Notes

[1] www.theatlantic.com/technology/archive/2010/12/steve-wozniak-to-the-fcc-keep-the-internet-free/68294/.

[2] Except for John Naughton in the *Guardian*: 'the first really sustained confrontation between the established order and the culture of the internet. There have been skirmishes before, but this is the real thing.' See www.guardian.co.uk/commentisfree/cifamerica/2010/dec/06/western-democracies-must-live-with-leaks.

[3] Johan Söderberg, *Hacking Capitalism: The Free and Open Source Software (FOSS) Movement*, Routledge, London, 2007; emphasis added.

[4] See http://en.wikipedia.org/wiki/LOIC.

[5] Thomas Apperley, *Play and Counterplay from the Situated to the Global*, Institute of Network Cultures, Amsterdam, 2010.

[6] Sean Cubitt, 'Digital Aesthetics', *Theory, Culture & Society*, SAGE, London, 1998, p. 142.

[7] *Le Monde*'s article on Julian Assange as 'Man of the Year 2010': www.lemonde.fr/documents-wikileaks/article/2010/12/24/julian-assange-homme-de-l-annee-pour-le-monde_1456426_1446239.html.

[8] Laura DeNardis, *Protocol Politics: The Globalization of Internet Governance*, MIT Press, Cambridge MA, 2009.

[9] See www.isoc.org and www.unpan.org.

[10] Douglas Rushkoff, *The Next Net*, 2011, www.shareable.net/blog/the-next-net.

Keyspace

WikiLeaks and the Assange papers

Finn Brunton

Years ago, Julian Assange considered solutions for an unusual problem, the kind of thing cryptographers discuss: how can you make sure a message only becomes readable at a certain time, not before, such that no human frailty or mechanical error interferes with the schedule? He came up with three answers, which display his knack for odd lateral thinking, an unremarked gift that turns up throughout his work. One solution: encrypt the message, and then broadcast the key to the code out into space, to 'distant astral bodies', as he puts it, and wait for it to be bounced back. You can publicize the body, the distance, the coordinates; the satellite dishes of Earth will be oriented at that hour of that day to pick up the bounce and your message will be read. Another solution is quite baroque, with space probes passing a key stream between them, 'using space as the storage medium', before sending decrypts back to Earth. The last is by far the most elegant solution, the most difficult to realize, and in some ways the cruellest. 'If you can predict the future cost/CPU speed then you can create a problem which can't be solved with current technology at a reasonable price. The future isn't predictable enough to do this over the longer term.'[1] You can embed the solution in the future, sealed against every human force but the curve of increasing processing power – the present can only build, and speculate.

What Assange and his colleagues have built, what WikiLeaks embodies, is a kind of photographic negative of this last project: current technology has created a set of profound opportunities – and problems for the existing order – waiting for the arrival of human arrangements capable of making use of them. WikiLeaks is a preliminary solution, an initial sketch of a world in which the potential within these technologies has been unlocked. In cryptography, 'keyspace' is the realm of possible solutions for the keys to an encrypted message. If we can construe the problem, the question, of how we are to use these machines and algorithms we have built, WikiLeaks is a narrowing of the keyspace, clarifying some borders, edges and areas of possibility.

It is far from the only solution. WikiLeaks is more a model than it is some irreplaceable object. There are already diverging approaches. Birgitta Jónsdóttir, who was one of the crucial facilitators of the release of the 'Collateral Murder' video, has expressed concern with the emphasis on 'megaleaks': leaking as a high-visibility international media event, as opposed to the targeted release of information to relevant activist campaigns and organizations best positioned to make use of it.[2] A related critique has lead to OpenLeaks, run by an ex-WikiLeaker, Daniel Domscheit-Berg, which separates the submission of documents from their publication, providing secure drop boxes for anonymous submissions to websites, so any group can have their own channel for leaking. Country- and region-specific WikiLeaks-inspired organizations are proliferating: IndoLeaks (for Indonesia), BrusselsLeaks (the EU), Rospil (Russia), ThaiLeaks (Thailand), BalkanLeaks (the Balkans generally), PinoyLeaks (the Philippines – with the spectacular slogan 'Those who engage in Monkey Business should beware of the Monkey-Eating Eagle'), PirateLeaks (the Czech Republic), TuniLeaks (Tunisia).

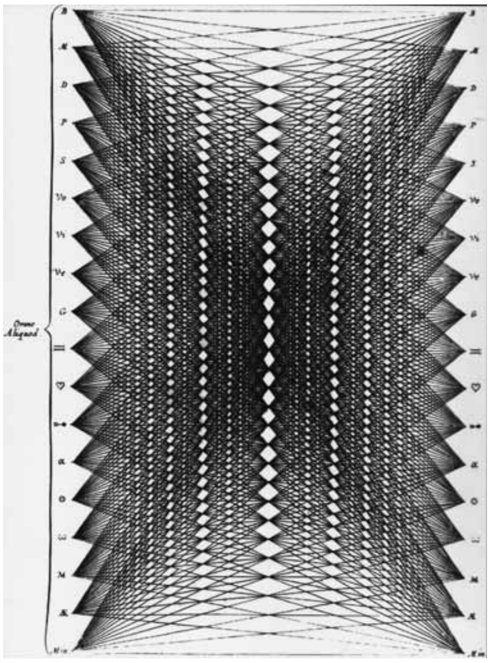
The copying and reinvention of the *Leaks structure (to use an asterisk as programmers do with '*nix' for any flavour of operating system similar to Unix) will be far more significant than any specific disclosure on the part of WikiLeaks itself – though for now the latter has the benefit of a core team of highly skilled programmers and administrators, working relationships with major publication outlets and a few trustworthy ISPs and governments, an articulate public face, and a number of unexpected allies, like the roving volunteer band of activists and troublemakers that constitutes Anonymous. WikiLeaks is a single organization, with a number of visible flaws, and more undoubtedly apparent to insiders, but encrypted drop boxes and distributed digital publishing are powerful and established technologies only now beginning to find the extent of their purpose. (It will be interesting to see if the local/national model in *Leaks projects so far is supplemented by more domain-specific groups – devoted to leaks concerning banks and the financial industry, universities, pharmaceuticals, or agribusiness, for example.) WikiLeaks is not the last word but the first, and it demands analysis as such.

Similarly, Assange is not the sum of the *Leaks project – there is deep concern within the ranks of WikiLeaks about his leadership, and indeed concern about the role of 'leaders' generally in such an organization – but he remains a vital figure for understanding the political role and the possibilities embedded in the current technological infrastructure. In his writings, which include a blog, papers and drafts of papers, a book for which he did much of the research, and postings to various mailing lists (primarily concerned with cryptography), we can find a set of ideas to illuminate the present event of WikiLeaks: the application of computational thinking to politics, a sustained consideration of the relationship between secrecy and publicity, a strategy for automatically rewarding open organizations relative to closed, and, perhaps most surprisingly, a philosophical engagement with logic and phenomenology that becomes a model for a politics that compensates technologically for human cognitive deficits. To understand the trajectory of these ideas, we must also understand the culture and the ethics of hackers and cryptographers in which they were nurtured – a culture that prizes elegant solutions to complex problems, transparency for organizations and privacy for individuals, and the free circulation of knowledge, all of which we find embedded in WikiLeaks.

This article was written at two speeds: the slow pace of reading and reflection – about that slowness, more in a moment – and the velocity of the urgent and exigent problems of the present situation. For the latter, this article's conclusion includes problems to be resolved and steps for immediate action if we are to sustain the techno-political future of which WikiLeaks has been the preliminary stroke. For the former, that slowness, what the moment demands of us here, in the pages of *Radical Philosophy*, is not more speculation as to Assange's character or the inner workings of the organization, nor further reminders of the revelations (or their lack) in the cables, nor more political oratory. Those things are all being done elsewhere, in volume and at length, by people and institutions on all sides – and duplication of effort is antithetical to the hacker ethos whose mindset we are seeking to understand. What a philosophical space is in a unique position to provide is interruption, contemplation and *slowness*. In the midst of the global 24-hour pulse of news and analysis, we can pause, to comprehend WikiLeaks as a historically and technologically embedded event, a gathering of many forces that we can draw apart. We have an opportunity to be 'true to the visible and the invisible', as Assange has said of his own work on the history of hacking, examining both present forms and the underlying fields of force that shaped them.[3]

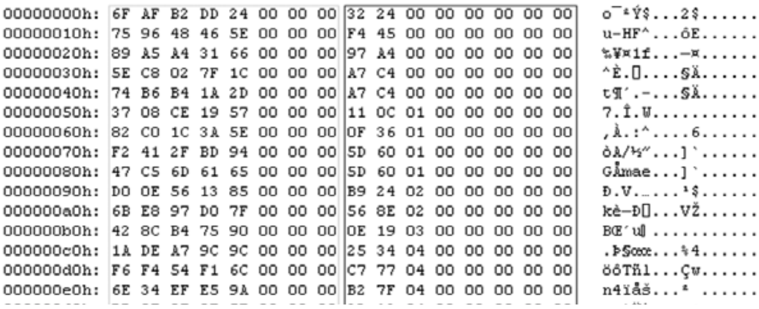
How long have you got?

The conversation of cryptography, Assange's milieu, often comes back to cosmic scales of time. Long strings of numbers are always present; sometimes these are hashes or public keys, but often they are years, the inconceivably long spans it would take to crack a particular code by crude means. The immediate business of crypto – so often protecting yesterday's secrets or today's mail – exists in the shadow of epochs and *kalpas* of potential computing time. So it is with 'insurance.aes256', the 1.4 gigabyte encrypted file posted to the WikiLeaks page for the Afghan War Diaries in late July of 2010. 'Insurance': it is, presumably, meant as a dead man's switch, in the event of something truly dire happening to the organization or its leader. After a certain number of days without logging in to a system or responding to an automated ping, the key will be made available (sent, automatically, to large groups of reporters and sympathizers, posted to blogs and Twitter, and so on). There are few more intensely contemporary digital objects than this opaque file: an unreadable document that is the focus of intense public scrutiny, the intersection of publicity and secrecy – indeed, a 'public secret' if ever there was one, an informational threat turned into a distributed protection scheme, made available to all, first by download and then shared on peer-to-peer networks, accumulating interpretations, and containing… what? Clear-and-present-danger information, Top Secret rather than merely classified, a scorched-earth response to damage? Or is it empty, just noise, a bluff – a contemporary version of the apocryphal telegram, suggestive but content-free ('All is discovered; flee at once') with which Arthur Conan Doyle claimed he could send any pillar of society rushing out into the night without even a change of clothes? Some in the crypto world see it as a challenge to the National Security Agency to reveal that it has known how to crack the Advanced Encryption Standard (the '.aes') all along – since why would they approve of an encryption method to which they didn't have a back door?



Kircher, *Ars Combinatoria*, 1669

All of this speculation plays out in the immediate foreground of a timeline that stretches beyond the end of the universe. The '256' in .aes256 means that decrypting the file requires a key 256 bits long. To guess this key by trying every possible combination, a 'brute-force' attack, means searching through a vast keyspace. Every popular discussion of cryptography involves a few back-of-the-envelope Fermi estimates with the inevitable conclusion: if we turned all the computing power on Earth to the problem of decrypting insurance.aes256, accounting for the steady increase in processing capacity – every microchip coming out of Intel dropped into another machine to enlist immediately into the work – it would still take longer than the life of the solar system, the galaxy, the universe, before we would get anywhere. The presence of this cosmic length is salutary, offering an opportunity to slow down, to read these events in light of the past, to contemplate.



```
00000000h: 6F AF B2 DD 24 00 00 00 32 24 00 00 00 00 00 00   o¯²Ý$...2$......
00000010h: 75 96 48 46 5E 00 00 00 F4 45 00 00 00 00 00 00   u–HF^...ôE......
00000020h: 89 A5 A4 31 66 00 00 00 97 A4 00 00 00 00 00 00   ‰¥¤1f...—¤......
00000030h: 5E C8 02 7F 1C 00 00 00 A7 C4 00 00 00 00 00 00   ^È.□....§Ä......
00000040h: 74 B6 B4 1A 2D 00 00 00 A7 C4 00 00 00 00 00 00   t¶´.-...§Ä......
00000050h: 37 08 CE 19 57 00 00 00 11 0C 01 00 00 00 00 00   7.Î.W...........
00000060h: 82 C0 1C 3A 5E 00 00 00 0F 36 01 00 00 00 00 00   ‚À.:^....6......
00000070h: F2 41 2F BD 94 00 00 00 5D 60 01 00 00 00 00 00   òA/½”...]`......
00000080h: 47 C5 6D 61 65 00 00 00 5D 60 01 00 00 00 00 00   GÅmae...]`......
00000090h: D0 0E 56 13 85 00 00 00 B9 24 02 00 00 00 00 00   Ð.V.…...¹$......
000000a0h: 6B E8 97 D0 7F 00 00 00 56 8E 02 00 00 00 00 00   kè—Ð□...VŽ......
000000b0h: 42 8C B4 75 90 00 00 00 0E 19 03 00 00 00 00 00   BŒ´u ...........
000000c0h: 1A DE A7 9C 9C 00 00 00 25 34 04 00 00 00 00 00   .Þ§œœ...%4......
000000d0h: F6 F4 54 F1 6C 00 00 00 C7 77 04 00 00 00 00 00   öôTñl...Çw......
000000e0h: 6E 34 EF E5 9A 00 00 00 B2 7F 04 00 00 00 00 00   n4ïåš...² ......
```

Nietzsche, no stranger to time-delay problems, writing as he often did for 'readers foreordained', passport-holders from Hyperborea with 'new ears for new music', notes the highest virtue available to the aristocracy – *slowness,* the 'slow glance', 'to take time, to become still, to become slow.'[4] From this comes philosophy's strength to consider an event like WikiLeaks (we could speak as well of Žižek's insistence that we wait in the face of immediate crisis, that we seize time to think). The brute-force strategy on .aes256-encrypted files invites us to think of a history before and after our present political and technological forms. To crack the key by force would open the 'insurance' file long after the continents had gathered again, the Earth fallen into the atmosphere of the dying sun, and the sun itself collapsed to an extremely dense and faintly luminous white dwarf. Amidst all the din of news and politics we can take some small part of the geological calm inherent in a huge keyspace, and think, slowly and in long perspective, about what is happening now – starting with the utopian imaginary of digital disclosure.

'I can't even read my own notes without wondering if I'm trying to send myself a secret message while doing everything possible not to be deciphered by myself', as one of the cryptanalysts says in Edmundo Paz Soldán's *Turing's Delirium,* a novel Assange cited on his now-defunct blog in 2006.[5] Soldán's novel, a political thriller devoted to the culture of hackers and cryptographers, plays out the struggle between the Black Chamber, an NSA-like gathering of cryptographers devoted to securing the secrets and information-gathering capacity of the state (and the transnational corporations with which it is partnered in the privatization of the country's utilities), and the loose team of dissident hackers who release hidden documents and engage in denial-of-service attacks. (In a beautiful touch which feels thoroughly in keeping with our moment of Berlusconi, Murdoch, and Roger Ailes of Fox News, the fatuous state-sponsored news is delivered on television by a Philip K. Dickian virtual avatar, Lana Nova, 'who has just been given an upgrade and now has twice the number of her original facial expressions'.[6] Any real understanding of the situation in Soldán's setting of Río Fugitivo belongs to those who can attend to the materials online.) The dissidents, led by a gifted hacker whose assumed identity, 'Kandinsky', becomes a flexible name another can assume to die in his place, are potent examples of the image of the young inventive programmer snatching secrets from the grip of those in power. But we can go further back for our icons of the present.

'This has been an unauthorized cybernetic announcement', concludes the note on the package in John Brunner's 1971 *The Shockwave Rider,* a science-fiction novel whose depiction of data liberation provides an instructive contrast to the existing reality and theories underlying WikiLeaks. The main character – another in the long line of supremely gifted fictional hackers with restlessly fluid identities – has gathered every instance of suppressed knowledge in his future United States and seamlessly interpolated it into everyday life, a one-step transition into an entirely transparent digital society. Financial fraud, featherbedding and an imminent bankruptcy appear in the company's annual report; an explicit breakdown of item-by-item spending in the back-tax demand; every health violation on the ingredients list of the can, and known present carcinogens on the box of cosmetics (and the cost of the out-of-court settlements): 'This is a cybernetic datum derived from records not intended for publication', say many of the notes. The protagonist who has launched this scheme says it simply: 'As of today, whatever you want to know, provided it's in the data-net, you can now know. In other words, *there are no more secrets*.'[7]

The project is a fantasy of rational action based on perfect knowledge – a subject at the heart of Assange's writings. It is also a fantasy of data delivered appropriately, made into knowledge through automatic processes. The product of the protagonist's surveillance worm program isn't some accumulation of raw data, hundreds of gigabytes of text exports, SQL dumps, KML and CSV files: it arrives, in Brunner's fictional vision, assembled and packaged as it would be by a muckraking journalist and posed in strident terms of bribery, propaganda, environmental degradation, human-rights abuses, and so on, neatly attached to the relevant area of public life.[8] Ask a question, and the system delivers you a cogent and polemical answer, outlining clear cases of malfeasance and atrocity – no ambiguous and convoluted financial instruments here, no structures that are disproportionately beneficial to some, no layers of complicity, but straightforward crimes with obvious perpetrators. It's the data version of Cockaigne, where cheeses fall from the sky and fish leap from the sea to the hungry peasant's feet. The public reacts appropriately, inquiring into every corner of diabolical mismanagement, and turning their outrage to the construction of a new society for the greater good. (This takes the form of an austere command economy whose logic springs from the detailed economic data redacted and withheld from the populace. It's a strange amalgam of Allende's pilot Cybersyn project and the guaranteed minimum income.) 'Therefore none shall henceforth gain illicit advantage by reason of the fact that we together know more than one of us can know', Brunner closes, one of the propositions of this new society of permanent data transparency. The layers of fantasy present here – that the secret data will be immediately useful, that social ills are the result of distinct and specific crimes whose perpetrators can be easily dealt with, that a cogent argument can be made to which the populace will respond with appropriate and focused action – are part of the enormous frustration which drove Assange to action, to a nonfictional project in collective data disclosure.

This problem of logical speech and rational action runs through much of Assange's non-cryptographic writing. He has described the goal of WikiLeaks as 'scientific journalism' – 'read a news story, then to click online to see the original document it is based on'[9] – with the evidence ever-present. He returns again and again in his writings to problems of argument, evincing the disappointment of the 'logical reductionist', as he characterized himself: 'I once thought that the Truth was a set comprised of all the things that were true, and the big truth could be obtained by taking all its component propositions and evaluating them until nothing remained.'[10] Argument is unavailing when it displeases the listener, the axiom of transitivity is revoked, and illogic wins the day. Why do people fail to act in their best interest? How can they condone the crooked, the venal, the obviously false and the wrong-headed? Assange takes notes throughout his blog on problems in cognition, psychology and epistemology: 'learned idiocy', measurement problems in physics, emotional manipulation by advertising, the social experience of gifted children, perceptual calibration. 'How to hack reality? How to pierce the skin? How to find the spot on the wall where the illusion flickers and rip it open?'[11] His anger at wilful misperception is intense:

> And before this [desire for truth] to cast blessings on the profits and prophets of truth, on the liberators and martyrs of truth, on the Voltaires, Galileos, and Principias of truth, on the

> Gutenburgs [*sic*], Marconis and Internets of truth, on those serial killers of delusion, those brutal, driven and obsessed miners of reality, smashing, smashing, smashing every rotten edifice until all is ruins and the seeds of the new.'[12]

Minus the Internet, Marconi (a technologically conservative fascist, but let that pass) and 'serial killers', this would not be out of place in a socialist pamphlet in the tradition of Bakunin – or, with the sentiment slightly toned down, the work of Marxist philosopher of language and information visualization pioneer, Otto Neurath. It is this deep disappointment in the failure of logical argument, of evidence, to spur righteous action, that gives WikiLeaks its two-tier strategy which distinguishes it from the *Shockwave Rider* fantasy.

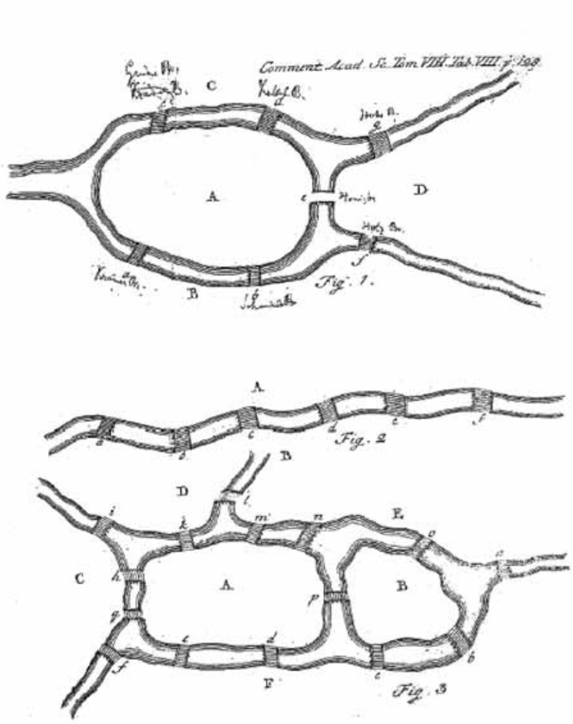
'You throttle it'

A state is a 'certain relationship', as Assange quotes Gustav Landauer: an arrangement of humans towards each other.[13] The genius of the WikiLeaks model, in all its various adoptions and adaptations, lies in the manipulation of this human arrangement from two sides – we can call them exoteric and esoteric. The exoteric model is the obvious work of a data disclosure project like WikiLeaks: providing the public with knowledge it would otherwise be denied. This carries a few strategic difficulties. First, the data must be manipulated into a useful format and provided with an interpretive and presentational layer for those who don't want to pore over a few hundred thousand text files, or figure out what 'CSV' means. This is the work of journalists, as in Cablegate, and volunteer programmers and designers, as with diarydig.org (now relocated following attacks to http://213.251.145.96/search/), and crowds of readers, as in the Reddit collective search through the 9/11 pager logs ('We need to get this to Page 1, to increase the number of people analyzing and reporting'[14]).

Second, and far graver, is the rationalist's complaint, the problem that makes the end of Brunner's novel such a painfully wishful thing to read: you can provide a public with the information, you can give them 'scientific journalism', and they still won't do anything. They will disregard your evidence, ignore the logic of your arguments, or persist, unsurprised, in acting as they always have. Perhaps they will, in fact, be reassured and heartened by their government's willingness to disappear and torture alleged suspects, cook evidence and cover up wrongdoing, and engage in secret drone strikes in Yemen. This is, to take a locution from bug reports, a 'known problem', the internal threat to social action – inertia, willed ignorance, misrepresentation, distraction, the condition of 'witnessed, but seemingly unanswerable injustices', to quote one of Assange's essays.[15] The possibility of public inaction provokes the second, esoteric element of the WikiLeaks strategy.

Assange has a very different public in mind as the esoteric audience for the disclosures of WikiLeaks, or any WikiLeaks-like organization: those who already know the secrets, those who created them. Over the course of two drafts (with different titles) of a document published in the last months of 2006, 'State and Terrorist Conspiracies' and 'Conspiracy as Governance', Assange outlined what is arguably the primary purpose of a leaks-driven project, with 'scientific journalism' being a positive second-order effect.[16] It builds on a mathematical discipline called graph theory and a conspiratorial view of politics to produce a computational model of the capture of state power. To be clear, Assange defines 'conspiracy' quite broadly – the actions and plans of a political elite which are kept secret to avoid inducing resistance on the part of a public: 'individual and collective will' in one draft, 'the people's will' in another. These conspiracies constitute the active political form, the 'primary planning methodology' of 'authoritarian regimes' – though an example of 'two closely balanced and broadly conspiratorial power groupings', the Republican and Democratic parties of the United States, suggests, again, that for Assange's purpose an 'authoritarian conspiracy' is a spacious category.

Given this breadth, and the sheer diversity of possible conspiracies in scale, means, goals and contexts, is it possible to generalize and abstract an anti-conspiratorial strategy? Assange turns to graph theory, a branch of mathematics devoted to the analysis of networks. Graph theory began with the superlative mathematician Leonhard Euler, who perceived within a party game about the bridges of Königsberg (can you cross each bridge once and return to your starting point?) a number of points and lines, nodes and paths. It provides a way to extract abstract diagrams from the messy specificities of real-world networks. Imagine, Assange asks, that we can describe a conspiracy in this abstract fashion: all the participants are nodes, points on the network, with lines of communication between them along which information flows. The edges of the conspiracy are defined by all those from whom these secrets must be kept. The lines of communication within the conspiracy can be of varying 'weight', describing the amount of important information being passed along, and nodes can be of higher or lower value depending on the weight and number of their connections to other nodes. This model allows Assange to bracket out the complexities of specific conspiracies, and produce an evaluative metric of 'total conspiratorial power' – the power of the group to communicate and plan internally, that is, rather than its capacity to effect change in the world: 'the ability of the conspiracy to think, act and adapt'.[17] (If any curators want to produce a highly relevant retrospective in 2011, Marc Lombardi's 'Narrative Structure' diagrams – intricate hand-drawn maps of conspiratorial projects, in the Assange sense – are crying out for a show.)



Assange takes this model further: the conspiracy is a type of device for taking an input, like reports, cables and intelligence, acting on it, and producing an output. A conspiracy 'computes the next action of the conspiracy', in his words, and the total conspiratorial power is the clock rate of this device, how fast it can advance to the next step and react to new states of affairs.[18] The traditional approach to dealing with conspiracies has been a patient and particular one: documenting their workings, finding the most significant nodes, and removing them from the graph – that is, imprisoning or assassinating people. Ideally, analysing the graph would allow you to target nodes whose removal might break a conspiracy into two separate and weaker units, for example, or abruptly isolate many other nodes. Assange wants an abstract and general strategy suited to his black box input–output model. What is the best way to lower the total conspiratorial power of *any* conspiracy, whether it's a political party, a group of insider traders, a terrorist cell, a multinational corporation or a small gang of bureaucrats?

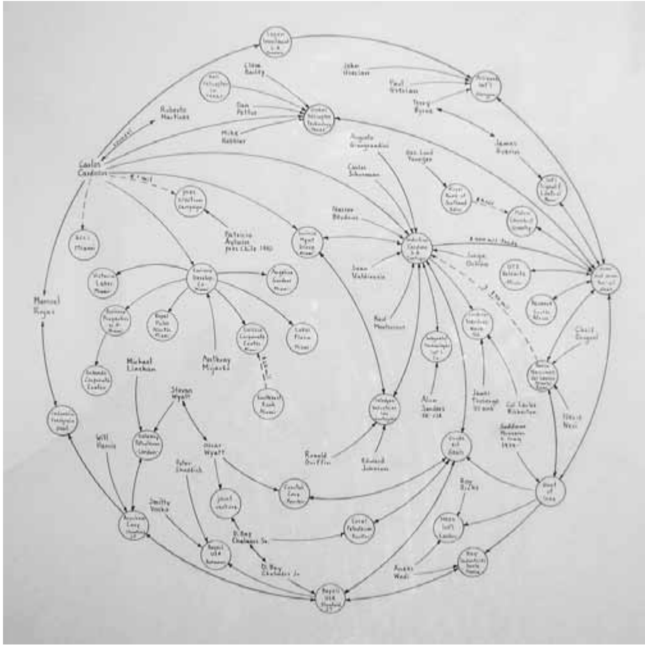
You do this by leveraging the Internet's capacity for anonymity of users and distribution of information. If anyone in the conspiracy leaks, and the information is disclosed anonymously, everyone in the graph becomes suspect, if not for leaking then for negligent security. You don't need to neutralize key nodes if they stop talking to each other, or if their conversations are so restricted by the possibility of disclosure that their links become far less important. You 'throttle' it, which Assange means in the mechanical sense: the fuel decreases, the speed slows.[19] The total conspiratorial power is turned down towards zero, the state where no one is talking to anyone else. The 'blood' of the conspiracy as creature 'may be thickened and slowed until it falls, stupefied; unable to sufficiently comprehend and control the forces in its environment'.[20] This is the esoteric strategy, and its goal is a power split into fragments and so locked in purges, silence, tactical internal denials and traceable lies that it is halt and lame, chewing on its own tail. This is a key reason why the WikiLeaks group are not 'hackers', in the crude but common sense of people penetrating secure systems to acquire information. To break into a system and steal a document merely provokes an organization to improve its security, and releasing the document is no guarantee of a positive social result. It is vital that the materials are *leaks* because that will foment suspicion and paranoia among the conspirators. The ideal application of the Assange model is a kind of panopticon turned inside out, where the main guard tower is gone because any given prisoner might be an informer.

Furthermore, such an approach places a differential burden on institutions: in a world where leaking is a strategy of redress, more secretive (which, for Assange, is synonymous with 'unjust') organizations will be hit much harder than comparatively open groups. In the blog post, from precisely four years ago today, that links to the PDF of 'Conspiracy as Governance', he summarizes his argument for the future:

> [I]n 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.[21]

It is this strategy that distinguishes something like WikiLeaks from yet another speculative icon of network politics – the engineer and 'cypherpunk' Timothy May's 1993 proof-of-concept BlackNet project, to which WikiLeaks has been somewhat misleadingly compared.

BlackNet was an entirely anonymous information marketplace, built on untraceable digital cash, for people to transact anything that could be transmitted digitally ('corporate secrets, military secrets, credit data, medical data, banned religious or other material, pornography, etc.').[22] In the long run, the adoption of anonymous, untraceable transactions would be an engine for May's specific school of anarchism. It would be a government-crushing machine – 'the real choice is between a total state and crypto anarchy', May asserted, at least as far as life informationally and life online are concerned.[23] WikiLeaks, in the long run, is meant as a way of filtering good/'open' organizations from bad/'secret' ones, creating an inhospitable environment in which to be secret, and thereby improving governance. Assange is not the nihilistic wrecker-of-civilization fantasized by the American right (who seem to have at last found the Bond villain their impoverished understanding of the world has led them to look for). His work reflects an attitude of intensely moral empiricism, empowered by a programmer's toolkit for abstraction and breaking big problems into smaller ones. The politics of WikiLeaks is a *cybernetic* politics, with built-in, auto-correcting feedback loops that tend a society towards transparent institutions and accurate information, because the cost of conspiratorial secrecy is pushed disproportionately high.



Marc Lombardi, Narrative Structure Diagram

Assange concludes the latter of the two 'conspiracy' papers, dated 3 December 2006, with this sentence:

> Later we will see how new technology and insights into the psychological motivations of conspirators can give us practical methods for preventing or reducing important communication between authoritarian conspirators, foment strong resistance to authoritarian planning and create powerful incentives for more humane forms of governance.[24]

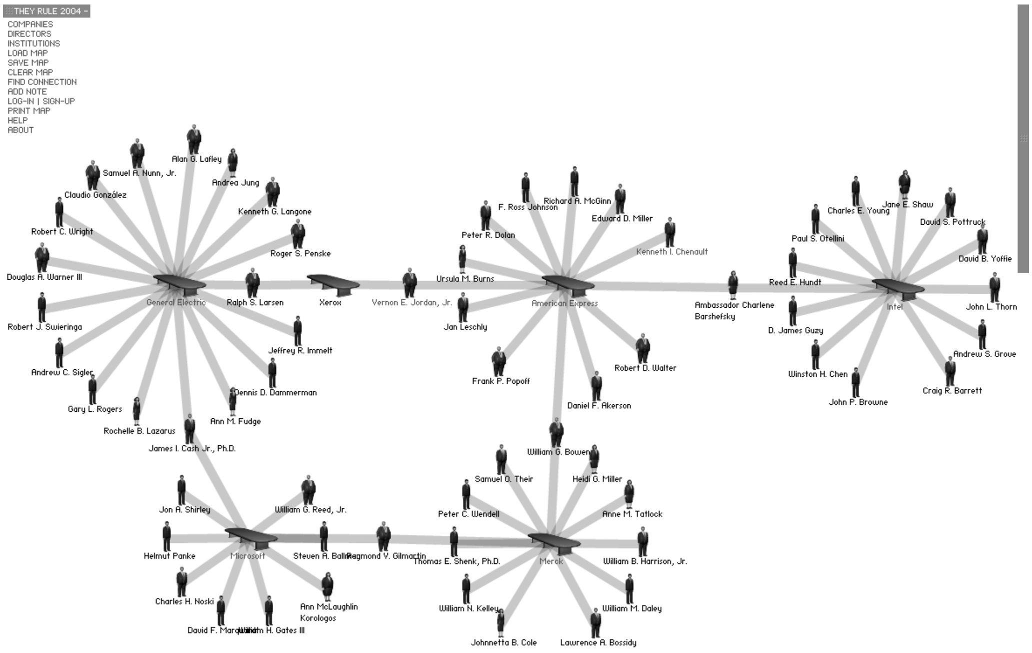
He never got around to concluding the paper – or, rather, its conclusion, those 'practical methods', is all around us, a demonstration of his anti-conspiratorial strategy. The domain name for WikiLeaks was registered in October 2006, and the site was publishing documents by that December.

That last goal – 'more humane forms of governance' – expresses part of the larger project with which Assange is engaged. It is a project that, strange as this may sound given his application of abstract computational thinking to politics, is fundamentally humanist, in a very specific sense. In 'scientific journalism' and strategies for exploiting paranoia, in his desire for immediate experience and accurate perception (as he contrasts, for example, the 'powerful, communicatable phenominological [*sic*] descriptions of nature' given by young children against the 'meaningless answers' given by older children who repeat what they've been told by teachers[25]), Assange seeks a technologically enabled political system that can compensate for human cognitive limits. He wants an open society not simply because it is less conducive to authoritarian conspiracies, or because it will encourage social justice, but because the circulation of accurate data will aid us in living in our almost unmanageably complex society.

Inky fingers

Another thought experiment for cryptographers, another project in human capacities for Assange: how to make a key operative only under certain psychological or physical conditions. Is it possible to create a key that, under coercion, locks the interrogator out of the file, using the limits of the human body and mind as a kind of failsafe? Pain, altered states, impaired cognition could become parameters for decryption. Assange sketched some solutions in a posting to a mailing list devoted to OCaml, a programming language with properties useful to his project.[26] Along with recognizing faces and creating meaningful similes (A is to B as…, etc.), Assange suggested a maze-walking exercise: a maze with landmarks that you pass in a certain order and direction to produce your key. This path would be immune to key-logging techniques (which track every stroke on a keyboard) and could draw a different maze every time; only you would know in what order the landmarks must be passed. It might be impossible to explain under coercion. Perhaps walking the maze in one progression would unlock something plausibly revealing but relatively innocuous – and a different route opens the text file with all the safehouses, all the names of colleagues. In any case, to produce the key, the human element needs to be there, at the mouse, conscious and willing.

Like this notional keying system, the event of WikiLeaks is only concerned with 'computer security' in the most peripheral way. What is actually at issue is the politics of secrecy, anonymity, and online distribution and collaboration – *new logics of organization*, as Alexander Galloway has put it. The security of the machines isn't really at issue; it's the humans that are fragile and dangerous. The term from military aerospace for building technologies that have to involve people, the 'man-in-the-loop', works perfectly here. You want to minimize the harm the man, in-the-loop, can do to your system: so slow, so prone to black out under high G-forces, so inclined to momentary hesitations, to calls of conscience, to leaks and confessions. A decade before Assange laid out the theoretical architecture for turning the people inside a conspiracy against one another, he was collaborating on a project named 'Marutukku' (a Mesopotamian god, 'master of the arts of protection'), a deniable cryptography package.[27] 'Deniable', in this case, meaning that you can provide a passphrase to decrypt some portion of your



data without revealing the whole thing, or that there's more to reveal. Marutukku was also known as Rubberhose, after the old crypto joke about 'rubber hose cryptanalysis': decrypting a file by beating the key out of someone who knows it. Marutukku was designed to provide both cover (you could plant some secrets to satisfy your interrogators – the maze-walking key was to be one notional part of Marutukku) and the deeper deniability of ignorance. You could receive a thumb drive, and a key to some portion of it, unaware that there are others, thus minimizing the informational damage that even torture can do, and working around human frailty. WikiLeaks, and what it portends, is all about working with and managing our points of failure and overload, as human minds and as social creatures.

Assange's particular design intelligence has always been about taking advantage of the irreducible humanity within computational processes, from our visual capabilities (another keying method he proposed involved generating moirés of color whose variations would be visible to a single individual's unique sense of hue) to our paranoia, our social arrangements, our difficulties with reductionist logical argument. On Sunday, 30 July 2006, apropos of Finland's transparent taxation system, he wrote an introductory comment that provides the context not only for WikiLeaks and related projects, but for our current dispensation, the horizon of the political thought that WikiLeaks represents:

> Society has grown beyond our ability to perceive it accurately. Our brains are not adapted to the environment in which we find outselves [*sic*]. We can't predict important aspects of our societal environment. It's not designed to run on our brains. We're maladapted. In our evolutionary history we spent a lot of time tracking the behavior and reputations of small number of people we saw frequently. If we want some of the social benefits that a small society brings then we need computational crutches so when A fucks over B any C considering dealing with A will know. A society that can 'think' in this way is able to route goodness to people who do good and away from those people who generate hurt. The decision as to what is good is too complicated to be formulated in regulation and elections are a very coarse expression of what people think is good. Any paper formulation will put power in the hands of a political and technocratic elite. Robust routing decisions must be made by individuals and individuals need tools to manage complexity enough so they can make them effectively in a modern society.[28]

We can discern in this that 'society' is a larger version of Assange's conspiratorial structure: an information-processing system, computing next steps and, ideally, routing towards the good and away from the bad. What society, understood like this, needs most is tools to circulate data, and to 'manage complexity' – such as an organizational model and a kit of technologies that will, theoretically, edge a society always towards increasing the flow of accurate information available to all eyes. From 1990 to now, the night that I write this, the power of a given computer has increased by a factor of about 8,000. Storage capacity relative to cost has grown still faster.[29] The release of the Pentagon Papers – another regular WikiLeaks comparison – was an event of extraordinary *paperwork*. Daniel Ellsberg's task primarily lay in arranging the reproduction, movement and storage of thousands of pages, using relatively rare photocopy machines, one page at a time ('To speed up, I tried to program my motions'[30]), and workflows of folders, scissors, glue, suitcases and cardboard boxes. The particular affordances and constraints of paper are intimately intertwined with the shape of bureaucratic governance, from Charles-Hippolyte Labussière – the clerk whose covert destruction of documents (using public baths and the Seine) created for the Committee of Public Safety during the Terror saved much of the Comédie Française from execution[31] – to the dossiers of the Stasi, the in-trays of the Eichmannian *Schreibtischtäter*, and the 'Vietnam War Study' folders Ellsberg pulled from the filing cabinets at RAND. To intervene in the flow of paperwork is still a heavy, toner-streaked, physical matter, requiring someone with Ellsberg's access over time coupled with a willingness to go to prison. Even given these characteristics there is no possible way for the most dedicated renegade diplomat, working with paper, to collect 250,000 confidential cables and make them available to journalists or the public. That's a lot of reams of paper, and pallets of documents, to transact secretly. Digitally, it's a thumb drive, a CD, a zipped file uploaded to a server. It can be forgotten in a taxicab, lost in a messy office. And it can be circulated with complete anonymity for the leaker. (Bear in mind that PFC Bradley Manning, the alleged leaker in the Cablegate case, was apprehended based on the advice and chat transcripts provided by Adrian Lamo, to whom he apparently confessed much of his activity.) New forms of information storage, distribution and analysis can enable new political arrangements – new apparatuses of surveillance and capture as well as publication, organization and resistance.

The promise of these new technologies and the new arrangements they could enable relies on more general action, our action. As I've suggested at the opening, WikiLeaks is only the first such object, and one of its most valuable contributions is the provocation to further work. I'd like to close this article with a direct address, at present speed rather than reflective philosophical slowness – a contemporary version of Fourier's chapter at the close of the *Théorie des quatre mouvements*, where, having presented his arguments for the political-ecological transformation to come, he provides hands-on counsel for those who would be prepared. We could even give it the same title: 'Advice to the Civilized Relative to the Coming Social Metamorphosis'.

Given WikiLeaks and the boom in *Leaks organizations, given our capacities for anonymity, data storage and distributed publication, what is to be done? Fourier's advice included 'not to sacrifice present good for future good'. To this we can add the following, which is only a starting point, welcoming further additions and conversation.

- If you understand and can deploy the technologies – and you should take this very seriously, as the safety of any potential leaker relies on it – you can launch your own *Leaks project. If you aren't in a position to roll them yourself with complete confidence in your security, keep a close eye on OpenLeaks, which, at the time of writing, has a promising approach to providing secure drop boxes for other organizations. As with blogs, the most successful leak sites will probably be those with quite specific subject domains, which can attract journalists and skilled crowds to their analysis and make sure stories particular to that area are heard. Any project like this is going to involve experience in the editing and redaction of releases, and painstaking internal security and ethical reflection – Geert Lovink and Patrice Riemens's thesis 11 of their 'Twelve theses on WikiLeaks' provides a concise overview of these issues.[32]

- There are numerous projects of infrastructural significance which need contributions. These are not reactions to WikiLeaks itself but to the very real problems with authority, control and rule of law online which it provoked into high visibility. They include: new cloud services (following Amazon's deplorable plug-pulling of the WikiLeaks resources on their servers), of which OpenStack (http://openstack.org) provides a good starting point; new Domain Name System (DNS) architecture, so people can type in a human-memorable name (as opposed to a string of digits) and get the Web site they want regardless of what parties may seek to make the name unavailable or unreliable – there are interesting proposals being mooted for a peer-to-peer DNS system that would decentralize addressing (see, as a starting point, http://dot-p2p.org); and on the farther horizon new systems of funding, to ensure the donation and asset freeze-out directed against WikiLeaks by PayPal and the credit card companies cannot continue to be a problem.
- There are a number of social and legal issues. While well-run *Leaks projects can provide anonymity and protection to the leakers with methods like encrypted connections and anonymous proxies, the human need for solidarity, empathy and companionship, especially on the part of one of who is running serious personal risks on principle, is profound – as the grim case of Manning, currently spending twenty-three hours a day in solitary in the Marine Corps brig, will attest. Some method to enable community and alliance without discovery seems warranted. As does assistance with how to talk to the media in the release of a leak – a means to counteract the inevitable spin, message management and public relations deployed by institutions to marginalize any potentially damaging information. One grave legal concern is the protections available to 'mirror sites'. A site like WikiLeaks, coming under attack, relies on volunteers hosting mirrors on other servers, so people seeking the site's information can reliably find it elsewhere if the main site is unavailable. Hosting a mirror is currently a legal grey area, however – especially for hosts within affected countries, like the United States. Will a mirror host face pressure from the state, their employers, or others, and what is their recourse to pressure?
- A massive document-gathering like that of the SIPRnet cables was probably lucky, and will not be repeated. Systems of logging access and document requests will make it far more difficult to collect material anonymously. Solutions for undetectably copying documents are needed.

Notes

Research for this article was supported by a grant from the National Science Foundation (CNS/NetS 1058333) and the AFSOR-MURI Presidio grant. It would not have been possible without the help and suggestions of several persons who would prefer to remain anonymous. Thanks to you, my friends. Hone-o oru! To simplify the process of future researchers, I have followed the different time/date formats used by the different online resources cited below.

1. Julian Assange, 'time-delayed release of information', post on the cypherpunks list, 2002–03–23. http://marc.info/?l=cypherpunks&m=101686313723681&w=2.
2. As interviewed on www.cbc.ca/thecurrent/episode/2010/12/06/dec-610---pt-1–julian-assange/.
3. Julian Assange, 'Researcher's Introduction', in Suelette Dreyfus and Julian Assange, *Underground: Hacking, Madness and Obsession on the Electronic Frontier*, Mandarin, Port Melbourne, 1997. Available electronically at www.xs4all.nl/~suelette/underground/.
4. Friedrich Nietzsche, 'Preface', *Daybreak: Thoughts on the Prejudices of Morality*, ed. Maudemarie Clark and Brian Leiter, Cambridge University Press, Cambridge, 1997, p. 5.
5. Julian Assange, 'Turing's Delirium', post on iq.org, 22 September 2006. Assange's blog was shut down some time ago; this and all other blog citations from the version archived on the Wayback Machine: http://web.archive.org/web/20071020051936/http://iq.org/.
6. Edmundo Paz Soldán, *Turing's Delirium,* trans. Lisa Carter, Mariner, New York, 2007, p. 207.
7. John Brunner, *The Shockwave Rider*, Harper & Row, New York, 1975, p. 219.
8. Conversation with those involved makes clear that creating a useful – that is, hyperlinked, searchable, reasonably fast – front-end for even a relatively constrained set of materials, like http://diarydig.org for the Afghan War logs, is not a trivial matter.
9. Julian Assange, 'Don't shoot messenger for revealing uncomfortable truths', op-ed in *The Aus-*

tralian, 8 December 2010; available online at www.theaustralian.com.au/in-depth/wikileaks/dont-shoot-messenger-for-revealing-uncomfortable-truths/story-fn775xjq-1225967241332.

[10] This particular thought actually appears twice, almost unchanged, in the final entry of his blog, as well as about a year earlier: 29 August 2007 and 12 July 2006.

[11] Julian Assange, 'How can we untie the unknot?' post on iq.org, 3 August 2006.

[12] Julian Assange, 'Iirationality [*sic*] in argument', post on iq.org, 29 August 2007.

[13] Assange quotes Landauer at the beginning of the last version of his homepage at iq.org, as preserved at http://web.archive.org/web/20071020051936/http://iq.org/.

[14] See the Reddit thread 'Conspiracy theories commence: WikiLeaks to release over half a MILLION text messages from 9/11', submitted 24 November 2009, comment by 'xyroclast': www.reddit.com/r/reddit.com/comments/a7xpt/conspiracy_theories_commence_wikileaks_to_release/c0gatuc.

[15] Assange, 'Conspiracy as Governance', p. 1 n1.

[16] Both drafts were released as PDFs, originally linked from Assange's blog and now hosted by John Young at the website Cryptome: http://cryptome.org/0002/ja-conspiracies.pdf.

[17] Assange, 'Conspiracy as Governance', p. 4.

[18] Ibid.

[19] Ibid.

[20] Ibid., p. 5.

[21] Assange, 'The non linear effects of leaks on unjust systems of governance', post on iq.org, 31 December 2006.

[22] Timothy C. May, 'Untraceable Digital Cash, Information Markets, and BlackNet', presented at Computers, Freedom and Privacy 1997; available online at: http://osaka.law.miami.edu/~froomkin/articles/tcmay.htm.

[23] Ibid.

[24] Assange, 'Conspiracy as Governance', pp. 5–6.

[25] Julian Assange, 'Tale of the Tesla coil, or learned idiocy', post on iq.org, 26 June 2006.

[26] Julian Assange, 'call for ocaml volunteers', post on the Caml mailing list, 2000–08–14; available at: http://caml.inria.fr/pub/ml-archives/caml-list/2000/08/6b8b195b3a25876e0789fe3db770db9f.fr.html.

[27] A basic overview of Marutukku/Rubberhose is available. See Suelette Dreyfus, 'The Idiot Savants' Guide to Rubberhose', available at: http://iq.org/~proff/rubberhose.org/current/src/doc/maruguide/t1.html.

[28] Julian Assange, 'Transparency in the cold light of Finland', post on iq.org, 30 July 2006.

[29] A few days ago, IBM's Almaden Research Center published demonstrations of the soundness of the physics underlying a new form of memory, 'Racetrack' – which uses the spin of individual electrons to move data along magnetic nanowires – pointing towards eventual production. Racetrack, or any number of other experimental models of memory, will lead to increases, relative to cost and electrical power, still more dramatic than what we've encountered so far: enormous libraries of data on a mobile device that can be accidentally put in the wash.

[30] Daniel Ellsberg, *Secrets: A Memoir of Vietnam and the Pentagon Papers*, Penguin, New York, 2003, p. 302.

[31] Benjamin Kafka, 'Paperwork', *Cabinet* 22, Summer 2006; available at www.cabinetmagazine.org/issues/22/kafka.php.

[32] Geert Lovink and Patrice Riemens, 'Twelve Theses on WikiLeaks', as posted in Eurozine, 2010–12–07; available at: www.eurozine.com/articles/2010–12–07–lovinkriemens-en.html.