WikiLeaks and the problem of anonymity: A network control perspective

*This is the accepted version of the article published in the May, 2013 edition of *Media, Culture and Society* 35 (4): 487 - 503.

Between July and November of 2010, WikiLeaks, a shoestring operation dedicated to disseminating confidential information, made available thousands of documents from a trove of half a million confidential U.S. military and diplomatic papers. Subsequently, restrictive measures were imposed to prevent the organization from releasing further information deemed damaging to the United States. Academics, journalists and activists criticized the United States because of the incongruity between these apparent retaliations and Secretary of State Hillary Rodham Clinton's criticism of authoritarian state suppression of Internet freedom in February 2010. This article picks up on that line of commentary that viewed the United States as acting like all states – authoritarian or otherwise - in the international system, and seeks to develop the concept of 'network control' to help us understand state objectives and the challenges they face in securing control over the global communications infrastructure.

Control over territory is the state's domain and it is fully realized when legal claims to sovereignty are backed up by economic and/or military might. Global communications networks have long posed a challenge to territorial control and the WikiLeaks case is but one contemporary example. The case highlights anonymity as the crucial technological obstacle in the 21st century to control over the global Internet. While the public telephone network was designed to identify the source of telephone messages and unidentified radio communications were outlawed early on, anonymity is the norm on the Internet. Individuals can express their views and even take action while concealing their real-world identities.

This article offers an analytical framework for historically specific analysis and demonstrates its usefulness by investigating the territory-technology nexus of network control in the WikiLeaks case. From a network control perspective, the battle is not so much for 'the soul of the networked fourth estate' as it is for the future of anonymity on the Internet (Benkler, 2011a: 311). From the perspective of the security establishment, the free speech aspect is tangential; the publication of sensitive information is just one of the many undesirable consequences of anonymity. In the long run, I submit, governments face the challenge of forging a consensus on identification as the norm governing the operation of the Internet while retaining their own ability to act anonymously − a key to geopolitical advantage in cyberwar.

The first section of the article applies the concept of network control to the Internet and analyzes WikiLeaks as an example of 'digitally correct hacktivism,' while the second section interprets the extrajudicial methods used by the U.S. government as examples of the tactical level of territorial control. The last section then shifts to the structural level to trace the contours of policy alternatives that, if realized, will affect the future of anonymity on the Internet.

Network control

In the wake of the publication of the State Department cables, newspaper articles, blogs and scholarly publications considered questions ranging from the future of diplomacy to the legality of WikiLeaks' actions under the First Amendment. It quickly became apparent that the problem of extending state control over the Internet, first raised in the 1990s, still had considerable current relevance. The *New York Times*, for example, invited commentary on the WikiLeaks case

with the following question: 'Even if WikiLeaks can be controlled, will others be motivated to flood the world with spilled secrets?'

The answer was a resounding 'yes.' 'Indestructible publishing,' in the words of the editor of the *Guardian*, or 'radical transparency,' in hacktivist parlance, was here to stay (Rusbridger, 2011; Sifry, 2011: 20). While organizational explanations such as the influence of hacktivism – online direct action rooted in the anti-globalization movement − received some attention, no factor was cited more widely than the unique technological features of the Internet (Jordan and Taylor, 2004; Ludlow, 2010; Benkler, 2011b; Sifry, 2011). WikiLeaks is so difficult to stop, Yochai Benkler argues, because it takes advantage of 'core modes of networked resilience,' such as redundancy and duplication (2011a: 350). Anyone who wants to remove content from WikiLeaks 'would have to practically dismantle the Internet itself' (Khatchadourian, 2010: 40).

The emphasis of these arguments on the robustness of the public Internet is reminiscent of late 1990s predictions about the challenge posed by electronically integrated global networks to state control (Johnson and Post, 1996; Neuman et. al., 1997). More recently, the scholarly bible of the early Clinton State Department suggested that the state should adjust itself to a 'networked world,' which exists 'above the state, below the state and through the state' (Slaughter, 2009: 95). In a sociological analysis that explicitly decenters the state, Manuel Castells (2009) similarly posits a discontinuous break with the past – the existence of a 'network society' –and seeks to understand how power operates via networks whose 'flexibility, scalability and survivability' have made them central to social organization (23).

By the turn of the 21st century, however, the territorialization of the Internet had begun, serving as the latest chapter in a half-a-century long U.S. effort to maintain control over world communications (Hills, 2007). Yet, what 'network control' actually means remains inadequately

understood. Definitions range from 'the power to decide how the communication network will be used and by whom,' a broad approach on the domestic level that is compatible with either property rights or state sovereignty and the instrumental approach of the literature on information warfare that identifies the concept with the Department of Defense's (DoD) goal of securing an uninterrupted flow of information and denying the same to its adversaries (Bar and Sandvig, 2008: 533; Clarke and Knake, 2010).

Just how governments rule the net and the extent to which they would manage to wrest control from private, non-governmental organizations or change the network's original free speech architecture has been subject to debate (Goldsmith and Wu, 2008; Lessig, 2006; Mueller, 2010). Despite an apparent interest in countervailing forces, as manifest in Lessig's (2006) view of a competition between the architecture of cyberspace as a regulator and the law's regulatory regime and Goldsmith and Wu's attention to the 'arms race' between geography-specifying and geography-defeating technologies, legal scholars have emphasized effective, rather than perfect, regulation (2008: x). When they argue that the regulation of a small number of 'intermediaries' is sufficient to shape the behavior of end users, legal scholars have the average user in mind (68). However, if we want to understand the leverage different parties wield, we must study serious conflict with a framework that better accommodates skilled and/or powerful opponents.

This article defines network control as decision-making ability over *territory*, *capital* and *technology* through which one party secures an uninterrupted flow of information while denying that ability to its opponent. The intersections of the three sites are the most promising for analysis because they act as clash points where different types of control collide. The definition combines the purpose of control identified by the military with three sites of control that provide countervailing influence and two levels of control -- tactical and structural – in order to retain the

analytical focus of the information warfare literature on the struggle for control while moving beyond its instrumentality. In particular, the inclusion of the state's objective links this framework to a concept with centuries-long pedigree – 'command of the seas' --in order to facilitate historical comparisons.

The tactical level of network control involves the struggle over relational power, where one party gets the other one to do what it wants via *existing* tools available in a given conflict, while the structural level refers to the ability to determine the rules of the game, including general policy principles, values embedded in technologies and the very definition of participants in discourse (Strange, 1997; Jordan and Taylor, 2004). In the context of global communications, for example, the instrumental use of the communications infrastructure in wartime exemplifies the tactical level, while the ongoing controversy around the location of Internet root servers belongs to the structural level.

To analyze the WikiLeaks case from a network control perspective means to take hackivists' appropriations of military logics seriously. Terms like 'troops,' 'blockade,' and 'thermonuclear device' point to their involvement in a struggle for network control, with goals -- maintaining an uninterrupted flow of information and denying the same to one's opponent -- similar to those of states engaging in information warfare. Since these activist groups can challenge state power largely because of their technological expertise, the analysis below contributes to our understanding of the territory-technology nexus of network control.

Anonymity, defined as a state of disconnect between one's self and one's identifiers, is at the center of the clash between territorial control and control over technology on the Internet (Kerr, 2007: 18). To be fully anonymous, sociologist Gary Marx argues, means that a person cannot be identified according to any of his seven dimensions of 'identity knowledge,' including

legal name and 'locatability' (1999: 100). Since locatability includes the ability to block and apprehend, it dovetails with the legal argument about the importance of geographic identity to making behavior 'regulable' on the Internet (Lessig, 2006: 59).

Both legal name and locatability are necessary for states acting on the tactical level of network control as the provisions of the European Convention on Cybercrime indicate. According to this treaty, which the United States relies on for apprehending perpetrators of DDoS (distributed denial of service) attacks, a state can exercise jurisdiction over individuals if they are citizens of the given state or have used the territory of that state for criminal activity (Sklerov, 2010). The WikiLeaks case presents a challenge to territorial control because of the anonymity of online submissions as well as the anonymity of DDoS protest attacks coordinated on behalf of WikiLeaks by a group of hackers who call themselves Anonymous. Insofar as circumventing locatability is the purpose of anonymous communication, members of Anonymous seek to avoid prosecution by the same measures analyzed below that WikiLeaks uses to ensure transmission security.

The anonymity of online submission and online protest

WikiLeaks was founded in 2006 with the express purpose of developing 'an uncensorable system for untraceable mass document leaking and public analysis' (Khatchadourian, 2010: 40). Untraceable leaking was made possible by the single most unique feature of the website: its electronic drop-box technology that allows leakers to submit documents anonymously (Morozov,

2010). This technology is best understood as the material embodiment of digitally correct hacktivism and represents an attempt at the applications layer of the Internet to amplify the anonymous orientation of the network's control software.

Figure 1 provides examples for structural-level sites of conflict and tactical-level tools to deal with them for each of the three layers of the Internet: the physical infrastructure, control software and communications applications (Bar and Sandvig, 2008). Not all layers of the Internet are affected in any given conflict. The anonymous orientation of the Internet, for example, was the result of structural-level decisions about the control software -- the TCP/IP transmission protocol --where network configuration was defined, while the physical layer was not affected. Moreover, values built into one layer of the Internet do not determine the values of other layers. WikiLeaks' focus on strong, cryptographic anonymity as a norm for online participation amplifies the values embedded in the network's control software, while Facebook's requirement of identification negates those values via corporate policy (*see also* Krotoski, 2011). Most of the WikiLeaks controversy takes place on the level of communications applications with implications for the software layer.

Figure 1.

	level of network control		
		structural	**tactical**
technological layers of the Internet	**physical infrastructure**	location of cables, root servers	DDoS, kinetic attack
	control software	values built into the transmission protocol	IP address spoofing, onion routing, geo-location technologies
	communications applications	norms for online participation	denying web hosting and name server services, DDoS

Insofar as technologies embody social values, rather than neutral forces, they may hide or reveal various forms of identity knowledge (Jordan and Taylor, 2004; *cf.* Clarke and Knake,

2010). Although a historical account of the structural level -- how anonymity became embedded in the network -- is yet to be written, it appears to be more of a case of anonymity by neglect. Simplicity was a core value for the framers of the Internet and their primary objective for the network was to deliver packets of data (Lessig, 2006). Who sent that data and what their intentions were was hardly considered; after all, trusted people in secure locations ran all the sixty or so computers that were initially connected. '[I]f anything bad got on the network,' relates national security expert Richard Clarke, 'it wouldn't be hard to get it off and to identify who had put it there' (Clarke and Knake, 2010: 84). The TCP/IP transmission protocol included no mechanism for managing personal identity, an arrangement that remained in place after the Internet was commercialized.

It is not that packets contain no information about their origins: when we send a message over the Internet, packets are identified by a header used for routing that reveals their source and destination to the network, making it easy to trace transactions. Rather, anonymity slips in because such identification is not enforced and the source of packets can be falsified (Lessig, 2006). Because of the lower priority assigned to security and identity management at the time of the network's creation, DoD now identifies the Internet as 'an offense-dominant environment' (Lynn, 2010: 99). It is nearly impossible to identify the source of a DDoS attack and retaliate. Anonymity hinders targeting.

WikiLeaks' emphasis on anonymity derives from the intellectual origin of the organization in hacktivist culture. In a study preceding the emergence of WikiLeaks, Tim Jordan and Paul Taylor (2004) identify two strands of the social movement: mass action hacktivism and digitally correct hacktivism. Mass action hacktivists such as Anonymous turn to the Internet for a virtual version of radical protest, using blockades, strikes and civil disobedience, while digitally

correct hacktivists pursue political resistance on the structural level. Anonymous' use of communication as action in the form of DDoS attacks -- high-volume requests for information intended to overload, and thus temporarily disable, computers --is confined to the tactical level of network control. By contrast, digitally correct hacktivists act on the structural level as participants in 'the battle over the technical infrastructure' where the winner gets to decide the values that are embedded within the network (102).

The central value that digitally correct hacktivists promote is the right to information as a human right. WikiLeaks, in particular, facilitates the uninterrupted flow of confidential government documents by ensuring that they get on the Internet. Anonymity is essential to even out the asymmetrical flow of information between the government and the public: information can only be free if those communicating do not fear reprisals.

What makes WikiLeaks controversial is its global twist on the whistleblower logic. Unlike mainstream journalism, which publishes leaks by national elites as part of a complex information game, WikiLeaks is a global organization which seeks to democratize leaking and extend the reach of the leaked information worldwide (*see also* Shirky, 2010b). The group has no headquarters or capital: its core team of five investigators pays their expenses from donations (Guilliatt, 2009; Khatchadourian, 2010). By rejecting such collective ties as race, nation and religion, just as the Hacker Manifesto did in 1986, WikiLeaks presents itself as a truly independent media organization (Ludlow, 2010).

The key to the dissemination of information WikiLeaks considers to be 'public' -- confidential government documents -- is reliable storage, while the key to the protection of information WikiLeaks holds confidential -- the names and locations of activists and sources -- is

secure transmission. On the tactical level of network control, WikiLeaks has used the geography-defeating potential of the Internet to meet both of these challenges.

Much like the multinational corporation (MNC) in search of cheaper raw materials or labor, WikiLeaks has shopped for the most favorable legal climate for reliable storage. WikiLeaks files are safeguarded by 'jurisdictional arbitrage,' i.e. exploiting the discrepancies in legal systems, and by the principle of redundancy (Benkler, 2011a: 347). The website is hosted on an underground server farm repurposed from a single-entrance nuclear bunker from the Cold War (Greenberg, 2012). If the physical site is a fort, its location in Stockholm is selected for the superior protection for free speech provided by Swedish law which makes it a criminal offence to breach the anonymity of journalists' sources (Khatchadourian, 2010: 48; Guilliatt, 2009).

Redundancy is manifest in the decision to store content on more than twenty servers around the world and using hundreds of domain names to provide access to the files (Khatchadourian, 2010). Even though a website would be available on the Internet without a plain language phrase to direct one to its numeric IP (Internet Protocol) address, the public dissemination of information would suffer without this convenience. Redundancy in servers and domain names ensures the uninterrupted flow of information in the 21st century much as it did in the earliest days of submarine cables when alternate routes were put in place to carry traffic in case a vital route was disabled (Winkler, 2009).

By according undue importance to storage, accounts sanguine about the continuation of 'indestructible publishing' miss the importance of transmission security. It matters little that WikiLeaks can make available existing content at hundreds of sites if it can't get new submissions. Trust is the key to the undertaking, as Army officials have correctly observed, and anonymity is the key to trust (Horvath, 2008). WikiLeaks had to design a secure system and

convince everybody about its security before it would receive valuable leaks. Otherwise, as a British computer security expert commented early on, 'who would be insane enough to contribute stuff?' (Guilliatt, 2009). When it comes to transmission security, therefore, the website's design and WikiLeaks' use of the geography-defeating features of the Internet both serve the structural goal of anonymity.

WikiLeaks' network of activists and technological network operate on the same principles: those of the security establishment. Since his 1991 arrest as a hacker in Australia, Wikileaks founder Julian Assange is said to have been obsessed with locatability, the identity knowledge that WikiLeaks' drop-box technology would safeguard the most. In their attempt to avoid government surveillance, WikiLeaks activists zigzag across the globe; Assange's physical location, encrypted cell phones and phone numbers and e-mail address constantly change. Members are known only by initials – even deep within the organization, where communication is conducted by encrypted online chat services (Khatchadourian, 2010).

WikiLeaks' website outlines three options for anonymous submission: the encrypted drop-box, the Tor network and the postal network. Although the physical network offers the most security, the combined use of the drop-box and the Tor network is promoted as vastly more secure than any banking network (Submissions, n.d., Khatchadourian, 2010). In contrast to traditional journalism, which works via confidentiality, i.e. a relationship of trust between two parties, the electronic drop-box and the Tor network operate on the principle that 'the best way to keep a secret is not to have it' (Marx, 1999; Assange, 2011). WikiLeaks keeps no records about where a leaker uploads the information from and 'onion routing' erases all indicators about the origins of messages, much like activists change their physical locations to hide their tracks (Submissions, n.d., Khatchadourian, 2010: 49, 46).

Designed in collaboration with the U.S. Navy and used by the Tor network since its introduction in 2001, onion routing is a peer-reviewed anonymity system that strips information about 'the externals' of a message such as its origins, destination, date of transmission and relative size by fragmenting the link between the sender and the receiver. The first parcel of data holding the encryption keys to such externals is bundled in three layers of encryption that Tor relays would peel off like layers of an onion. Thousands of nodes are involved and the last node before the destination replaces the source IP of the previous router with its own IP, so it will be seen as the source of the message (Greenberg, 2012; U.S. Naval Research Lab. (n.d.). Pfc. Bradley Manning, the source of the confidential government documents, allegedly set up a secure file transfer connection via the Tor network between a Verizon Internet address registered to his aunt's home and a secure server associated with PRQ, a Swedish Internet service provider that formerly hosted WikiLeaks' site and electronic drop-box (Nakashima, 2011c).

In the end, the security of WikiLeaks' system − widely reported to be 'beyond legal or cyber attack' – was not compromised (Rusbridger, 2011). After the disclosures discussed below, Manning himself revealed his identity to a former hacker and was reported to the police (Khatchadourian, 2011). The extent to which anonymous transmission itself will be a permanent fixture on the Internet, however, is not only for activist groups to determine. The following two sections analyze the WikiLeaks incident as a chapter in state efforts to extend territorial control over the Internet on the tactical and the structural levels.

The attack on WikiLeaks: the tactical level

If the anxiety over the Iraq and Afghanistan files is any guidance, when WikiLeaks published the first batch of diplomatic cables, policymakers' Blackberries were overheating with a 'fusillade of cabinet-level e-mail' (Keller, 2011). Within a week of the initial publication, five related developments made it difficult for WikiLeaks to continue the dissemination of its archive: 1) a large-scale DDoS attack, which led to 2) its domain-name provider dropping it; 3) its web hosting service, Amazon.com, denying access; 4) credit card companies and banks no longer processing donations to the organization; and 5) Interpol seeking Assange for questioning in connection with rape charges in Sweden (Benkler, 2011a). This section compares the American and the French governments' efforts at territorial control over Yahoo! and WikiLeaks, respectively, and argues that American policymakers' recourse to extrajudicial methods on the tactical level is best explained by the differences between these two global organizations.

The extent, if any, of policymakers' interference with the operations of the WikiLeaks site is for historical research to uncover. The State Department did inform the news media that the United States was trying to track where WikiLeaks was publishing from, but both the diplomats and the Pentagon denied obstructing the operations of the site (Keyes and Ure, 2010). The official line was received with skepticism: the developments described above were identified as 'extrajudicial pressure,' however diffuse and uncoordinated, whose effect amounted to 'a multi-system attack' on WikiLeaks (Benkler, 2011a: 330; Benkler, 2011b, pp. 154, 157; Shirky, 2010a).

Indeed, DoD had already considered a confidential report from the Army Counterintelligence Center, published by WikiLeaks and analyzed below, that identified the group as an online reference for America's enemies and a threat to the Army (Horvath, 2008, pp. 1-2). In early 2010, the department pressured WikiLeaks activists to remove the Afghanistan

documents from the site, threatening 'to compel them to do the right thing' (Batty, 2010). The 2011 resignation of a State Department spokesman for criticizing DoD's treatment of Manning as 'ridiculous and counterproductive and stupid' indicates internal disagreement about how best to handle the case (Pilkington, 2011).

The United States was in the hot seat this time, but governments all around the world were watching, the same way they had watched France in the early 2000s, when it sought to extend its national jurisdiction into cyberspace (Goldsmith and Wu, 2008). Cablegate prompted gleeful questions from the Russian prime minister as to whether the United States was a 'full-fledged democracy,' given its reaction to such glasnost, but reaction abroad was far from jubilant (Erlanger, 2010). Foreign governments unanimously reaffirmed the necessity of secrecy for diplomacy (Neuman, 2010). While other areas of Internet governance confer geopolitical advantage and thus divide states, safeguarding diplomatic secrets is in the interest of all states. Thus, the lawsuit in France against Yahoo! serves as a context for the WikiLeaks controversy because it was the first high-profile case for extending territorial control over the global Internet.

In the late 1990s, Yahoo!, a fledgling multinational corporation expanding from a country with First Amendment protections for hate speech, faced the court system in a powerful industrialized state where hate speech was outlawed. The case raised the problem of offering Nazi memorabilia, including copies of *Mein Kampf*, on the Internet to citizens of states where such products were illegal. Yahoo! did not operate the auction site where the memorabilia was traded, much as Amazon did not run WikiLeaks, but it did go to bat for the party that ran the auction site. Yahoo! argued that imposing national regulation on the Internet was both impossible and undesirable. Executives claimed that they were unable to tell where users accessed its sites from and that subjecting the company to French law would have ripple effects

all over the world. A 'race to the bottom' would result where the rules for the global communications infrastructure would be set by the most restrictive national system in each area of the law (Goldsmith and Wu, 2008: 6).

Identification via geo-location technology played a prominent role in the case. Witnesses demonstrated that Yahoo! could, in fact, tell where people accessed its site from and had actively sought this knowledge to target them with advertising. The French court rejected the company's overblown pronouncements and ordered it to make the Nazi material unavailable to French citizens or face a $13,000 per day fine. Capital's brief challenge to territorial control ended in Yahoo!'s decision to remove all Nazi material from its site (Goldsmith and Wu, 2008). The French state exercised control over the Internet indirectly by linking Yahoo! users to French territory and by holding Yahoo!'s assets on French soil as collateral for the fine. The case marked the end of the widespread belief that the Internet could not be regulated.

By contrast, the immediate goal of the U.S. government was to remove the confidential files from WikiLeaks' website, as evidenced by DoD's request for the removal of the Afghan files and the administration's interest in prosecuting WikiLeaks under the Espionage Act. The French government's solution in the Yahoo! case -- denying undesirable content to French citizens -- was employed as a stop-gap measure in the United States, as we see from the U.S. government's continued classification of the information published by WikiLeaks as well as initiatives to bar federal employees from accessing the material (Benkler, 2011a; Air Force tries, 2010).

Four of the five aspects of the attack on WikiLeaks targeted the material underpinnings of the site's operations and rested on the state's control over its territory. Although the source of the DDoS attack on WikiLeaks' domain name provider is unclear, such attacks are notoriously

difficult to attribute. According to Benkler, the scale and sophistication of the attack points to a state sponsor (2011a). Indeed, the trend in Internet censorship, i.e. 'second generation blocking,' favors offensive means of filtering access to controversial sites such as DDoS attacks on servers hosting information (Deibert and Rohozinski: 2010: 27).

While control over territory and control over capital clashed briefly in the *Yahoo!* case, Amazon.com and major credit card companies were quick to comply with a November 27, 2010 letter from the Department of State that included a 'legally insufficient but publicly salient insinuation of illegality' (Benkler, 2011b: 155-156). When American companies denied name server and web hosting services, WikiLeaks was no longer able to operate on American territory. In Benkler's assessment, the partnership between the state and large corporations enabled the government 'to achieve extra-legally much more than law would have allowed the state to do by itself' (2011a: 342). In financial operations as in technical services, therefore, the state exercised control over the global infrastructure indirectly, by putting pressure on the intermediaries that manage the technology. The 'banking blockade' has had a detrimental effect: WikiLeaks lost 80-90 per cent of its revenue in the first two months (Benkler, 2011b: 158).

Such extrajudicial methods may have had as much to do with policymakers' perceptions of WikiLeaks as with a desire to get around the First Amendment. WikiLeaks appeared to be a decentralized postindustrial organization, more like Al-Qaeda than Yahoo! If multinational corporations are often described as 'stateless,' WikiLeaks is characterized as a 'a stateless and penniless pariah' (Knickerbocker, 2011). The lack of profit motive or any assets to speak of is a prominent trope both on the organization's website and in the mainstream media. In the latter, however, hacktivism is articulated to terrorism (Benkler, 2011a). '[E]ven when the attacker is identified,' notes Deputy Secretary of Defense William Lynn in connection with DDoS attacks, '

if it is a nonstate actor, such as a terrorist group, it may have no assets against which the United States can retaliate' (Lynn, 2010: 99). France was able to assert territorial control over Yahoo! because the fear of expropriation attendant on assets in a given country makes MNCs vulnerable to state power. By contrast, states' lack of leverage with regard to diffuse non-state actors is a common theme in policy discourse.

If the exercise of territorial control hinged on the real-world underpinnings of WikiLeaks' operations, the last aspect of the 'multi-system attack' concerns the body of the activist. An organization with no capital or assets runs on individual commitment and individuals are vulnerable to state power via their physical persons (Goldsmith and Wu, 2008). In the past, criminal prosecution was difficult, as Australian authorities found out, because of 'WikiLeaks' opaque structure' (Guilliatt, 2009). In 2010, however, Assange became internationally known and getting possession of his person became crucial, albeit challenging because he was not an American citizen, nor did WikiLeaks' drop-box operate on American territory. An important thrust of the Army hearings on Manning was whether Assange influenced the soldier's decision to leak the U.S. documents or provided technical assistance, which, if proven, would help U.S. authorities distinguish WikiLeaks from a media organization (Nakashima and Tate, 2011; Dorling, 2011). Were this attempt successful, charges of criminal conspiracy could be in the offing, which could bring Assange under American jurisdiction.

Because WikiLeaks operated publicly, the push for territorial control on the tactical level was not linked to anonymity. In fact, possession of WikiLeaks activists' legal names enabled American prosecutors to subpoena their Twitter accounts, demanding such personal information as addresses, screen names, telephone numbers as well as credit card and bank account numbers (Shane and Burns, 2011). By contrast, the effort to apprehend Anonymous members for their

involvement in the DDoS attacks against Visa, MasterCard and PayPal depended on revealing their identities and linking their computer use to the attacks. Anonymous members in the United States, the United Kingdom and Holland were arrested for their involvement in the attacks (Sengupta, 2011).

Whether motivated by preventing access to the leaked materials or by the desire to restrict the dissemination of leaked documents to the responsible press, the attack on WikiLeaks has been evaluated as a failure. Based on the interest in duplicating the site as well as copycat sites such as BrusselsLeaks and RuLeaks, distributed leaking is expected to stay (Benkler, 2011a). However, financial difficulties may undermine the likes of such sites entirely. Like any other business on the web, WikiLeaks had been struggling to find a 'funding model' since its inception. Both subscriptions and the selling of documents at auction were considered as a revenue source at one point along with the transformation of the site into a clearinghouse for leaked information: a common carrier model for leaks (Khatchadourian, 2010: 51; (Nakashima, 2011a). This latter model is more likely to find funding, but the activist edge involved in selecting the materials to publish and the commentary around it would disappear.

Second, the test of WikiLeaks' survival is new submissions, but the link to submissions on the website was removed in 2010 with the promise that it would be back after the site is reengineered to be more user-friendly and secure. Publication of sensitive official documents has since slowed to a trickle and much of these have been obtained via Anonymous, an organization WikiLeaks used to distinguish itself from, rather than from aspiring whistleblowers (Palmer, 2012). In the meantime, developments on the structural level of network control may signal an overhaul of the network environment for leaking.

The attack on WikiLeaks: the structural level

In contrast to the short-term objective of denying access to the confidential files already published, the long-term goal of the state is to discourage anonymous uses of the Internet by unauthorized parties. The military mindset, captured in the concept of network control, is central to the state's objectives with regard to strategic communications technologies. The focus of the 2008 Army Counterintelligence Report on anonymous submission, this section argues, is part and parcel of the military establishment's concern with the security flaws of the Internet. The U.S. government as a whole, however, is ambivalent about anonymity on the Internet.

Unlike the steps aimed at hindering the publisher, the 2008 report prepared by the U.S. Army Counterintelligence Center recommended intimidating future whistleblowers as way to prevent further disclosures.

> Wikileaks.org uses trust as a center of gravity by assuring insiders, leakers, and whistleblowers who pass information to Wikileaks.org …that they will remain anonymous. The identification, exposure, or termination of employment of or legal actions against current or former insiders, leakers, or whistleblowers could damage or destroy this center of gravity and deter others…. (Horvath, 2008: 3)

The key to intimidating future whistleblowers is identification of current ones, which is necessary for all organizational and legal action against them.

The author of the report is clearly impressed with the software programs WikiLeaks activists wrote to extract information from the mountain of dry data they had received, but not more impressed than with the technical sophistication required to provide a secure operating environment for whistleblowers (Horvath, 2008). Transmission security is expected to improve, Michael D. Horvath warns, 'as new technology, the technical skills of current members, or new funding sources allow' (2008: 18). The government must act quickly while it is technically feasible to identify and trace whistleblowers through cyber investigations and advanced cyber tools (6). Assange regarded this report as a declaration of war (Khatchadourian, 2010).

In the course of the WikiLeaks controversy, anonymous submission and anonymous action in the form of DDoS attacks called attention to what's long been a sore point for the security establishment: the widespread availability of military-grade security for Internet communications. Currently, numerous studies are being conducted to perfect 'IP traceback' methods that could reliably determine the origin of a packet on the Internet. The most common justification for tracebacks is to counter DDoS attacks. However, source identification is not a technical problem. If all Internet Service Providers implemented mechanisms to prevent IP address spoofing, the problem would be solved (Park and Lee, 2000). In the absence of such a corporate decision, technical and policy solutions have been contemplated.

On the international level, national security experts from the United States and China have sought to reduce perceived vulnerabilities by proposing standards for source identification in an IP traceback working group under the auspices of the International Telecommunication Union (ITU). The 2008 proposal prompted concern among activists that server operators would be arrested if they do not log every packet that goes through their service (McCullogh, 2008). Source identification recently resurfaced during preparations to revise the ITU's regulations at

the aborted World Conference on International Telecommunications in late 2012. Under a cybersecurity proposal discussed in Dubai, member states would have required operating agencies to identify subscribers and ensure 'the appropriate processing, transmission and protection of identification information' in international telecommunication (Council Working Group, 2012).

Domestically, two main alternatives have emerged: a secure military network, set apart from the public Internet, and 'an Internet minus the anonymity' (Ackerman, 2011). In an attempt to find a technological solution, DARPA is funding research aimed at making the Pentagon's basic architecture more secure, with senior DoD officials expressing hope that the United States could 'engineer its way out' of the most problematic vulnerabilities (Lynn, 2010: 106). In the meantime, military strategists have recommended to Congress that the U.S. 're-engineer the Internet to make attribution, geo-location, intelligence analysis and impact assessment -- who did it, from where, why and what was the result -- more manageable' (Singel, 2010).

While reshaping the Internet to fit security requirements may be appealing to the Pentagon, the U.S. government's position is more conflicted. On the one hand, Secretary of State Hillary Clinton lumped together anonymous expression with incitement to violence and hate speech, examples of free expression that no society tolerates, in her 2010 speech on Internet freedom. 'Those who use the internet to recruit terrorists or distribute stolen intellectual property cannot divorce their online actions from their real world identities,' she declared (Clinton, 2010). 'Cannot,' of course, means 'should not' since such a disconnect between one's self and one's identifiers is at the very heart of anonymity. The Department similarly disapproves of the use of the Tor network to reveal confidential government information. In her second speech on Internet freedom, shortly after the State Department cables hit the newsstands, Secretary Clinton drew a

distinction between the WikiLeaks incident, which 'began with an act of theft,' and authoritarian governments' repression of freedom of speech (Clinton, 2011). Stolen government property rhymes with stolen intellectual property – the focus is on ownership rights to information, rather than, say, the appropriate extent of government secrecy.

On the other hand, the State Department supports the use of anonymizing technologies abroad in an effort to he lp activists speak out against repressive governments. 'Circumvention services' like the Tor Project were considered for part of a $30 million set aside to promote Internet freedom and were widely used in the Arab Spring uprisings (Landler, 2011). Given the Pentagon's interest in improving the attribution of DDoS attacks as well as the State Department's interest in supporting approved uses of anonymizing systems, anonymity on the Internet will be central in any discussion about new norms for cyberspace in the 21st century.

Conclusion

Indestructible publishing is here to stay only if anonymity as the norm on the Internet is here to stay. However, scholars have long identified – and generally favored -- a growing trend toward authenticated identity as a condition of Internet membership with some starting to outline the kinds of ID-rich environments we might choose from (Lessig, 2006; Goldsmith and Wu, 2008; Solove, 2007). On the technological level, significant changes are afoot. IPv6 -- the next generation of the Internet protocol --marks each packet with an encryption key, securely identifying the packet's origin. According to Lawrence Lessig, governments are piggybacking on commercial initiatives toward authentication and need a large scale disaster to muster the

political will to effect change (2006). Whether a larger disaster than the WikiLeaks disclosures is necessary remains to be seen.

Rather than adjusting themselves to 'the networked world,' states seek to shape that world to their desires. They are less focused on controlling *content* than on the broader problem of anonymous action, of which content-related transgression is only one example. Anonymity has been subject to restrictions in the past, either at the outset, as in telephony, or after it was identified as a problem, as in radiotelegraphy. For example, the transmission of radio signals in the first decade of the twentieth century was anonymous, but today § 97.119 of the Code of Federal Regulations prohibit unidentified signaling by amateur stations. Thus, it is not a coincidence that the leading court case for anonymous speech only covers written communications (*McIntyre v. Ohio Election Commisssion*, 1995).

The WikiLeaks case became a lightning rod for controversy because it allowed for a vivid clash between those who see anonymity as essential for whistleblowers and those who criticize it for engendering a lack of accountability. Given widespread concerns about online accountability in the context of defamation and the spread of closed environments like Facebook, norms on the Internet may have already shifted toward identification. Yet, any government action on source identification will still require justification, which means that the discursive field will become central to the structural level of network control. Future research will investigate how the contemporary 'offense dominant' environment developed as well as how the U.S. government's arguments fit into the broader debate about the legitimacy of anonymous activity on the Internet.

This article has sought to offer an analytical perspective on network control that allows us to link developments on the tactical level, which has been widely explored, to policy initiatives

on the structural level. Legal scholars' focus on the tactical level stems from their conviction that control over the global infrastructure means controlling the behavior of end users. Where this is the case, the focus on intermediaries is sufficient, especially if intermediaries choose to act as 'pliant targets of regulation' (Lessig, 2006: 68; Goldsmith and Wu, 2008). In the present case, intermediaries have not required source identification by themselves, which may necessitate regulatory action on the structural level.

However, a larger problem should now be apparent: what if state control over the global infrastructure requires control over intermediaries that are not at all the pliant targets that researchers imagine them to be? The assertion about the motivations of large companies – the capital aspect of network control in the framework presented here -- ignores a host of cases where their transnational operations bring them into contact with many states with different levels of power in the international system and differing demands. Only a framework attentive to the structural level of network control and the leverage conveyed by control over capital can guide us through these cases.

Finally, the analytical framework presented above is intended to be broad enough to help us understand the similarities and the differences between the present and the past. It is increasingly common to assert that globalization had a past, but much less common to investigate it. If states have objectives that span centuries, but varying power to realize them, as well as such timeless sources of leverage as control over territory, to what extent, if any, do we live in a 'network society' today? What aspects, if any, of the other sites of network control are truly new? If research reveals more similarities than differences between the present and the past, when did we start living in a network society? The analytical framework presented here does not dispute that there are key differences between the present and the past, but prompts us to

investigate how significant they are. 'Only by recognizing what is recurrent in ongoing transformations of world capitalism,' advises historical sociologist Giovanni Arrighi, can we hope to isolate what is truly new and anomalous in these transformations' (1998: 59).

References

§ 97.119 Station identification. Code of Federal Regulations. http://edocket.access.gpo.gov/cfr_2010/octqtr/pdf/47cfr97.115.pdf

Ackerman, S. (2011, November 7) 'Darpa begs hackers: secure our networks, end 'Season of Darkness,' *Wired.* http://www.wired.com/dangerroom/2011/11/darpa-hackers-cybersecurity/

'Air Force tries to block reality,' (2010, December 16) *USA Today*,17A. Online. Lexis-Nexis.

Arrighi, G. (1998) Globalization and the rise of East Asia,' *International Sociology*. 13(1): 59-77.

Bar, F. and Sandvig, C. (2008) 'US communication policy after convergence,' *Media, Culture and Society*. 30(4): 531-550.

Batty, D. (2010, August 6) 'Pentagon increases pressure on WikiLeaks to return military files,' *Guardian*, 23. Online. Lexis-Nexis.

Benkler, Y. (2011a) 'A free irresponsible press: WikiLeaks and the battle over the soul of the networked fourth estate,' *Harvard Civil Rights and Civil Liberties Law Journal*. 46(2): 311-397.

Benkler, Y. (2011b) 'WikiLeaks and the PROTECT-IP Act: the New Public-Private Threat to the Internet Commons,' *Daedalus*. 140 (4): 154-164.

Castells, M. (2009) *Communication Power*. New York: Oxford University Press.

Clarke, R. and R. K. Knake (2010) *Cyber War*. New York: Ecco.

Clinton, H. (2010, January 21) Remarks on Internet freedom. http://www.state.gov/secretary/rm/2010/01/135519.htm

Clinton, H. (2011, February 15) Internet rights and wrongs. http://www.state.gov/secretary/rm/2011/02/156619.htm

Council Working Group to prepare for the 2012 World Conference on International Telecommunications (2012, June 18). 'Anticipated final draft of the future ITRs' (first revision). http://files.wcitleaks.org/public/T09-CWG.WCIT12-120620-TD-PLEN-0064!R1!MSW-E.pdf

Deibert, R. (2010) 'The post-Cablegate era,' http://www.nytimes.com/roomfordebate/2010/12/09/what-has-wikileaks-started/after-wikileaks-a-new-era

Deibert, R. and R. Rohozinski (2010) 'Risking security: Policies and paradoxes of cyberspace security,' *International Political Sociology*. 4:15-32.

Dorling, P. (December 3, 2011) 'U.S. targets WikiLeaks like no other organization,' *Sidney Morning Herald.* 10. Online. Lexis-Nexis.

Erlanger, S. (2010, December 10) 'Many Europeans find U.S. attacks on WikiLeaks puzzling,' *New York Times*, A12. Online. Lexis-Nexis.

Goldsmith, J. and T. Wu (2008) *Who Controls the Internet?* New York: Oxford University Press.

Greenberg, A. (2012) *This Machine Kills Secrets.* New York: Dutton.

Guilliatt, R. (2009, May 30) 'Searching for Assange,' *The Australian Magazine*. Online. Lexis-Nexis.

Hills, J. (2007) *Telecommunications and Empire.* Urbana, Ill.: University of Illinois Press.

Horvath, M.D. (2008, March 18) *WikiLeaks.org – An online reference to foreign intelligence services, insurgents or terrorist groups?* http://mirror.wikileaks.info/leak/us-intel-wikileaks.pdf

Johnson, D.R. and D. Post (1996) 'Law and borders – the rise of law in cyberspace,' *Stanford Law Review*. 48: 1367-1402.

Jordan, T. and P. A. Taylor (2004) *Hacktivism and Cyberwars.* New York: Routledge.

Julian Assange, the man behind WikiLeaks. (2011, January 26). *60 Minutes.* http://www.cbsnews.com/stories/2011/01/26/60minutes/main7286686.shtml

Keller, B. (2011, January 26) 'Dealing with Assange and the secrets he spilled,' *New York Times*. http://www.nytimes.com/2011/01/30/magazine/30WikiLeaks-t.html

Kerr, I.A. (2007) 'Anonymity,' In: W. G. Staples (ed) *Encyclopedia of Privacy*. Westport, CT: Greenwood Publishing Group, 17-18.

Keyes, C. and L. Ure (2010, December 3) 'U.S. officials deny they are urging technical takedown of WikiLeaks,' http://articles.cnn.com/2010-12-03/politics/WikiLeaks.takedown_1_julian-assange-WikiLeaks-cybercommand

Khatchadourian, R. (2010, June 7) 'No secrets: Julian Assange's mission for total transparency,' *New Yorker*: 40-51.

Khatchadourian, R. (2011, May 20) 'Manning, Assange and the Espionage Act,' http://www.newyorker.com/online/blogs/newsdesk/2011/05/manning-assange-and-the-espionage-act.html

Knickerbocker, B. (2010, December 4) 'WikiLeaks and Julian Assange: Stateless, penniless pariahs?' *Christian Science Monitor*. Online. Lexis-Nexis.

Krotoski, A. (2011) 'WikiLeaks and the new, transparent world order, *Political Quarterly.* 82 (4): 526-530.

Landler, M. (2011, February 15) 'U.S. policy to address Internet freedom,' *New York Times*. A10.

Lessig, L. (2006) *Code: Version 2.0.* New York: Basic Books.

Ludlow, P. (2010, October 4) 'WikiLeaks and Hacktivist Culture,' *Nation*. 25-26.

Lynn, W.J. (2010 September/October) 'Defending a new domain,' *Foreign Affairs*. 89: 97-108.

McCullagh, D. (2008, September 12) 'U.N. agency eyes curbs on Internet anonymity,' http://news.cnet.com/8301-13578_3-10040152-38.html

McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995).

Morozov, E. (2010, December 11) 'Why it's hard to duplicate,' http://www.nytimes.com/roomfordebate/2010/12/09/what-has-wikileaks-started/wikileaks-relationship-with-the-media

Mueller, M. (2010) *Networks and states*. Cambridge, MA: MIT Press.

Nakashima, E. and A. Faiola (2010, October 24) 'Despite latest coup, WikiLeaks faces challenges,' *Washington Post*. A14. Online. Lexis-Nexis.

Nakashima, E. (2011a, April 12) 'U.N. frustrated over Manning,' *Washington Post*. A2. Online. Lexis-Nexis.

Nakashima, E. (2011b, December 9) 'A cyberspy is halted, but not a debate,' *Washington Post*. A1. Online. Lexis-Nexis.

Nakashima, E. (2011c, December 20) 'Prosecutors show Manning link to WikiLeaks, Assange chats,' *Washington Post*. A4. Online. Lexis-Nexis.

Nakashima, E. and J. Tate (2011, December 23) 'Assange role cited in Manning case,' *Washington Post*. A3. Online. Lexis-Nexis.

Neuman, W.R. et. al. (1997) *The Gordian Knot.* Cambridge, MA: MIT Press.

Neuman, S. (2010, November 29) 'Clinton: WikiLeaks 'tear at fabric' of government,' http://www.npr.org/2010/11/29/131668950/white-house-aims-to-limit-wikileaks-damage

Palmer, M. (February 28, 2012) 'WikiLeaks publishes hacked Stratfor e-mails,' *Financial Times.* 8. Online. Lexis-Nexis.

Park, K. and H. Lee (2000) 'On the Effectiveness of Probabilistic Packet Marking for IP Traceback Under Denial of Service Attack,' *Computer Science Technical Reports.* Paper 1491. http://docs.lib.purdue.edu/cstech/1491

Pilkington, E. (2011, March 12) 'Clinton aide attacks Manning's treatment,' *Guardian*. 32. Online. Lexis-Nexis.

Rusbridger, A. (2011, January 28) 'WikiLeaks; The Guardian's role in the biggest leak in the history of the world,' *Guardian.* http://www.guardian.co.uk/media/2011/jan/28/wikileaks-julian-assange-alan-rusbridger

Sengupta, S. (July 26, 2011) 'For suspected hackers, a sense of social protest,' *New York Times*. B1. Online. Lexis-Nexis.

Shane, S. and Burns, J. F. (January 8, 2011) 'Twitter records in WikiLeaks case are subpoenaed,' *New York Times.* A1. Online. Lexis-Nexis.

Shirky, C. (2010a, December 6) 'WikiLeaks and the long haul,' http://www.shirky.com/weblog/2010/12/wikileaks-and-the-long-haul/

Shirky, C. (2010b, December 31) 'Half-formed thought on WikiLeaks and Global Action,' http://www.shirky.com/weblog/2010/12/half-formed-thought-on-wikileaks-global-action/

Sifry, M. L. (2011, March 21) 'The End of Secrecy,' *Nation*. 17-22.

Singel, R. (2010, March 1) 'Cyberwar Hype Intended to Destroy the Open Internet,' *Wired*. http://www.wired.com/threatlevel/2010/03/cyber-war-hype/

Sklerov, M. (2010) 'Responding to international cyber attacks as acts of war,' In J. Carr (ed) *Inside Cyber Warfare*. O' Reilly Media: Sebastopol, CA.

Slaughter, A. (January/February 2009) 'America's edge: Power in the networked century,' *Foreign Affairs*. 88(1), 94-113.

Solove, D. J. (2007). *The Future of Reputation*. New Haven: Yale University Press.

Strange, S. (1997) 'An international political economy perspective,' In J. H. Dunning (ed) *Governments, Globalization and International Business*. New York: Oxford University Press, 132-142.

Submissions (2011, n.d) http://wikileaks.org/wiki/Submissions#Submissions_via_secure_upload

U.S. Naval Research Lab. (n.d.) www.onion-router.net/summary.html

Winkler, J. R. (2009) 'Information warfare in World War I,' *Journal of Military History*. (73)3: 845-867.