologies seem to bring this closer. Corporations and banks gather personal information on consumer and credit behaviour for the purposes of marketing, managing risk and ‘social sorting’. These surveillance techniques, as David Lyon points out, are reductionist, control-oriented, undemocratic, one-way, not relational and without reciprocity. They produce digital discrimination, operating in advance, in which surveillance leads to social sorting.40

The rules of one-way transparency also apply to international institutions. The IMF and World Bank demand openness of the books of Mexico, Indonesia, Greece, or whichever state seeks financial support, but do not open their own books and do not disclose which programmes and projects are funded and for what reasons. ‘Good governance’ as the yardstick and aid conditionality, upheld by Western institutions since the 1990s, hold a similar implication in that governance and human rights in the USA, other Western countries and international institutions are not in question. ‘Crony capitalism’ is supposed to be practised overseas (which is belied, of course, by the Enron series of corporate scandals, the subprime mortgage collapse and subsequent banking crises in the USA and elsewhere). Double-speak and double standards are intrinsic features of hegemonic transparency.

WikiLeaks upsets the etiquette of hegemonic transparency and poses the option of radical transparency. ‘In the networked age, when the watched can also be watchers, nothing less than the credibility of authority itself is at stake…In this changed environment, the people formerly known as authorities can re-earn that trust only by being more transparent, and by eliminating the contradictions between what they say and what they do’.41

One problem is policy incoherence—colluding with autocratic governments in one sphere while undercutting them in another. Thus, ‘the United States could expose itself to charges of hypocrisy if the State Department maintained its support, tacit or otherwise, for autocratic governments running countries like Saudi Arabia or Bahrain while deploying technology that was likely to undermine them’.42 States are complex institutions; multi-channel politics is as common as hedging your bets, just as major political campaign funders will fund both the incumbent and the opposition. No doubt this is generally a willed, deliberate incoherence. Yet implementing it requires a degree of discretion. WikiLeaks poses the problem not of back
channels (which are always available) but of embarrassment and trespassing on the fine art of double dealing.

According to Julian Assange, ‘It is not our goal to achieve a more transparent society; it’s our goal to achieve a more just society’. Assange’s approach is based on the view that ‘authoritarian power is maintained by conspiracy’, as discussed in his essays on ‘Conspiracy as governance’:

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...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.

Forcing authoritarian institutions to greater secrecy, to shelter against leaking, would render them more opaque unto themselves and less effective in dealing with the changing environment. ‘An authoritarian conspiracy that can not think efficiently, cannot act to preserve itself against the opponents it induces’. In part this sounds like an endorsement of Popper’s open society (which inspires the Open Society Foundation) and parallels general arguments in favour of information circulation (as in knowledge economy and management literature) and in part it gives a limited, simplistic account of government institutions. First, it does not take into account the divisions within government—for instance, the State Department’s endorsement of openness isn’t shared by the Pentagon and intelligence agencies. The classification levels of government information (confidential, classified, secret, top secret) already indicate insulated information circuits. Second, when it comes to covert operations and war theatres, the outer circles of government do not necessarily know the rationales and agenda of inner circles, as in the Iraq war. Third, secrecy as a mode of operation of authoritarian institutions may be operationally effective, up to a point, but is ineffective in terms of legitimacy, so these operations are inherently contradictory. While the State Department supported openness of information in the ‘colour revolutions’ in Eastern Europe, the CIA and the Pentagon engaged in secret renditions, sending terrorism suspects to Eastern Europe, the Arab world and other locations for interrogation and torture. The openness endorsed by the State Department also led to disclosures of American covert operations, as in the Arab Spring and Libya after the fall of Gaddafi. For several reasons, then, more secrecy and the ring fencing of information to guard against leaks would probably have little or no effect.

This discussion leaves aside the question of transparency in WikiLeaks itself. WikiLeaks as an organisation and Julian Assange as a key figure have been criticised for various reasons. Some criticisms may reflect disinformation and a smear campaign against Assange; some may reflect faulty judgment on the part of an organisation under pressure, a small
organisation that handles large concerns and data flows. According to Geert Lovink, WikiLeaks is an organisation shaped by 1980s hacker culture and by the political values of 1990s techno-libertarianism; it has been criticised for being ‘a typical SPO [Single Person Organisation]’, for lack of transparency in its funding and for ‘secrecy in this way of making-things-public’. Organisational problems have given rise to alternative channels such as OpenLeaks, founded by WikiLeaks dissident Daniel Domscheit-Berg.

In this discussion the issue isn’t WikiLeaks as an organisation per se but WikiLeaks as part of 21st century techno-politics, which reflects, informs and enables a new wave and new culture of popular awareness and emancipation. It belongs alongside websites and list serves such as Move On, Truth Out, AlterNet, Open Democracy, Huffington Post, Tuenti (Spain), QQ (China) and Naver (Korea), but, from the outset, with the specific function of enabling leaking. WikiLeaks is a non-American internet project, led by an Australian, which primarily operates from Europe. WikiLeaks belongs in a different category from hacker websites such as Anonymous, LulzSec and the Chaos Computer Club. It represents the shift from hacking to leaking, or facilitating ‘insiders from large organizations to copy sensitive, confidential data and pass it on to the public domain while remaining anonymous’.

**Democracy and democratisation**

Is democracy merely a noun or is it also a verb, democratisation? While democracy is a particular institutional framework, democratisation is an ongoing process which assumes that democracy is always ‘unfinished’, open-ended and up for maintenance or repair. While WikiLeaks poses dilemmas for democracy it provides openings for democratisation.

In the 1980s the USA supported showcase or ‘demonstration elections’ from El Salvador to the Philippines. Upon the end of the Cold War this approach evolved to the promotion of liberal democracy (the keynote of Fukuyama’s ‘End of History’). This particular institutional framework of democracy is, in Colin Crouch’s words, ‘a form that stresses electoral participation as the main type of mass participation, extensive freedom for lobbying activities, which mainly means business lobbies, and a form of polity that avoids interfering with a capitalist economy. It is a form that has little interest in widespread citizen involvement or the role of organizations outside the business sector’. I think this characterisation overlooks human rights activism (although it often enters the public sphere as a tool of political conformity); but the larger issue is that it is part of a wider condition in Western democracies. Crouch characterises this phase as post-democracy:

Under this model, while elections certainly exist and can change governments, public electoral debate is a tightly controlled spectacle, managed by rival teams of professionals expert in the techniques of persuasion, and considering a small range of issues selected by these teams...Behind this spectacle of the electoral game, politics is really shaped in private by interaction between elected governments and elites that overwhelmingly represent business interests.
Structural trends that underlie the phase of post-democracy are the rise of global firms, post-industrialism and the erosion of the working class and trade unions, and the institutionalisation of techniques of democracy. Under the rules and etiquette of post-democracy hyper-connectivity and cyber activism are supposed to function within limited bounds—they are to serve social interaction, personal fulfilment and entertainment needs. By using them to expose elite machinations and elite reflexivity, WikiLeaks and other digital media upset the traffic rules of liberal democracy and contribute to deliberative democracy or radical democratisation. The WikiLeaks disclosures reopen and reinvigorate the public sphere as a sphere of democratisation.

One of the dilemmas this poses is the possibility of harm. Whistleblowing and radical transparency may unwittingly expose third parties to danger. Establishment sources present the possibility of harm (to named sources or informants) as the major threat the disclosed materials pose. ‘Damage of various kinds is sure to result’. Across a wide spectrum and certainly in right-of-centre views this is invariably the leading argument against unauthorised disclosures. In relation to a batch of unredacted disclosures in September 2011, newspaper headlines declared that ‘deaths are feared because of WikiLeaks disclosures’. However, so far no significant case of such harm has come to light. But more importantly, while the disclosures are deemed reckless, irresponsible and dangerous, the danger and recklessness of the actions of the US government and its allies, and the death toll and collateral damage of military operations remain out of view. The former is regarded as a major and possibly treasonous breach while the latter is taken as a routine by-product of war. In US wars in Afghanistan, Iraq, Pakistan and the ‘war on terror’ tens of thousands have been killed or assassinated, millions displaced and countries ravaged, but this is not part of polite conversation. US agencies duly promoting democracy overseas at a time when democracy in the USA is in a state of profound gridlock (as in the federal debt ceiling and budget debates) adds to the ironies and perplexities of the moment.

Banks and democracy

In December 2010 Visa, MasterCard, PayPal, Western Union and Bank of America cut off donations funding WikiLeaks. These include three of the world’s biggest payment providers. Ten months later Julian Assange announced that WikiLeaks would suspend operations until the blockade was lifted and warned that the site does not have the money to continue into 2012. The banks’ blockade was encouraged by several US senators, including Joe Lieberman. Several institutions such as the UN High Commissioner for Human Rights criticised the move. According to James Ball, ‘Whether you support WikiLeaks or not, the blockade by Visa, MasterCard, PayPal and others is a sinister attack on free speech’:

The banking blockade against WikiLeaks is one of the most sinister developments in recent years, and perhaps the most extreme example in a
western democracy of extrajudicial actions aimed at stifling free speech—made all
the worse by the public support of numerous people sitting in the US like many
of the country’s leading corporations, WikiLeaks has neither been charged with,
nor convicted of, any crime at either state, federal, or international level. If they
are allowed to cut off payment to lawful organisations with whom they disagree,
the US’s first amendment, the European convention on human rights’ article 10,
and all other legal free speech protections become irrelevant.53

The reality of the ‘free market’ is control by giant corporations. The US
Congress gives corporate oligopolies a free reign as part of a network of
lobbies, interest groups and media that has been referred to as ‘Permanent
Washington’ and a constellation that Crouch refers to as ‘post-democracy’.54
James Ball’s comments appear in the Guardian, which has long cooperated
with WikiLeaks, without withholding criticism of Assange or of WikiLeaks.
In contrast, the US media have reported the payments blockade but refrained
from critical editorial comments. The New York Times media columnist,
David Carr, notes the payments blockade to WikiLeaks but only mentions
‘the legal and social strictures against making the private public’, echoing the
State Department’s criticisms.55 In other words, Washington’s reservations
come up but the ethical and legal problems that the banks’ blockade poses do
not. This illustrates a culture of compliance and conformity that is routine in
the USA, to the point that one hardly notices it.

The payments blockade is noteworthy at a time when banks have led the
US and the world economies into crisis, essentially because of deregulation
and lack of accountability and transparency, condoned and institutionalised
by US lawmakers. Banks then return the favour by blocking transparency
and accountability in US government operations, confirming the impression
that ‘banking is politics by other means’.56 At a time when major banks—in
particular the six remaining US megabanks—contribute to rising wealth
inequality and manipulate the institutions of democracy, Congress included,
their blocking informal democratic networks comes across as part of the
same parcel.

According to WikiLeaks’s website on the banks’ blockade, the Bank of
America, one of the principle promoters of the blockade and the creator of
Visa, commissioned three US intelligence contractors to propose a systematic
attack to hack and smear WikiLeaks, which would also target journalists and
lawyers supporting it.57 The approach outlined matches a classic format of
US intelligence campaigns, such as those against Muslim fundamentalists in
the Arab world: spread disinformation to sow dissent between hardliners and
moderates.58 The allegation, if true, points to a further level of collusion
between the US government and banks than hitherto assumed.

In June 2012 Assange sought asylum at the Ecuadorian Embassy in London,
a request that was accepted by Ecuador. The UK government however
continues to insist on his extradition to Sweden and refuses to grant him free
passage. In Sweden Assange is accused of rape, but the treatment of his case is
quite different from the way other accusations of rape are dealt with. ‘The
politicisation of the Swedish case was clear from the initial leak of the allegations
to the prosecutor’s decision to seek Assange’s extradition for questioning –
described by a former Stockholm prosecutor as “unreasonable, unfair and disproportionate” – when the authorities have been happy to interview suspects abroad in more serious cases’. In a nutshell: ‘WikiLeaks provided fuel for the Arab uprisings. It didn’t just deliver information for citizens to hold governments everywhere to account, but crucially opened up the exercise of US global power to democratic scrutiny.’

In August Assange assigned the Spanish judge Garzón, with a formidable record, to defend him.

Conclusion

In conclusion we can distinguish between WikiLeaks’ disclosures and the reception of its actions. The disclosures, even if they trespass on the traffic rules of liberal democracy, without a doubt contribute to democratisation. The reception of WikiLeaks’ disclosures casts light on the non-democratic character of the dominant institutions, public and private, ensconced in the niches of institutional democracy.

Over recent decades globalisation and financialisation have led to a major hiatus of regulation and to a global governance gap. While digital technologies are part of the package deal of contemporary globalisation and part of the technological changes that enable or facilitate global finance, offshoring and outsourcing, they also provide opportunities for communication and resources for deliberative democracy, some of which were undreamt of until recently. Organisations such as WikiLeaks and movements from the Arab Spring to Occupy Wall Street and frustrated voters in Russia show other faces of the digital turn. They help expose authoritarian rule as well as the bounds of liberal democracy and do so at a time when the institutions of liberal democracy are proving to be inadequate to the challenges of globalisation and financialisation. They point to a new sphere of contestation between authoritarian institutions, public and private, and social forces that can no longer be contained within the existing institutional frameworks. Nor can they be contained in new market equations such as the knowledge economy. They contribute to new emerging equations of emancipation that will not be easily contained or co-opted. They are expressions of emancipatory cosmopolitanism.

Notes

With thanks to René Gabriels and Geert Lovink for comments on an earlier version.

9 M Glenny, ‘We will rue the cavalier deployment of Stuxnet’, Financial Times, 7 June 2012, p 9.
WIKILEAKS AND THE CONTRADICTIONS OF DEMOCRACY

10 This draws on J Glanz & J Markoff, ‘US underwrites internet detour around censors’, New York Times, 12 June 2011. Financed with a $2 million State Department grant, the suitcase could be secreted across a border and quickly set up to allow wireless communication over a wide area with a link to the global internet, and would include small wireless antennas; a laptop to administer the system; thumb drives and CDs to spread the software to more devices and encrypt the communications.

11 This project would modify Bluetooth so a file containing, say, a video of a protester being beaten could automatically jump from phone to phone within a ‘trusted network’ of citizens, a system that would only require software modification on ordinary phones.

12 Glanz & Markoff, ‘US underwrites internet detour around censors’.

13 The cables can be explored and browsed according to various search criteria (by country, date, tag, etc) at http://www.cablegateresearch.net. See also http://www.cabledrum.net/.

14 ‘WikiLeaks turned over all of the classified US State Department cables it obtained to Le Monde, El Pais in Spain, The Guardian in Britain and Der Spiegel in Germany. The Guardian shared the material with The New York Times, and the five news organizations have worked together to plan the timing of their reports. They also have been advising WikiLeaks on which documents to release and what redactions to make to those files’. J Keaten & BJ Blackledge, ‘WikiLeaks, 5 major newspapers collaborate’, Associated Press, 3 December 2010.


27 Stephens, ‘A history of the present in 250 000 cables’.


31 T Khantong, ‘More confrontation is inevitable’, The Nation (Bangkok), 1 July 2011, p 14A.


34 Ibid.


38 Glanz & Markoff, ‘US underwrites internet detour around censors’.


41 Sifry, WikiLeaks and the Age of Transparency, p 18.

1923
42 In Glanz & Markoff, ‘US underwrites internet detour around censors’.
47 For example, H Brooke, The Revolution will be Digitised: Dispatches from the Information War, London: Heinemann, 2011; and Lovink, ‘Techno-politics at WikiLeaks’.
51 Caryl, 2011.
52 Also in relation to national security, for according to the lawyer representing US Army Private Bradley Manning in a court filing, the information in question did not do ‘any real damage to national security’. L Shaughnessy, ‘Lawyer: WikiLeaks cables did little harm’, at CNN.com Blogs, 29 November 2011.
57 The sabotage plans include: ‘Feed the fuel between the feuding groups. Create messages around actions of sabotage or discredit the opposing organizations. Submit fake documents and then call out the error. Create concern over the security of the infrastructure. Create exposure stories. If the process is believed not to be secure they are done. Cyber attacks against the infrastructure to get data on document submitters. This would kill the project. Since the servers are now in Sweden and France put a team together to get access is more straightforward. Media campaign to push the radical and reckless nature of WikiLeaks activities. Sustain pressure. Does nothing for the fanatics, but creates concern and doubt among moderates.’ See wikileaks.org/Banking-Blockade.html. The intelligence firm HBGary, which is involved in operations against hackers, is among the agencies allegedly recruited by Bank of America. Menn, ‘The scary face of hacktivism’.Cached
58 For example, see C Benard, Civil Democratic Islam: Partners, Resources, and Strategies, Santa Monica, CA: Rand Corporation, 2003.

Note on contributor

Jan Nederveen Pieterse is Mellichamp Professor of Global Studies and Sociology, University of California, Santa Barbara and specialises in globalisation, development studies and cultural studies. His current focus is on 21st century globalisation. He has held previous posts in the USA, Africa and Europe and is Honorary Professor of Globalisation at Maastricht University. He is the author/editor of 21 books, including Globalization and Culture: Global Mélange (second edn, 2010); Development Theory: Deconstructions/Reconstructions (second edn, 2010); Beyond the American Bubble: Is there Hope for Uncle Sam? (2008); and Ethnicities and Global Multiculture (2007).