The unfurling of violent rhetoric and the show of force that has lead to the arrest, imprisonment, and impending extradition of WikiLeaks founder, Julian Assange, serve as an exemplary moment in demonstrating state-sanctioned violence. Since the cables began leaking in November 2010, the violent reaction to WikiLeaks evidenced by numerous political pundits calling for
among geographers to how ‘the material’ and ‘the cyber’ differentially map onto each other in various sites as either a dialectic or dissonant process.

Human Lives
Finally, a major accusation levelled at WikiLeaks has been that the organisation has needlessly endangered human lives by releasing the Iraq and Afghanistan documents, as well as US embassy cables. While we are inclined towards believing that these are largely media scare-mongering tactics, it would be imprudent to not at least consider the idea that people could potentially be harmed as a result of these releases. Of course, the real villain here is US foreign policy, which is responsible for some of the worst episodes of violence in human history, and certainly within the last few decades. While we are hopeful that the release of these documents might alter US foreign policy, this does not appear be happening. Instead of taking this moment as an opportunity to reflect critically on the damage wrought by decades of subversion, coercion, and jingoism, the US is now talking openly about the need for even tighter security on information and ratcheting down what little transparency remains in its veiled foreign policy. The irony of public debate on the issue of secrecy is not lost on us. Yet while we remain concerned about the benefits versus the potential harms in releasing this information, and refuse to concede that the loss of a few lives in the service of some greater good is a justified means to an end, we wonder whether this is even a fair debate to have at this stage. The vast majority of the cables, while politically embarrassing, have so far been relatively banal. Thus the harm being done – at least as of yet – is not being tallied as a body count, but in terms of damaged reputations among global elites. The fact that WikiLeaks has, as of October 2011, ceased its leaking operations as a result of the financial blockade mounted by corporate America only compounds our scepticism.

In what follows, the assembled contributors of this forum unpack these issues in greater detail. Our collective hope is that these collected reflections will encourage those interested in critical, anti-, and alter-geopolitics to weigh in on and critically engage with the important debates that the WikiLeaks affair has invoked.

OUTSOURCING THE STATE—JEREMY CRAMPTON

What’s important to understand about WikiLeaks is that it’s not WikiLeaks that is important. Assessments of WikiLeaks tend to revolve around WikiLeaks as either a force for good or ill and ignore two important questions. First, what are the merits of the material published by WikiLeaks? It is often claimed that this material is already known – but we might ask, known
to whom? There are multiple levels of information asymmetry. Second, what does the varied response to WikiLeaks tell us about the nature of power and sovereignty?

WikiLeaks is paradox. It is in pretty poor shape. The founding editor Julian Assange faces accusations of sexual assault and as of May 2012 he had not been formally charged. Within WikiLeaks there has been much dissent, with former Assange deputy Daniel Domscheit-Berg acrimoniously leaving to found OpenLeaks after accusing WikiLeaks of losing its way and betraying its remit. (Founded in January 2011, OpenLeaks has yet to publish anything). Since December 2010 there has been a blockade against WikiLeaks by banks, credit card companies and PayPal, which prevents it from receiving donations. In 2011 it was revealed that three companies, HBGary Federal, Palantir, and Berico, known as Team Themis, had put together plans to target WikiLeaks, left-wing activists and the journalist Glenn Greenwald of Salon.com at the request of the Bank of America. The plan was revealed when Anonymous hacked and published internal e-mails between the companies. Berico and Palantir then severed connections with HBGary Federal, and its CEO Aaron Barr resigned. (In February 2012 HBGary was bought by ManTech International, a defence and intelligence contractor).

If WikiLeaks is impoverished and attacked, it is because it is part of an epistemic shift in sovereignty. This is by no means to be understood as a central government trying to suppress challenges, or of the state in crisis. Rather, it is the state itself that is outsourcing and spinning off its capabilities in an unprecedented manner, especially in the defence and intelligence sectors. Paradoxically, WikiLeaks is part of this outsourcing, and the insecurities of it playing in this larger game reveal much about how it is supposed to be played – and who can play it and profit from it. Palantir received $2 million from the CIA’s technology venture capital company In-Q-Tel and now has $300 million in funding to provide analytic capabilities historically done by the National Security Agency (NSA). Its links to the defence and intelligence community (IC) are strong. It recently hired former National Counterterrorism Center director Michael Leiter. As a military-intelligence contractor, it and the many other similar contractors get security clearances and access to the government’s most guarded secrets. Indeed, of the 1.4 million people with the nation’s highest clearance (Top Secret) at last half a million are held by contractors.

Let’s examine the two questions posed above; whether WikiLeaks is merely providing information that is already known, and second what the responses to WikiLeaks might tell us about contemporary sovereignty.

Certainly, the question of whether something is known is complex, and there are multiple levels of information asymmetry involved. Something can be known to a few (such as area experts), but not generally known to the public. For example, when WikiLeaks published the State Department cables it was sometimes argued that these were trivial observations, gathered at
embassy cocktail parties. Yet we did learn that the USA carried out rendition prior to 9/11, that in violation of international law the US sought “biometric data” on senior UN officials, and more about the pressure the US receives from Saudi Arabia to depose Iran’s leadership.

It is true that the cables themselves were classified at relatively low levels (only 6.2 percent were classified as “Secret” and 53 percent were “Unclassified,” none were “Top Secret”). However, it is this very differential in information and knowledge that is at stake in whistle-blowing, or bringing to public light activities and facts not known more widely. In the case of the Pentagon Papers for example (which were Top Secret) the leaker, Daniel Ellsberg, did so because he had evidence that successive administrations were lying to the public. The Pentagon Papers, said Ellsberg, need not have been classified at all because they contained no national security implications and were only classified for political reasons.

In today’s Obama administration, which ran on a promise of governmental transparency but has failed to deliver, whistle-blowing remains of critical importance. In this regard, alongside WikiLeaks we may acknowledge the case of Thomas Drake, a whistle-blower who worked for the NSA. Drake, who provided unclassified information to a reporter regarding billion-dollar inefficiency and waste at the NSA, was charged by the government under the Espionage Act for retaining classified documents, but the case dissolved in 2011. Notably, after the case in a very rare move, the NSA and the Department of Justice had a formal complaint filed by the former Bush administration classification official that the allegedly retained documents should not have been classified in the first place. There is no doubt then that whistle-blowing activities are part of this ongoing struggle between access to and continual over-classification of documents. According to official figures, over 77 million documents were classified in 2011, a 40 percent increase year-on-year.

Even when something is published by WikiLeaks, and presumptively known to all, this does not mean that the information can be utilised. In 2011 for example WikiLeaks released hundreds of files about prisoners being held in the Guantánamo prison. Compiled by the Joint Task Force at Guantánamo (JTF GTMO) and known as Detainee Assessment Briefs (DABs) they provided new information on almost all the 779 prisoners held there since the prison opened. This has created some novel legal implications because the attorneys representing Guantánamo prisoners have been enjoined by the government from using information in the DABs since they remain classified documents. Although the government can use the DABs against the detainees (they contain what defence lawyers contend is unreliable information extracted under torture, duress or coercion) and the documents are published globally, the defence lawyers initially had no access to them, nor can they discuss them. The government later allowed defence lawyers to view them on a non-government computer but not to download
or transport them. Defence lawyers have now filed a motion arguing that the
government has no legal right to restrict access since the lawyers are
only prevented by Nondisclosure Agreement (NDA) and Protective Order
from viewing classified material supplied by the government, and that these
documents come from an independent source (that is, WikiLeaks and the
original leaker) and are publicly accessible.

These examples show that WikiLeaks is part of the ever-ongoing contest
over control and access to information that we see in copyright disputes,
geographies of knowledge, the digital divide, censorship, counter-censorship
and many other related issues. The question of what is “known” is certainly
a political question.

What can WikiLeaks tell us about power, government and sovereignty?
It might be interesting to get beyond the usual dichotomies here. As noted
by a referee on an earlier draft, these tend to see WikiLeaks as powerful
threat to sovereignty. But what if, instead of being opposed, we see them as
part of the same trend, that is, the outsourcing of government beyond the
state? As government spins off, we can then see that WikiLeaks (and other
democratic uses of social media such as Twitter, Facebook, etc.) is part of
the struggle to pick up the pieces.

Matt Hannah’s concept of “epistemic sovereignty” is useful in this light,
and we can use it to place WikiLeaks into a wider historical context. Epistemic
sovereignty refers to the rights that authorities such as the state can
assert over information and knowledge, typically in an asymmetric fashion.
These rights can be (to a certain extent) resisted. Some historical examples
will illustrate this point.

Government domestic dataveillance takes at least two forms: open
data collection, for example the census and closed collection, for exam-
ple signals intelligence (SIGINT) of the NSA which collects all e-mails,
texts and phone calls. There is a big difference. Closed (classified) infor-
mation collection has no public oversight, no public budgets, and no public
descriptions of programmes and activities. Despite constitutional protections
it can be subject to political pressures. President Kennedy signed off on
FBI surveillance of Martin Luther King (partly because J. Edgar Hoover had
evidence of the president’s extra-marital affairs). These COINTELPRO activi-
ties went unknown for fifteen years and included illegal wiretaps and other
shady activities known as the “dirty tricks.” Negative public response to the
COINTELPRO programme, as well as Nixon’s Watergate illegalities, led to the
Church Committee Report of 1975 restraining covert surveillance. The Church
Committee also established the FISA (Foreign Intelligence Surveillance Act,
1978) Court, which oversees government requests for surveillance on foreign
powers or agents.

There are several issues worth highlighting here. Given that the right
of government to perform dataveillance is almost universally conceded
(Hannah’s book is about a rare example where a government census was
successfully boycotted) the question that next arises is that of oversight and transparency. The FISA Court provides an important mechanism in ensuring that warrants, based on probable cause, are used in surveillance. What WikiLeaks usefully reminds us is not that we should be opposed to dataveillance in principle (I cannot see how any individual or social organisation can operate without collecting information, that is, without knowing things), but that it should be bi-directional and not asymmetric. Currently, we are very far from this, and the little oversight we have can break down. (The New York Times revealed in 2005 that after 9/11, the Bush administration and the NSA carried out a series of warrantless wiretaps.) This is not an argument for the efficacy of pure knowledge (that if we just know something everything will be alright). Knowledge is struggled over as I discuss above.

The second issue lies in the outsourcing of government. It is now estimated that there are two government contractors for every government employee. Information available from USASpending.gov (an oversight database) reveals that no fewer than 50,000 contractors received money from the Department of Defense between 2000 and 2012. These include large military contractors such as Lockheed-Martin (recipient of $286 billion in DOD funding) but also companies such as CACI, which provided interrogators for the Abu Ghraib prison and were revealed in 2004 to have substantially mistreated prisoners (recipient of $12.5 billion). WikiLeaks has covered this area on a couple of occasions, including the Stratfor e-mails (hacked by Anonymous) known as the "Global Intelligence Files" and another project known as "The Spyfiles" which contain documents from various intelligence contractors.

In the geography sector similar developments have occurred. In 2010, two spy satellite companies, GeoEye and Digital Globe, were awarded a ten-year contract by the National Geospatial-Intelligence Agency (NGA) worth $7.3 billion to supply the government with imagery (an activity traditionally performed by the secretive National Reconnaissance Office). However, very little is known about the contract, the imagery to be delivered and whether defence cutbacks will negatively affect the companies and their own subcontractors.

An inescapable conclusion is not that sovereignty is being weakened or challenged, but rather that it is being outsourced and redeployed beyond the state. This is cause for concern, because there is less accountability in such arrangements, not to mention that contractors can work outside the military chain of command (for example, contractors are used to operate the CIA’s drone system). WikiLeaks is a minor but symbolically powerful figure operating among governmental outsourcing and acting as an outlet for whistle-blowers and providing oversight and transparency. Until (at a minimum) there is true participatory bi-directional dataveillance, we must continue to value WikiLeaks for these efforts.
7. M. Hannah, *Dark Territory in the Information Age* (Farnham, UK: Ashgate 2010).
10. A spreadsheet is available from the author, or visit USAspending.gov and perform a filtered search on the Department of Defense.
11. Lockheed-Martin constructs the GeoEye satellites. Furthermore, the NGA issued the contracts, known as the “Enhanced View” programme, without securing a cash-guaranteed letter of credit from the company. In the event of a problem such as the recent attempts by each company to buy each other, or a failure to launch, the government would not be reimbursed.
18. Ibid., p. 146.
22. Ibid., p. 76.
23. Ibid., p. 78, emphasis added.
24. Ibid., p. 79.
27. Ibid.
29. Ibid.
45. Morozov (note 41).
53. Ibid.

59. Agamben (note 56); Butler (note 58) p. 56.


68. Hyndman (note 62).


71. Ibid.


75. B. Anderson (note 66).


77. Lee and Sexton (note 56).