Science, Technology, and Public Policy Program
Explorations in Cyber International Relations Project

WikiLeaks 2010: A Glimpse of the Future?

By Tim Maurer

HARVARD Kennedy School
Belfer Center for Science and International Affairs

August 2011

Discussion Paper #2011-10
Explorations in Cyber International Relations Discussion Paper Series

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138
Fax: (617) 495-8963
Email: belfer_center@harvard.edu
Website: http://belfercenter.org

WikiLeaks 2010: A Glimpse of the Future?

By Tim Maurer

Science, Technology, and Public Policy Program
Explorations in Cyber International Relations Project

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138
USA

Belfer Center Discussion Paper 2011-10
August 2011

Citation

This paper may be cited as: Maurer, Tim, "WikiLeaks 2010: A Glimpse of the Future?" Discussion Paper 2011-10, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, August 2011.

Comments are welcome and may be directed to Tim Maurer, tim.maurer@post.harvard.edu

Funding Acknowledgment

This work is funded by the Office of Naval Research under award number N000140910597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author (s) and do not necessarily reflect the views of the Office of Naval Research.

Abstract

The recent publications on WikiLeaks reveal a story about money, fame, sex, underground hackers, and betrayal. But it also involves fundamental questions regarding cyber-security and foreign policy. This paper argues WikiLeaks is only the symptom of a new, larger problem which is the result of technological advances that allow a large quantity of data to be 'stolen' at low or no cost by one or more individuals and to be potentially made public and to go 'viral', spreading exponentially online. From this flows my assessment that the unprecedented quantity constitutes a new quality, "a difference in quantity is a difference in kind". Therefore, we need to delink WikiLeaks from Julian Assange for a serious discussion of the policy implications. Assange, himself, could represent the revival of a modern version of anarchism challenging governmental authority. First, I outline a conceptualization of the process of leaking. This part weaves the chronology of WikiLeaks into the discussion of the source, publisher, and an examination of the role of mainstream media, including references to Daniel Ellsberg and the Pentagon Papers. In the second part I enlarge the frame to look at the issues that emerge once a leak has occurred and the government's response. Third, I examine the cyber-security implications since WikiLeaks' early releases only brought to public light what seems to already be known in the shadow world of government espionage, raising larger questions about cyber-security and foreign threats.

Table of Contents

Introduction[1]

"Weak servers, weak logging, weak physical security, weak counter-intelligence, inattentive signal analysis – a perfect storm. >sigh< Sounds pretty bad huh? … Well, it SHOULD be better! It's sad. I mean what if I were someone more malicious? I could've sold to Russia or China, and made bank!"[2] These are said to be the words of Private Bradley Manning, the man who is awaiting trial on the charge to be the source for the WikiLeaks releases in 2010. It shows that WikiLeaks is not only a First Amendment issue. The recent publications on WikiLeaks reveal a story about money, fame, sex, underground hackers, and betrayal.[3] But it also involves fundamental questions regarding cyber-security and foreign policy.

Today, there is not only WikiLeaks. Crymptome.org run by John Young in New York has been around since 1996.[4] New websites such as OpenLeaks, BrusselsLeaks, LocalLeaks, BalkanLeaks, IndoLeaks have sprung up.[5] Al Jazeera launched its own transparency project with the release of the Palestine Papers.[6] The Wall Street Journal created SafeHouse.[7] Moreover, WikiLeaks only released material from the Secret Internet Protocol Router Network (SIPRNet), the network hosting material classified as secret. What would happen in case of a leak from the Joint Worldwide Intelligence Communications System (JWICS) network containing Top Secret/Sensitive Compartmented Information?[8] In short, WikiLeaks and the events of 2010 are likely a wake-up call for what is to come.

I therefore examine WikiLeaks as the symptom of a new, larger problem which is the result of technological advances that allow a large quantity of data to be 'stolen' at low or no cost by one or more individuals and to be potentially made public and to go 'viral', spreading exponentially online. (Note that unlike a physical object, 'theft' in the virtual world means the act of copying, therefore not removal but duplication of data.) From this flows my assessment that the unprecedented quantity constitutes a new quality, "a difference in quantity is a difference in kind".[9]

WikiLeaks has raised awareness among top government officials how vulnerable our security systems are to infiltration. Interestingly, Richard A. Clarke, former White House "cyber czar",

[1] *I would like to thank Joseph S. Nye, Jr. for his helpful comments and insights. Special thanks go to Jonathan Zittrain who taught me that we hold the future of the Internet in our own hands. I am especially grateful to Kathryn Peters, Molly Sauter, and Philipp Schroegel for their help in editing the manuscript. Venkatesh "Venky" Narayanamurti was crucial for the realization of this paper and I particularly appreciate the patience and outstanding support from Michael Sechrist. The research for this paper ended in July 2011.*

[2] The Guardian: 87

[3] The Guardian, The New York Times, Der Spiegel, Domscheit-Berg

[4] Der Spiegel: 55

[5] The Guardian: 247 Sifry: 176

[6] Benkler: 31; http://english.aljazeera.net/palestinepapers

[7] https://www.wsjsafehouse.com/

[8] Clarke: 173

[9] Jones - Shorenstein: 24

has mentioned the vulnerability that facilitated the 2010 leak in his 2010 book describing the "sneakernet threat" of service members breaching the airgap.[10] This paper, however, moves beyond the mere technical cyber-security aspects to focus on what happens if such material becomes public which raises a number of challenging technical but also legal and policy questions. For this purpose, the releases of 2010 particularly lend themselves to a case study although WikiLeaks has been registered since 2006: There is one massive leak by a single source yet released in several tranches revealing different patterns of publishing and ultimately involving a country that, as the sole superpower, has the capacity to fight back, also because most of the corporations that run the Internet are headquartered there and subject to its laws.

My analysis highlights four aspects. First, we need to delink WikiLeaks from Julian Assange for a serious discussion of the policy implications. Building on my hypothesis of WikiLeaks being a symptom, there would be no Assange without WikiLeaks, but it seems plausible that there would be a WikiLeaks without Assange. It could be that Assange represents the revival of a modern version of anarchism challenging governmental authority. Second, we need to focus on one of the key questions, Why did the leaker, allegedly Bradley Manning, not go to The New York Times but to WikiLeaks? Third, with WikiLeaks' former number two, Daniel Domscheit-Berg, having launched Openleaks.org on December 30, 2010,[11] is a WikiLeaks-like platform an archive, source, wire service, or online newspaper? Fourth, WikiLeaks' first documents show that WikiLeaks only brought to public light what seems to already be known in the shadow world of government espionage, raising larger questions about cyber-security and foreign threats.

All of this is tied to the primary research question guiding this analysis: Is WikiLeaks a new phenomenon? First, I outline a conceptualization of the process of leaking. This part weaves the chronology of WikiLeaks into the discussion of the source, publisher, and an examination of the role of mainstream media, including references to Daniel Ellsberg and the Pentagon Papers. In the second part I enlarge the frame to look at the issues that emerge once a leak has occurred and the government's response. Third, I reexamine whether WikiLeaks is a new phenomenon and cyber-security implications.

The analysis is based on secondary literature, namely the recently published books by the media involved in the 2010 releases as well as Domscheit-Berg's account of his time at WikiLeaks, as well as government, media, and legal experts expressing their assessments and opinions on the matter. This paper has particularly benefitted from the insights of Harvard faculty, notably those expressed at an executive session on WikiLeaks hosted by the Shorenstein Center on the Press, Politics and Public Policy at the Harvard Kennedy School, on February 3, 2011 as well as the publications by the Berkman Center for Internet and Society.

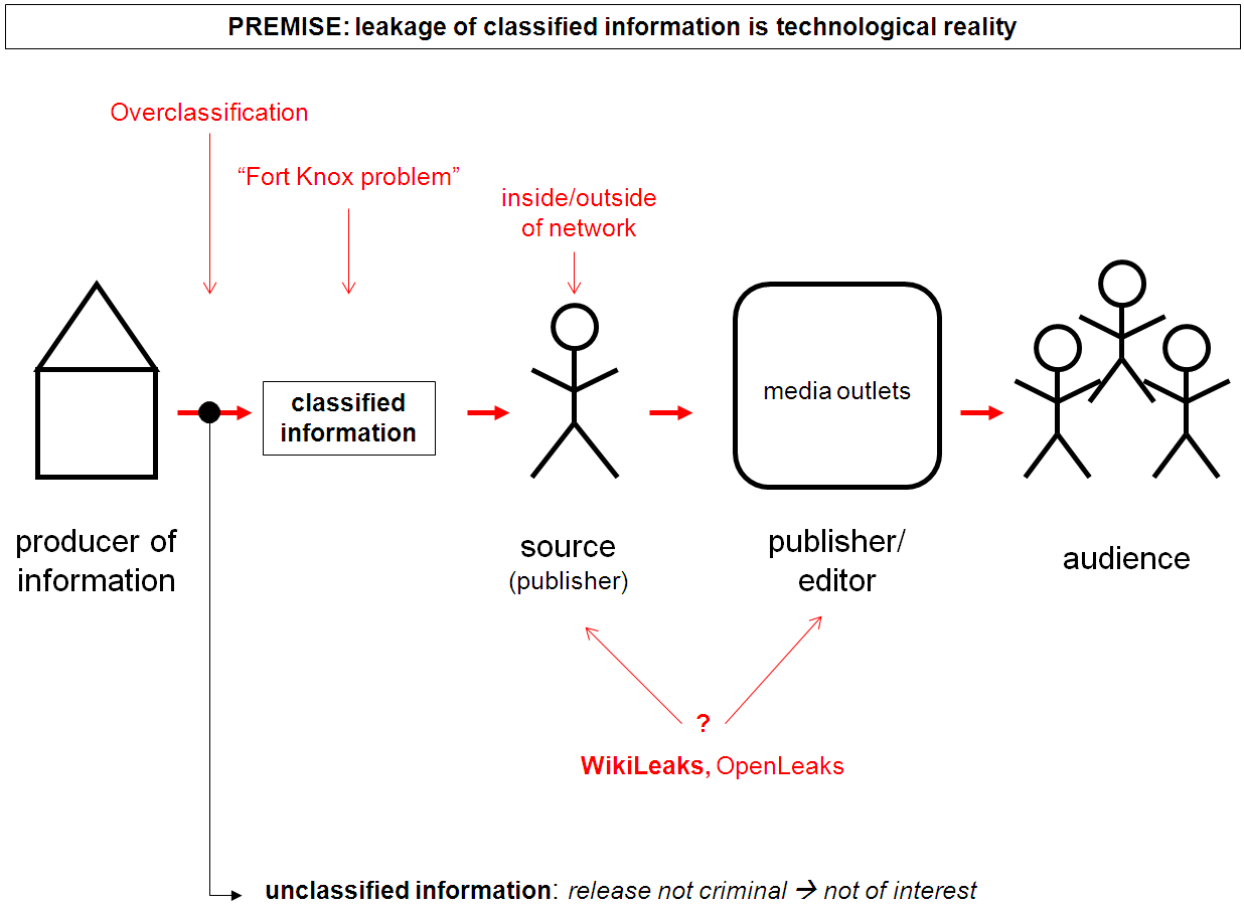
[10] Clarke: 171
[11] The Guardian: 109; Domscheit-Berg: xiv

PART I: WikiLeaks - Who, What, Where, When, Why

I.1 Conceptualization of Leaking

Much has been written about WikiLeaks in the past months. Many of the publications provide a descriptive account on the origins of WikiLeaks, its early years, and what happened after it received thousands of classified cables exposing the world's sole superpower, the United States. This paper strives to deduce some more abstract, general lessons learned from the events of the past months since WikiLeaks was registered as a domain on October 4, 2006.[12] As a first step, it is helpful to conceptualize the general process of leaking as illustrated in Figure 1 before diving into the various questions that WikiLeaks has raised.

Figure 1



(1) The producer of the information. In the beginning, someone produces information. After its production, the individual or institution also has the choice of designating information to be classified or unclassified (since the Atomic Energy Act of 1946 there has also been the principle

[12] Der Spiegel: 61; Domscheit-Berg: xi

that certain information is "born classified" in the U.S. government context)[13]. In case of the latter, the information is public, its publication not criminal and therefore not of interest for the purpose of this paper.

(2) The source. To leak classified material is usually considered a crime described as information theft. I use the word leak here because it implies that the material becomes accessible to someone who has not been authorized to have access. The term leak also differentiates the described activity from someone copying classified information to continue work on the personal computer at home (see Thomas A. Drake case[14]). In the latter case, while theoretically theft, the information is not a leak in the sense used here as the intent of the copying is not to provide access to someone who is not authorized.

The person leaking classified material is the source. There are two options: (1) the individual is inside the network and is authorized to have access to the material in the first place such as Private Manning; (2) the individual is outside the network not authorized to have access to the material but manages to access the material from outside through hacking. This would be the Chinese hackers that are reported to have infiltrated the networks of numerous foreign governments.[15]

Whether leaking is considered treason depends on the perspective. Ask yourself, for instance, how your reaction would have been if WikiLeaks had published thousands of cables exposing the government of the People's Republic of China, including its suppression of Tibetans, the massive labor camps, and revealing the depth of its Internet censorship program. Whistleblowing is a subcategory of leaking and exposes something that is illegal under the law. It therefore often enjoys special protection decriminalizing the information theft. (However, the exemplary articles by philosophers Terrance McConnell and Michael Davis show how the discussion on whistleblowing is far from having developed clear principles.[16]) Interestingly though, section 1034 of the U.S. Code on General Military Law outlines a whistleblowing provision specifically described as "Whistleblower Protections for Members of Armed Forces" when it was required to be included under President George H.W. Bush's administration in 1991.[17] Its key sections read:

> (a) Restricting Communications With Members of Congress and Inspector General Prohibited.-- (1) No person may restrict a member of the armed forces in communicating with a Member of Congress or an Inspector General. (2) Paragraph (1) does not apply to a communication that is unlawful […]

[13] Moynihan: 156
[14] http://www.nytimes.com/2011/06/10/us/10leak.html
http://www.nytimes.com/2011/06/11/us/11justice.html?_r=1&scp=1&sq=leak&st=cse
[15] The Guardian: 55-56; Der Spiegel 68-69
[16] McConnell; Davis
[17] Pub. L. 102-190, div. A, title VIII, Sec. 843, Dec. 5, 1991, 105 Stat. 1449

(c) (2) A communication described in this paragraph is a communication in which a member of the armed forces complains of, or discloses information that the member reasonably believes constitutes evidence of, any of the following:

(A) A violation of law or regulation, including a law or regulation prohibiting sexual harassment or unlawful discrimination.

(B) Gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.[18]

(3) The publisher. The source needs a publishing infrastructure to make the material widely available. The "mainstream media", a term The Guardian uses in contrast to the broader term 'news organization' used by The New York Times, have developed such infrastructures. First, newspapers created their nationwide distribution networks, radio moved from local frequencies to national dissemination followed by television via cable and satellite, and eventually the global Internet largely dependent on undersea cables. Traditionally, the distinction between source and publisher was easy. The source had the information and the publisher had the distributional network to make the information widely known.

The Internet obviates this need. Anyone can create a website at nearly no cost, accessible to all users of the world wide web. Of course, if we anticipate a hacking attack or add specific countries like China to the picture, the person would need to be Internet savvy enough to host the website on a server powerful enough to withstand a Distributed Denial of Server attack and in a country with strong freedom of speech protection laws and no extradition treaties. This assessment of the Internet must be qualified though if we think of environments such as in the People's Republic of China where the government has modified the Internet's infrastructure with significant additional hurdles.[19] Generally speaking though, in the age of the Internet, a source can also be the publisher and the distinction becomes blurred. In other words, "Long before WikiLeaks was born, the Internet had transformed the landscape of journalism, creating a wide-open and global market with easier access to audiences and sources, a quicker metabolism, a new infrastructure for sharing and vetting information, and a diminished respect for notions of privacy and secrecy".[20]

This is why another feature of mainstream media has often been highlighted in the debate on Manning, Assange and WikiLeaks. Over time, mainstream media not only developed their physical infrastructures but also their own version of the Hippocratic Oath, a set of principles to navigate between public interest and privacy, on the individual citizen's side, and secrecy, on the government's side. Investigation and redaction became crucial to perform this function.

[18] U.S Code / Title 10 – Armed Forces / Subtitle A – General Military Law / Part II – Personnel / Chapter 53 – Miscellaneous Rights and Benefits / Section 1034 – Protected communications; prohibition of retaliatory personnel actions

[19] I owe special thanks to Professor Nye for this comment.

[20] The New York Times: 21

(4) The audience. Ultimately, leaking implies the intention that the leaks are consumed by an audience. In the past, the range of a publication was confined by the physical publishing infrastructure and distributional network. However, the Communist East German government, for example, quickly realized that it could not stop its people from watching West German television via satellite. The Internet expanded this range even further from regional to global unless a government takes proactive steps to limit access and censor material such as the People's Republic of China's Great Firewall. In the words of Philip J. Crowley, the State Department spokesman, "The marriage of the data, the technology and the media yields impact that is global, not local."[21] Moreover, the Internet has transformed the audience from being merely a recipient to a potential participant in the role of a "citizen journalist" e.g. blogger.[22]

[21] The New York Times: 338
[22] The New York Times: 379

I.2 WikiLeaks

Before focusing on the events in 2010 as a case study, I will first present a few basic facts about WikiLeaks starting with (1) a few words on the two key public figures of WikiLeaks, Julian Assange and Daniel Domscheit-Berg, followed by a description of WikiLeaks' infrastructure, and an overview of the 2010 releases. I will then analyze (2) the role of Bradley Manning and (3) the role of Julian Assange as well as (4) the relationship between WikiLeaks and the mainstream media. I will conclude by discussing (5) what type of entity WikiLeaks represents.

(1) Julian Assange is the founder of WikiLeaks. WikiLeaks at its core is a project of people from Western democracies.[23] Of what Assange calls WikiLeaks' advisory board, only one of the alleged eight members has publicly acknowledged a link to WikiLeaks, C J Hinke a net activist from Thailand.[24] Assange claims that in 2006 WikiLeaks consists of 22 people but according to Der Spiegel the actual number of paid staff was limited to five.[25] Over the next four years its membership remained fluid with fewer than twenty people having official WikiLeaks email addresses[26]and even its number two, Daniel Domscheit-Berg, states not to have known all of its members.[27] Domscheit-Berg left his full time job in January 2009 after he first met Assange in December 2007. He eventually became WikiLeaks' second speaker then known under the pseudonym Daniel Schmitt.[28] His 2011 book *Inside WikiLeaks – My Time with Julian Assange at the World's Most Dangerous Website* has been the only extensive account so far from inside WikiLeaks which given its claim to be anti-secrecy has been rather secretive about its own internal affairs.

Domscheit-Berg's real name is known to us today because of internal fights among WikiLeaks members. On September 15, 2010, Domscheit-Berg, Birgitta Jonsdottir, a member of the Icelandic parliament who had supported WikiLeaks since the summer of 2009[29], as well as about a dozen other members left WikiLeaks.[30] Another key member among those who have left is 'the architect', a German programmer, who designed the WikiLeaks architecture.[31] The reasons for the infighting are manifold[32] including frustration over Assange using the official WikiLeaks Twitter account for his personal matters relating to sex crime charges in Sweden.[33] New members subsequently joined WikiLeaks particularly people Assange met during his time in London: Joseph Farrell from Swaziland and Sarah Harrison, both journalistic interns at the

[23] Der Spiegel: 74
[24] Domscheit-Berg: 86
[25] Der Spiegel: 61
[26] Domscheit-Berg: 196
[27] Domscheit-Berg: xi; Der Spiegel: 205
[28] Der Spiegel: 95
[29] The Guardian: 68; Der Spiegel: 115; Domscheit-Berg: xiii
[30] The New York Times: 41; Der Spiegel: 204
[31] Der Spiegel: 207
[32] Domscheit-Berg
[33] Der Spiegel: 199

time[34], James Ball former reporter for Grocer trade magazine who is the new WikiLeaks spokesman[35], the controversial Israel Shamir[36], and a connection to the French 'La Quadrature du Net'[37]. A chronological overview of known members of WikiLeaks is shown in the Appendix.

The technical infrastructure of WikiLeaks consisted, for most of its early days, of one server in Berlin.[38] Since 2008, the main server has been located in Sweden which not only has very strict rape laws but also very strong free speech protection. In mid-2010, WikiLeaks used some 50 servers "located in countries with the most favorable laws and the best protection of sources".[39] Between March and May 2010, seventeen new servers were added.[40] WikiLeaks' system for anonymous submissions was tested in 2007 by the British journalist Gavin McFayden. The cyber-security firm that he had hired to crack it gave up after unsuccessfully trying for a few weeks.[41] The mechanism was so complex that even members of WikiLeaks themselves are not able to trace submissions back to the source unless there is another channel of communication.[42] By 2010, WikiLeaks had "cryptophones, satellite pagers, and state-of-the-art servers".[43] However, when the WikiLeaks team broke apart in August 2010, its technical infrastructure suffered and was partly replaced by relying on servers provided by Amazon.[44]

The first releases in 2010 occurred in December 2006 shortly after the WikiLeaks domain had been registered. However, it was the year 2010 that made WikiLeaks famous with the launch of four major releases over the course of seven months. The latest release was the Gitmo papers on April 24, 2011, as the fifth.[45] (For a categorization of WikiLeaks' releases Ethan Zuckerman has proposed three phases.[46] For an alternative chronology see Benkler: 4-14). The timeline for the 2010 releases is as follows:

> **April 5: Collateral Murder** video presented at National Press Club in Washington, DC[47] to be viewed more than ten million times on YouTube and considered by Domscheit-Berg to have been WikiLeaks' "definite breakthrough"[48]

[34] Der Spiegel: 208; The Guardian: 14, 17
[35] The Guardian: 16
[36] The Guardian: 174
[37] Der Spiegel: 209
[38] Domscheit-Berg: 22
[39] Der Spiegel: 83; Domscheit-Berg: 125
[40] Domscheit-Berg: 131
[41] Der Spiegel: 84
[42] Domscheit-Berg: 40
[43] Domscheit-Berg: 131
[44] Domscheit-Berg: 247
[45] Der Spiegel: 7
[46] Zuckerman at Berkman
[47] The Guardian: 70; Domscheit-Berg: xiii
[48] Domscheit-Berg: 162

July 26: Afghan War Diaries, 77,000 cables released at once,[49] except for 15,000 that were withheld[50]

October 22: Iraq War Logs, 391,832 documents released at once [51] covering January 1, 2004 to December 31, 2009[52] with no top secret or no distribution material included and no documents on Abu Ghraib, hunt of al-Qaida leader al-Zarqawi or on Fallujah[53]

November 29: Cablegate, 220 cables released on the first day of a total of 251,287 cables[54] of which 40% were classified as confidential, 6% as secret (15,652 cables), one dating back to 1966, most newer than 2004, 9,005 from 2010 with the latest being dated February 28, 2010.[55] As of January 11, 2011, 2,017 cables have been released with many media falsely reporting that all had been released.[56]

The debate about whether only 220 or all of the 251,287 cables is somewhat misleading as Professor Burns, former Under Secretary of State for Political Affairs, points out. He argues, that even the leak of some 200 documents at once is unprecedented while 250,000 certainly have a wider, systemic, impact.[57] Interestingly, The Guardian mentions in its publication, "In all, jaw-droppingly, there were more than a million documents"[58] while the numbers above amount to only 735,119 however. Let us now turn to who is said to be the source of this material.

(2) Bradley Manning is an Army Intelligence analyst who was arrested on May 26, 2010, on the charge of allegedly being responsible for leaking the video that was published as the Collateral Murder video by WikiLeaks.[59] This charge sheet alone includes eight violations of law and four violations of the internal army code.[60] However, the full scope of the leak emerged only later. Manning had access to the U.S. Department of Defense's SIPRNet also used by the U.S. Department of State as part of the net-centric diplomacy system implemented in response to the 9/11 commission's recommendations.

According to the chat transcript published in Wired between the hacker Adrien Lamo and Manning, the latter took note of WikiLeaks when it released 500,000 text messages sent from cell phones on September 11, 2001, on Thanksgiving 2009.[61] (From a cyber-law perspective, an

[49] The New York Times: 34
[50] Zittrain - Berkman; Domscheit-Berg: xiii
[51] The New York Times: 250
[52] Der Spiegel: 218
[53] Der Spiegel: 218; The New York Times: 1; Domscheit-Berg: xiv
[54] The Guardian: 6
[55] The Guardian: 182, 197
[56] The New York Times: 56; Benkler: 13, 17; Domscheit-Berg: xiv; http://en.wikipedia.org/wiki/United_States_diplomatic_cables_leak#cite_note-5
[57] Burns - Shorenstein: 59
[58] The Guardian: 99
[59] Domscheit-Berg: xiii
[60] Der Spiegel: 261
[61] Wired. June 10, 2010. 'I Can't Believe What I'm Confessing to You': The

interesting question is whether those chat transcripts will be considered to be legitimate evidence.[62]) The transcript further outlines that Manning knew the material must have come from a National Security Database and was first in touch with Assange in late November 2009.[63] His motivation for ultimately passing on the classified material is reported to have been triggered by an incident in which Manning observed the arrest of 15 Iraqis by the local police because of what turned to be out an exercise of free speech and his army superior ignoring this fact and instead supporting the Iraqi police.[64] While it is unclear if the chat transcript is authentic, the fact that Manning called his aunt in Potomac while in military prison in Kuwait, giving her his Facebook password and asking her to type in as a new status update "Some of you may have heard that I have been arrested for disclosure of classified information to unauthorized persons. See http://collateralmurder.com" suggests the transcripts are an accurate account of what happened.[65] Otherwise, Manning's situation might have resembled that of FBI's Associate Director, Mark Felt, who waited 33 years to admit to be the source Deep Throat.[66]

Manning claims whistleblower protection. The complexity of this question was highlighted at a press conference on November 29, 2005. Secretary of Defense, Donald Rumsfeld, stated that U.S. soldiers have no obligation to actively stop torture through Iraqi officials but to merely report them. However, General Peter Pace, who was also present, disagreed responding that "It is absolutely the responsibility of every U.S. service member, if they see inhumane treatment being conducted, to intervene to stop it".[67]

However, Manning seems not to have first exploited the whistleblowing protections outlined in the U.S. Code on General Military Law. Moreover, he did not limit the leaks to what he believed where unlawful actions. This is why, in Harvard Professor Joseph Nye's judgment, Manning is not a whistleblower because of the sheer quantity of the material released, with the vast majority not qualifying for whistleblowing protection.[68] In addition, Harvard Professor Jonathan Zittrain, co-founder of the Berkman Center for Internet and Open Society, points out that while Daniel Ellsberg, the source of the Pentagon Papers, considers Manning to be a modern-day Ellsberg, Ellsberg himself had withheld four volumes of the Pentagon Papers at the time which included diplomatic correspondences. He considered them to be too sensitive and "he did not want to destroy the business of the diplomats".[69]

WikiLeaks Chatshttp://www.wired.com/threatlevel/2010/06/wikileaks-chat/
[62] Domscheit-Berg: 173
[63] The Guardian: 31, 74
[64] Der Spiegel: 140 ; The Guardian: 131
[65] http://www.pbs.org/wgbh/pages/frontline/wikileaks/manning-facebook-page/; Der Spiegel: 153; Poulsen and Zetter
[66] Der Spiegel: 142
[67] http://www.defense.gov/transcripts/transcript.aspx?transcriptid=1492; Der Spiegel: 262-263
[68] Nye - Shorenstein: 27
[69] Zittrain - Shorenstein: 9

Manning himself raises the question, "I'm not sure whether I'd be considered a type of 'hacker', 'cracker', 'hacktivist', 'leaker', or what […] I couldn't be a spy. Spies don't post things up for the world to see."[70] Nye points out though that while spies might have kept their information secret traditionally, in an age where public opinion influences foreign policy there is no reason why a spy would not publish data if it is considered useful to the home government. It also does not preclude him or Assange from potentially other serious charges such as sabotage.) What do the other terms mean though? Former hacker, Raoul Chiesa, offers the following definition,

> "originally, 'cracker' meant someone who removed the protection from commercial software programs. Recently, the term has started to appear in the papers and on mailing lists and has started to mean 'violent' hackers, i.e. hackers who are happy to become a nightmare for system administrators, deleting files and causing permanent damage"[71]

Chiesa therefore sees hackers at the beginning of the evolutionary chain adhering to what became known as hacker ethics of which the 1986 Hacker Manifesto forms an important part.[72] Crackers eventually emerged, a violent version of the original hacker although the latter term has become synonymous with the former in popular usage. However, both groups, hackers and crackers, share the view of being apolitical in a certain sense. This changed with the next evolutionary step and the emergence of hacktivism which is political activism through hacking according to Chiesa. Oxford Dictionaries defines a hacktivist as "a computer hacker whose activity is aimed at promoting a social or political cause".[73] An early example of hacktivism was the 1989 WANK worm expressing an anti-nuclear political agenda.[74] Another example of this "marriage between politics and hacking" is the first HackMeeting in Florence, Italy, in 1997.[75] Chiesa argues that "Hacking is by its very nature apolitical, and these excesses are not seen with approval, whether they are left or right wing".[76]

(3) Julian Assange is a hacktivist. This assessment is based on (i) his prior activities as a hacker, (ii) his 2006 writings, and (iii) his actions and comments with WikiLeaks post 2006.

In 1988, Assange, whose hacker pseudonym is 'Mendax', hacked into Minerva a system of mainframes in Sydney by government-owned Overseas Telecommunications Commission. By 1991, he was "Australia's most accomplished hacker" according to The Guardian.[77] Assange is part of a group called "international subversives" and contributed as a researcher to the 1997

[70] The Guardian: 87
[71] Chiesa: 54
[72] Chiesa: 112
[73] I thank Molly Sauter for highlighting that one could develop more granular definitions differentiating between cypherpunk and crypto-anarchic philosophies which is beyond the scope of this paper.
http://oxforddictionaries.com/definition/hacktivist?region=us
[74] The Guardian: 42
[75] http://www.nytimes.com/2011/06/11/technology/11hack.html?scp=4&sq=anonymous&st=cse
[76] Chiesa: 120
[77] The Guardian: 42

essay *Underground: tales of hacking, madness & obsession on the electronic frontier.*[78] It was also in the late 1990s that hacktivism emerged.

In 2006, Assange wrote a new essay which he first entitled "State and terrorist conspiracies" then changed to "Conspiracy as Governance".[79] It reads "When we look at conspiracy as an organic whole we can see a system of interacting organs. A body with arteries and veins whose blood may be thickened and slowed until it falls unable to sufficiently comprehend and control the forces in its environment".[80] In addition, Domscheit-Berg reports that Assange "professed to despise hackers because they weren't politically motivated".[81]

WikiLeaks' initial statement of purpose stated that "the primary interest is in exposing oppressive regimes in Asia, the former Soviet bloc, sub-Saharan Africa, the Middle East. We also expect to be of assistance to people of all regions who wish to reveal unethical behavior in their governments and corporations". Der Spiegel points out that in addition WikiLeaks was driven by the pursuit of "maximum political impact [translation by author]" and that successful leaking would topple several governments including the US government.[82] Domscheit-Berg adds another more banal reason for the focus on the United States in 2010. He points to language barriers and that none of WikiLeaks staff spoke Korean or Hebrew.[83] L. Gordon Crovitz writes in his piece The Wall Street Journal that Assange saw the "U.S. as the only enemy.'" citing Domscheit-Berg.[84] However, reading Domscheit-Berg's book carefully, this interpretation is rather skewed and is better summed up by Domscheit-Berg's self-assessment that "When I joined WikiLeaks in 2007, I found myself involved in a project devoted above all to one goal: subjecting the power that was exercised behind closed doors to public scrutiny. The idea of using an Internet platform to create transparency where it was most resisted was as simple as it was brilliant".[85]

Presenting WikiLeaks at the World Social Forum in Nairobi in 2007, Assange gave a presentation whose title also suggests a political agenda to achieve open government through mass leaking.[86] In 2010, for the release at the Frontline Club a poster is set up behind Assange showing a Viet Nam soldier, an analogy to Ellsberg and his political activism hoping to end the war in Viet Nam.[87] Ellsberg was an inspiration for Assange and the former received an email on December 9, 2006 signed "WL".[88] Assange himself told other WikiLeaks members, "there are

[78] The Guardian: 41; Der Spiegel 8
[79] Der Spiegel: 109
[80] Zittrain -Berkman
[81] Domscheit-Berg: 175
[82] Der Spiegel: 104
[83] Domscheit-Berg: 188
[84] Crovitz
[85] Domscheit-Berg: ix
[86] Der Spiegel: 77-78
[87] Der Spiegel: 173
[88] The Guardian: 47

two wars I have to end".[89] (It was not until October 23, 2010, that Assange met Ellsberg for the first time in person at an event in London[90]) The New York Times remarks that WikiLeaks had a "zeal to make the video a work of antiwar propaganda".[91]

Harvard Professor Lawrence Lessig calls this ideology "The naked transparency movement [which] marries the power of network technology to the radical decline in the cost of collecting, storing, and distributing data. Its aim is to liberate that data, especially government data, so as to enable the public to process it and understand it better, or at least differently".[92] Lessig, however, doubts that the world which the supporters of the naked transparency movement envision will be one that we would want to live in.[93] Instead, he proposes to tie the transparency movement to a movement for reform rather than revolution or anarchy since in his judgment "with the ideal of naked transparency alone – our democracy, like the music industry and print journalism generally, is doomed". [94]

So if Assange is a hacktivist, who is the target of his political activism? Der Spiegel offers the following assessment, different from Crovitz's view,

> "This fundamental confrontation does not target the administration in Washington alone, nor is it anti-American, but a matter of principle. The ideology of WikiLeaks is a potential challenge for every state, for oppressive regimes more so than democratic governments. WikiLeaks is an enemy of the state in the eyes of many governments. Following this view, Assange and his supporters are anarchists [translation by the author]".[95]

A response to this fundamental tension concerning government secrecy was given by the German political scientist Professor Muenkler in Der Spiegel. He describes secrecy as essential for the success of the modern nation-state. He doubts that those secrets would be in better hands if they were with WikiLeaks. It would destroy the state and simply replace the state as the guardian of secrecy.[96] Burns offers a concrete example by pointing out that nobody would want nuclear codes to be leaked, a point also made by Zittrain.[97]

Interestingly, WikiLeaks former number two, Domscheit-Berg, reiterates this point in his book.[98] However, Domscheit-Berg's notion of people with power does not seem to include the idea that controlling secrets in itself is a source of power. Muenkler's writing instead suggests that as soon as Domscheit-Berg and WikiLeaks have that control there is little that distinguishes them from

[89] The Guardian: 167
[90] Der Spiegel: 224
[91] The New York Times: 5, 232
[92] Lessig: 37
[93] Lessig: 38
[94] Lessig: 43
[95] Der Spiegel: 287
[96] Der Spiegel: 288
[97] Burns - Shorenstein: 55
[98] Domscheit-Berg: 267

what they consider "people with power". Moreover, WikiLeaks stated claim to promote transparency in the public interest is contradicted by a statement of Domscheit-Berg describing how "From the media we tried to learn how to manipulate public opinion [emphasis made by the author]"[99]. His explicit references to anarchist literature also underline the aforementioned assessment by Der Spiegel.[100]

(4) WikiLeaks and Mainstream Media. Some hacktivists view mainstream media as part of 'the establishment'. This relates to The New York Times description that it contacts the government before publishing a story, that "The journalists at the Times have a large and personal stake in the country's security"[101] and its chief Washington correspondent pointing out how "sometimes reporters get too close to government officials".[102]

So if WikiLeaks is a mainstream media critical project in the first place[103], why did it decide to cooperate with them in 2010? In short, WikiLeaks earlier releases had attracted the attention of mainstream media who started to actively seek out WikiLeaks. Assange himself on the other hand had tried to garner this attention. There are three main reasons for WikiLeaks to cooperate. First, it is a question of capacity. Mainstream media have the staff and experience to handle and redact a large amount of documents.[104] Second, working with mainstream media provides some protection. There is a well established series of precedents addressing mainstream media and the First Amendment that WikiLeaks on its own was not clear to fall under. Particularly prior to the release of Cablegate, Assange said that "We need to survive this publication" which is also why there was not a press conference and mainstream media were scheduled to publish first.[105]

Last but not least, the aforementioned goal for maximum political impact could be better achieved not only through an unprecedented amount of leaked material but also through an unprecedented cooperation among five of the world's largest media organizations. This latter point could be interpreted also to be an attempt to gain legitimacy but given the underlying culture of hacktivism permeating the WikiLeaks ideology; it seems that mainstream media were rather important for their force multiplying effect.

With regard to mainstream media, it is no secret that the industry has been in crisis in recent years.[106] Staff has been cut massively and newspapers shut down across the country. The U.S. Senate has even held hearings on the Future of Journalism.[107] It is therefore an intense competition among media organizations about exclusive stories. While the Internet is global, the mainstream media market continues to be predominantly national. The New York Times main

[99] Domscheit-Berg: 44
[100] Domscheit-Berg: 113
[101] The New York Times: 16
[102] Sanger - Shorenstein: 81
[103] Der Spiegel: 301
[104] Lessig: 41
[105] Der Spiegel: 233
[106] Lessig: 41
[107] Benkler: 51

competitor is The Wall Street Journal. Der Spiegel's counterpart is Der Stern. Forging a worldwide alliance among each other giving each participating organization a competitive advantage in their home markets allowed to reduce this competition and the three later five organizations worked well together and managed to coordinate near synchronous releases.[108] Working with WikiLeaks gave the papers "massive exposure", in other words, revenue.[109] The Guardian's website, for example, registered 4.1 million unique users the day of the Cablegate release, the highest in its history, and the currency by which their advertising fees are calculated.[110]

WikiLeaks first contact with mainstream media was with Der Spiegel through Domscheit-Berg in 2009. Der Spiegel had taken note of WikiLeaks after it had released a leak relating to Germany's secret service and a subsequent email exchange with its Director Uhrlau.[111] Assange first met with journalists from Der Spiegel in London in July 2010.[112] The Guardian's Nick Davies had met Assange only a month earlier in Brussels at the end of June.[113] The Guardian's interest was specifically a legal one given that the United Kingdom has one of the more restrictive laws regarding free speech under the Officials Secrets Act as The Guardian had recently experienced again through a gag order requested by Barclays Bank.[114] The Guardian brought The New York Times on board and for the Iraq War Logs, Le Monde joined followed by El Pais in the release of Cablegate.[115] For Cablegate, Assange also included the TV stations Al Jazeera and Channel4.[116]

The relationship between the mainstream media and WikiLeaks was complicated and eventually turned sour mostly because of the dynamic among the personalities involved but also because Assange reached out to other media organizations to increase his leverage. For the purposes of this paper, however, the key element is not the personal clashes; those are not be unique to mainstream media and WikiLeaks. However, the challenges concerning redaction were of a new quality given the vast quantity of classified material to sort.

The first question WikiLeaks and mainstream media faced centered on authentication. How could they know the documents were not fake? Der Spiegel and The New York Times' Eric Schmitt quickly concluded the cables were authentic given their own, independent sources and familiarity with similar material.[117] Der Spiegel was able to determine that the Afghanistan cables were authentic because of its knowledge of Germany's own federal parliament's

[108] The New York Times: 6
[109] The Guardian: 115
[110] The Guardian: 202
[111] Der Spiegel: 10, 160; Domscheit-Berg: 56-58
[112] Der Spiegel: 7
[113] The Guardian: 4; Der Spiegel: 159
[114] The Guardian: 63
[115] The New York Times: 1; Der Spiegel: 230, 232
[116] Domscheit-Berg: 244
[117] Der Spiegel: 160

investigation including secret US military material.[118] Second, in The Guardian's words," How are we ever going to find if there are any stories in it? […] The WikiLeaks project was producing new types of data. Now they needed to be mined with new kinds of journalism"[119] Third, the material exposed the names of individuals and other information that mainstream media usually redact prior to their publications. This challenged one of WikiLeaks core principles of publishing documents in their original unredacted form.

The mainstream media throughout the process adhered to their established principles for redaction. The Guardian had set up an operations center in London and each media organization had its own team of journalists around the world redacting the material.[120] For instance, Der Spiegel had a team of 50 people working on Cablegate alone.[121] The parties did not exchange their stories among each other or with WikiLeaks prior to the releases.[122] At the same time, The New York Times and Der Spiegel both approached the White House on the Thursday prior to the Afghanistan War Diaries publication on Sunday.[123] The New York Times again gave an early warning to the White House on November 19, 2010[124] providing the 100 or 150 cables used for its Cablegate stories.[125]

WikiLeaks' own approach to redaction has been the subject of much debate and criticism. It is also one of the key questions that come up in discussions whether WikiLeaks is a source, publisher, traditional news organization or something entirely new. In short, WikiLeaks has certainly exhibited adaptive behavior with regard to redaction. Two hypotheses emerge from its analysis, either WikiLeaks was undergoing a sort of learning process out of a genuine realization of the value of established journalistic principles or the change in behavior was due purely for self-protection purposes in anticipation of future legal struggles.

The facts are that WikiLeaks in its early days did not redact any documents. It was one of its core principles to release documents in their original, unredacted form as stipulated in the Frequently Asked Questions section on the website.[126] In 2010 with the release of the Collateral Murder video, WikiLeaks broke not only with its core principle of publishing documents in their original, unredacted form but also with its second core principle to publish documents in order of receipt.[127] The discrepancy between the shorter and the longer version in addition to the provocative title have been interpreted as additional signs of WikiLeaks political agenda. At the same time, the video was the first release that had received substantial input from journalists with

[118] The Guardian: 110
[119] The Guardian: 105-106
[120] The Guardian: 179
[121] Der Spiegel: 235
[122] Der Spiegel: 165
[123] Der Spiegel: 174
[124] The Guardian: 190; The New York Times: 12
[125] Sanger - Shorenstein: 18
[126] Der Spiegel: 83, 165
[127] Der Spiegel: 112-114; Domscheit-Berg

the Icelandic journalist Kristinn Hrafnasson and the cameraman Ingi Ragnar Ingason not only assisting in the redaction but also went to Iraq to check the facts.[128]

This set the stage for a much bigger endeavor, a cooperation no longer with only two journalists from the small country of Iceland, but a cooperation with what many consider to be the global industry leaders of the media. In the next release, the Afghanistan War Diaries, WikiLeaks still included the names of individuals in the documents accessible on its website while the three mainstream media had redacted them.[129] The Guardian reports that Assange did not care much about harm to informants "Well, they're informants,' he said. 'So, if they get killed, they've got it coming to them. They deserve it."[130] In light of the previous incident in Kenya, this would speak in favor of the self-protection hypothesis rather than the learning one. The latter would be supported in turn by The Guardian ensuing statement that "In fairness to Assange, he eventually revisited his view […] five months later, Assange had entirely embraced the logic of redaction, with his role almost that of a mainstream publisher"[131]

Domscheit-Berg's offers yet another explanation. The fact that some hundred names appeared in the documents was not because of a lack of effort by the WikiLeaks staff themselves but rather because Assange had not informed them of the agreement with the mainstream media on the redaction.[132] "I think that from that Wednesday to the following Monday I got only twelve hours of sleep, if that".[133] In light of the descriptions of Assange's character in the other books, this latter explanation sounds the most realistic and would also conform to the rather messy and less strategic nature of reality.

For the Iraq War Logs, WikiLeaks designed sophisticated software to redact names[134] and its staff emulated the redactions of the mainstream media implementing what Assange calls WikiLeaks' "harm minimization policy".[135] At this point, The Guardian reports WikiLeaks adopted all of its redactions.[136] This change from the original principle moved so far that the mainstream media eventually even adopted a proposal by a WikiLeaks staff member who suggested replacing any blacked out name with a dozen upper-case Xs to cover up the length of the original word. This would suggest that learning occurred not only within WikiLeaks but both ways, similar to what mainstream media had already learned from WikiLeaks on encryption.[137] The culmination of this process is a letter Assange sent to the U.S. embassy in London on November 26, 2010, prior to the release of Cablegate similar to the aforementioned practice of

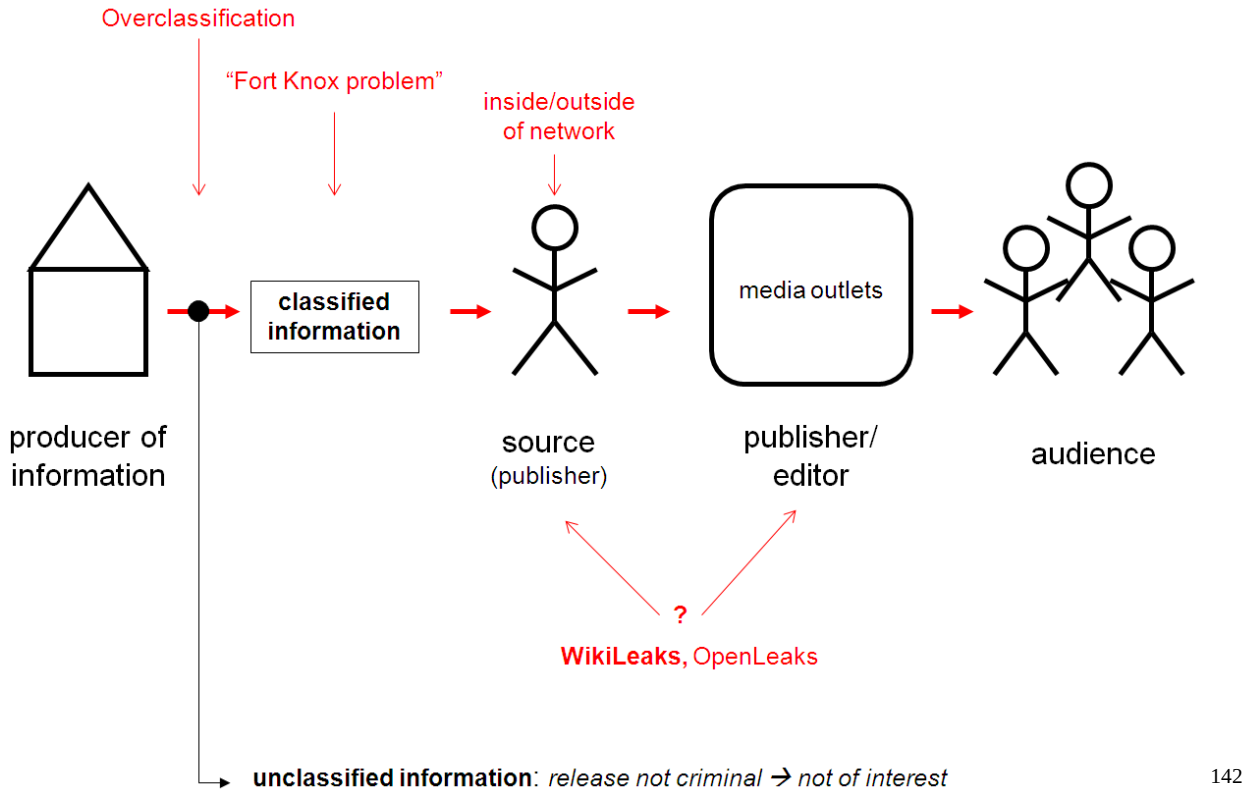
[128] Der Spiegel: 121
[129] The New York Times: 19
[130] The Guardian: 111
[131] The Guardian: 112
[132] Domscheit-Berg: 182-183
[133] Domscheit-Berg: 183
[134] The Guardian: 112
[135] The New York Times: 19; Der Spiegel: 301
[136] The Guardian: 5
[137] The New York Times: 19

the mainstream media.[138] (The head of the US State Department's legal team responded that "the United States did not negotiate with people who had acquired material illegally".[139])

In retrospect, one could argue that Assange seems to have changed from being a radical anarchist in 2006 into perceiving himself to be a journalist or publisher by 2010. After the release of the Afghan War Diaries Assange adopted the narrative of calling WikiLeaks a "media organization" and himself occasionally editor-in-chief. Moreover, in August, he went to Sweden trying to acquire a press card to solidify the First Amendment protection.[140] This would be a classic example for the logic of appropriateness and the power of norms and the pressure to assimilate. At the same time, it is not clear whether this change was due to an actual learning process Assange was subject to or part of an effort to protect himself in line with a logic of consequences.[141] Ultimately, the two hypotheses are not mutually exclusive.

Figure 4 summarizes how the classified material from SIPRNet eventually became public.

Figure 4



142

[138] The Guardian: 192
[139] Domscheit-Berg: 257
[140] Der Spiegel: 176
[141] March and Olsen
[142] GNU Free Documentation License http://commons.wikimedia.org/wiki/File:Globe.png

(5) So what type of entity is WikiLeaks? Is it a source? A media organization? One comparison that has been neglected in the literature so far is the analogy to a wire service such as Reuters. Jack Shafer, a Slate columnist, is pragmatic when he states Assange "acts like a leaking source when it suits him. He masquerades as publisher or newspaper syndicate when that's advantageous".[143] Assange's changing behavior further complicates answering this question.

In Australia, Assange's home country, WikiLeaks is listed as a library.[144] Originally, Assange pursued what he called "scientific journalism" the publication of raw material.[145] This made it similar to an archive.[146] The New York Times calls WikiLeaks and Assange a source prominently on the cover page of the introduction to its publication, the only one making this explicit statement of the three major news organizations, The New York Times, The Guardian, Der Spiegel.[147] However, it also refers to The Guardian as a source in the context of Cablegate after Assange refused to continue to work with The New York Times.[148] This is probably because The New York Times is the only news organizations headquartered in the U.S. where the judicial investigations are ongoing.

Harvard Professor Yochai Benkler says The New York Times is trying to distance itself from Assange[149], an assessment shared by Paul Steiger, editor-in-chief of ProPublica, adding as a reason that "WikiLeaks is not the A.P."[150] Importantly, the staff of a wire service is composed of journalists who adhere to the profession's principles and are the first instance selecting and redacting information which are then sold to other media organizations.

At the same time, Assange called WikiLeaks a media organization and quoted sections from the Pentagon Papers Supreme Court ruling for the text announcing the Iraq War Logs.[151] And while The New York Times tries to distance itself, Bill Keller does admit,

> "while I do not regard Julian Assange as a partner, and I would hesitate to describe what WikiLeaks does as journalism, it is chilling to contemplate the possible government prosecution of WikiLeaks for making secrets public, let alone the passage of new laws to punish the dissemination of classified information, as some have advocated. Taking legal recourse against a government official who violates his trust by divulging secrets he is sworn to protect is one thing. But criminalizing the publication of such secrets by someone who has no official obligation seems to me to run up against the First Amendment and the best traditions of this country"[152]

[143] The Guardian: 7
[144] Der Spiegel: 305
[145] The New York Times: 21
[146] Der Spiegel: 9
[147] The New York Times: 1, 4-5
[148] Der Spiegel: 231
[149] Benkler: 57
[150] The New York Times: 410
[151] Der Spiegel: 2010
[152] The New York Times: 2-21

The Guardian goes beyond the established categories and describes WikiLeaks as "a new breed of publisher-intermediary"[153], a hybrid between traditional media and a platform that is difficult to censor and that would not exist without the digital revolution.[154]

With regard to their cyber-security systems, Assange had told The Guardian, "You guys at the Guardian, you have got to do something about your security. You have got to get your email secure and encrypted"[155] and The New York Times did not have encrypted phone lines which is why Skype was a more secure way of communicating.[156] Domscheit-Berg in his recent book continues to state "Based on my experience, I wouldn't advise any informant to contact the traditional media with a digital secret document, not even if that person had a personal contact or was offered a small financial reward for the material".[157] He concludes, "the anonymity guaranteed by WikiLeaks' anonymizing mechanisms is the main advantage WL enjoys over all classical forms of investigative journalism".[158] This comment gains weight in light of The Wall Street Journal's SafeHouse which after a link within a link reveals the caveat that

> "There is nothing more sacred than our sources; we are committed to protecting them to the fullest extent possible under the law. Because there is no way to predict the breadth of information that might be submitted through SafeHouse, the terms of use reserve certain rights in order to provide flexibility to react to extraordinary circumstances. But as always, our number one priority is protecting our sources. [emphasis made by the author].[159]

This question is not likely to be settled soon. The technological platform itself does not seem to serve a useful starting point. After all, The New York Times could create a similar website to inform its traditional reporting. An alternative therefore is not to start with the technological platform but the way it is used. SafeHouse will operate differently than WikiLeaks. Should it be considered a different entity then, although it uses the same technology? The answer to this question might also manifest itself to whom press cards will be issued in the future. Will people working for SafeHouse receive press cards while WikiLeaks hacktivist ideology keeps it out of the club? Are such platforms a new type of wire service serving as a first filter of the massive amount of information available globally for journalists to sift through what is actually newsworthy? My guess is that this question will not be settled by a specific law or policy but is likely to emerge out of practice, laws, and courts rulings in the years to come much like traditional newspapers and media developed over the decades.

It is now time to move beyond the process of leaking to the response of the producer of the information.

---

[153] The Guardian: 7
[154] Der Spiegel: 304
[155] The Guardian: 98
[156] The New York Times: 2
[157] Domscheit-Berg: 166-167
[158] Domscheit-Berg: 170
[159] http://www.dowjones.com/pressroom/presskits/safehouse.asp

PART II: The Government's Response

II. The Leak is Out – The Government's Response

So what happened, once the leak was out? The U.S. Government's response to the various releases of WikiLeaks can serve as a blueprint but is also a starting point for lessons learned. In general, the response of the government was framed by what it knew. After (1) a few words on the state of the cyber-security at the beginning of 2010 and (2) a discussion of the releases' overall impact, a detailed analysis of (3) the government's response follows, closing with a brief outline of (4) alternative views.

(1) According to The New York Times referring to Pentagon figures, about 500,000 people have access to secret cables[160] with the Washington Post estimate at some 850,000.[161] Ultimately, "the government actually doesn't know precisely how many people overall have security clearances to classified material".[162] While the Department of Defense did not allow USB sticks for its computers because they were considered to be small enough physically to be easily leaked, Bradley Manning was allegedly able to use CD/DVD drives capable of rewriting. This also enabled him to bridge the airgap between the secure SIPRNet and the general Internet and to leak the material via the Internet. This is how Manning is said to have been able to copy/steal and share the data. In addition he is believed to have used encryption and the Tor network to transfer the data anonymously via the Internet.[163]

In addition, classified material was stored in what Zittrain calls the "Fort Knox" problem,

> "Fort Knox represents the ideal of security through centralization: gunships, tanks, and 30,000 soldiers surround a vault containing over $700 billion in American government gold. It's not a crazy idea for a nation's bullion; after all, the sole goal is to convincingly hoard it. But Fort Knox is an awful model for Internet security." [164]

It is an "awful model" when an individual can overcome the "gunships, tanks, and 30,000 soldiers" and copy thousands of cables from the Fort Knox of the U.S. government, SIPRNet, a centralized database for secret documents. The situation was even worse compared to Fort Knox in that there was no system in place to monitor who had accessed which material when and whether the material had been copied in order to be able to trace potential leaks. As a result, the government is said to have "massively over-briefed about what was in the cables" according to

[160] The New York Times: 18
[161] Der Spiegel: 17
[162] John Fitzpatrick, director of ODNI Special Security Center quoted in Sifry: 157; Fitzpatrick (December 1, 2010) www.fas.org/sgp/news/2010/12/clearances.html
[163] Der Spiegel: 141-142
[164] http://futureoftheinternet.org/fort-knox-problem

The Guardian's Ian Katz since the government could not know if the cables dated up to Manning's arrest in June. The most recent cable actually dated at the end of February.[165]

(2) Impact. Harm has been one of the key elements in the discussion on the impact of WikiLeaks' releases. In short, the picture is messy. First, there are some methodological challenges in that it is yet too early to fully assess the situation and many of the variables are hard to measure such as a deterioration of trust among diplomats or the relevant indicators, e.g. number of phone calls per month, not publicly available. Burns for instance points out that "Diplomacy in my judgment, diplomacy among governments is built on trust among diplomats"[166] which is echoed by his former colleague from France, Bernhard Kouchner, founder of Doctors without Borders, "We will all terribly mistrust each other. That is the risk".[167]

The fact is that a number of governmental officials in the U.S. and abroad either had to leave their jobs or were relocated including the U.S. ambassador to Libya in January 2011, the U.S. ambassadors to Mexico and Ecuador, a charge d'affaires in Turkmenistan, and a German party official.[168] Among those concerned about potential harm, were five human rights organizations including Amnesty International, Reporters without Borders that sent a letter to the Wall Street Journal last year calling on WikiLeaks to change its policy. [169] Other reports, such as those by the London Times, owned by Rupert Murdoch, titled "Man named by WikiLeaks 'war logs' already dead" turned out to be false. In reality, the man had already been dead for two years.[170] However, a Taliban spokesperson announced that the Taliban would analyze the cables[171] and in early December 2010 WikiLeaks released a cable on infrastructures worldwide critical for the U.S.[172]

This is in contrast to a number of assessments by government officials and media representatives that no harm has occurred. These point out that informants felt nervous[173] but there had been no reports of actual harm while some had been relocated within their countries, some moved abroad (which for the people affected might have actually been a very concrete harm to be forced to leave their homes).[174] According to a Pentagon spokesman speaking in January 2011, there has been no confirmed case of harm in response to Afghan War Diaries.[175] Secretary of Defense Robert Gates had told the Senate a few months earlier that "the review to date has not revealed any sensitive intelligence sources and methods compromised by this disclosure".[176] With regard

[165] The Guardian: 188; The New York Times: 241
[166] Burns - Shorenstein: 55
[167] The New York Times: 214
[168] The Guardian: 225; The New York Times: 242
[169] Der Spiegel: 197; The New York Times: 242
[170] Der Spiegel: 182; The Times
[171] The New York Times: 321
[172] Der Spiegel: 257; Benkler: 13
[173] The New York Times: 214
[174] The New York Times: 230, 241
[175] The New York Times: 242
[176] http://articles.cnn.com/2010-10-16/us/wikileaks.assessment_1_julian-assange-wikileaks-documents?_s=PM:US quoted in Benkler: 1

to Cablegate, his judgment is "Is this embarrassing? Yes. Is it awkward? Yes. Consequences for U.S. foreign policy? I think fairly modest".[177] In addition, according to Reuter's Mark Hosenball, State Department officials told Congress in private that leaks were "embarrassing but not damaging".[178]

The Guardian reports that six months after the release of the Iraq logs there was no proof of lost lives.[179] It continues,

> "By the end of the year in which WikiLeaks published its huge dump of information, no concrete evidence whatever had surfaced that any informant had suffered actual reprisals. The only reports were of defence secretary Robert Gates telling a sailor aboard a US warship in San Diego, 'We don't have specific information of an Afghan being killed yet.' CNN reported on 17 October that, according to a senior Nato official in Kabul, 'There has not been a single case of Afghans needing protection or to be moved because of the leak.' "[180]

Will Tobey, Senior Fellow at the Belfer Center, makes the interesting observation however that "Gates and Keller [from The New York Times] have an interest in diminishing the impact. Gates, because he wants diplomacy to continue, and Keller because he doesn't want to seem like such a bad thing has been done".[181] One could add also that Secretary Gates has an interest to downplay the consequences of a leak that originated from a network of his department and was leaked by one of its service members.

The truth probably lies somewhere in between. In Nye's view, also former Chair of the National Intelligence Council, "So, some damage? Yes. But not overwhelming"[182] such as. He mentions the Singapore Defense Minister who cautioned people in Singaporean government not to speak freely to Americans.[183] It is also likely that Secretary Gates is in this group, as well. Der Spiegel quotes a letter from Secretary of Defense Robert Gates to US Senators Carl Levin and John McCain on August 16, 2010, that so far the leak had not exposed sensitive intelligence sources or methods[184] and David Sanger from The New York Times reports conversations have continued.[185] According to The Guardian. " One congressional official briefed on the reviews told Reuters that the administration felt compelled to say publicly that the revelations had seriously damaged American interests in order to bolster legal efforts to shut down the WikiLeaks website and bring charges against the leakers".[186]

---

[177] http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4728 quoted in Benkler: 2
[178] Sifry: 155
[179] The Guardian: 6
[180] The Guardian: 113
[181] Tobey - Shorenstein: 45
[182] Nye - Shorenstein: 25
[183] Nye - Shorenstein: 25
[184] Der Spiegel: 185
[185] The New York Times: 2
[186] The Guardian: 245-246

It remains unclear to what degree the leak has prevented harm such as the reports on the Bangladeshi government death squad that was exposed but no further deaths reported since the publication.[187] Similarly, reports on Shell's infiltration of the Nigerian government might fall in this category and the big elephant in the room is to what degree the leaked cables contributed to the Arab Spring.[188]

At the same time, there is a serious danger that in the medium and long term, "our enemies will mine this information, looking for insights into how we operate, cultivate sources and react in combat situations, even the capability of our equipment".[189] One concrete example is the previously unknown paramilitary CIA group and detailed information on its operations uncovered by the Washington Post.[190] And while mainstream media regularly publish similar stories, the question remains whether the sheer wealth of information will allow groups like Al Qaida to not only get a snapshot but a systematic picture of how the U.S. military operates.

(3) Government response. Against this background, the U.S. Government's response was divided up as follows. President Obama spoke with a number of heads of state including the Turkish Prime Leaders about the leaks. Apart from a few instances, this sort of damage control, however, was mainly conducted by the State Department while the Defense Department reexamined its cyber-security standards.[191] The overall response itself can be categorized to consist of the following four components, as once described by The Guardian's Davies to Assange: (I) "physical – that someone would beat him up or worse", (II) "legal – that Washington would attempt to crush WikiLeaks in the courts", (III) "technological – that the US or its proxies would bring down the WikiLeaks website", and (IV) public relations - "a PR [public relations] attack – that a sinister propaganda campaign would be launched".[192]

(I) Physical response. While not an official position of the Executive, a number of people publically called for a physical response such as Mike Rogers, a congressman from Michigan who suggested the death penalty.[193]

(II) Legal response. The possibilities of a legal response have been limited by the general challenges encountered in cyber-law. They relate to jurisdictional uncertainty in a theoretically borderless Internet[194] and the attribution problem, as well as unanticipated consequences. Moreover, they face the specific challenge regarding the unresolved question whether WikiLeaks

[187] The Guardian: 226
[188] Gordon and West
[189] The New York Times: 324
[190] Der Spiegel: 184
[191] The New York Times: 218
[192] The Guardian: 96-97
[193] The Guardian: 202-203
[194] Wu and Goldsmith

is protected under the First Amendment or not as highlighted in the report on WikiLeaks prepared by the Department of Defense in 2008.[195]

An example of the jurisdictional challenges and attribution problem is highlighted by the experience of the bank Julias Baer, an early victim of a release by WikiLeaks exposing its money-laundering practice.[196] Baer had a very difficult time figuring out in what country the release might be considered illegal and whom to file charges against in the first place. The bank eventually tried to go after Daniel Mathews, whose name was among the few publicly associated with WikiLeaks as he had registered its domain and who could be prosecuted in the United States because he was a student at Stanford. However, Mathews was supported among others by the American Civil Liberties Union and the Electronic Frontier Foundation, and the case eventually dropped by Baer setting an important precedent.[197] CBS News even reported on this incident with the headline 'Freedom of Speech has a number', WikiLeaks IP address.[198]

At the same time, the potential threat of a gag order like the ones the U.S. Government sought in case of the Pentagon Papers is why "What was needed, Davies [from The Guardian] felt, was a multi-jurisdictional alliance between traditional media outlets and WikiLeaks, possibly encompassing non-governmental organizations and others."[199] This was a practice The Guardian had already applied when it cooperated with a Dutch newspaper and Norwegian TV channel to circumvent Britain's laws.[200] The lesson learned from the Pentagon Papers is probably why the administration decided not to seek a gag order after the first major release of the Afghan War Diaries.[201]

A second constraint in cyber-law generally is unanticipated consequences. Barbara Streisand experienced this in 2003 in what has come to be known as the 'Streisand effect'.[202] Mike Masnick from techdirt coined this term[203] to describe the "online phenomenon in which an attempt to hide or remove a piece of information has the unintended consequence of publicizing the information more widely"[204]. "The name goes back to a lawsuit by actress Barbara Streisand, who sued a photographer and website in 2003 because the latter showed a photo of her home. However, only her lawsuit revealed that it was her home in response to which the photo went viral on the Internet [translation by author]". Domscheit-Berg's account reveals that WikiLeaks clearly included such effects in its strategy "we […] hoped that Scientology would try to sue us. The sect would almost surely have lost any suit it chose to file, and the case would have attracted

[195] Benkler: 6
[196] Domscheit-Berg: xi
[197] Der Spiegel: 90-92
[198] Domscheit-Berg: 21
[199] The Guardian: 97
[200] The Guardian: 177
[201] The Guardian: 110
[202] Der Spiegel: 324
[203] http://www.techdirt.com/articles/20050105/0132239.shtml
[204] http://en.wikipedia.org/wiki/Streisand_effect

more public interest in the spectacular documents, as had been the case with Julius Baer".[205] The effect arguably does not apply though to the well publicized releases in 2010.

Against this background, the U.S. Government took a number of legal actions. First, the task forces set up by the Department of Defense and Department of State were not only set up to manage the releases but also to conduct a criminal investigation.[206] This ultimately led to the arrest of Manning. The Army however only has jurisdiction over its service members. The investigation against Assange and WikiLeaks is under the jurisdiction of the Department of Justice. [207] The basis is a 1985 ruling that the 1917 Espionage Act can also be applied abroad.[208]

On December 14, 2010, the Department of Justice issued secret subpoenas to access a number of Twitter accounts including that of Assange and the Icelandic Parliamentarian, an action eventually made public by Twitter.[209] There have also been reports of a secret grand jury in Alexandria, Virginia.[210] As aforementioned, unlike the Pentagon Papers, the focus however is not on prior constraint but the possibility of legal punishment which has not yet been settled by the Supreme Court. That is where the question whether Assange/WikiLeaks actively solicited classified material becomes important highlighted by the statement of Geoff Morrell, the press secretary of the Department on October 22.[211] In this context, Crovitz is right on point by highlighting that "It's the political motivation of Mr. Assange that qualifies him to be prosecuted" under the Espionage Act. He points out that what differentiates Assange from The New York Times is that Assange intended to harm the US.[212] Whether the 2005 case against employees of the American Israel Public Affairs Committee a lobby firm, accused of transferring information from military analyst to Israel, which was eventually dropped in 2009 is any indication of the likely outcome of a prosecution against Assange remains unclear.[213]

To date apart from Senator Lieberman no government official has suggested prosecuting news organizations in court.[214] However, the legal uncertainty would explain The New York Times behavior. While its lawyers are said to consider the newspapers' actions to be within the law based on the Pentagon Papers case[215], the newspaper published a portrait critical of Assange only a day after publishing the Cablegate cables in what has been interpreted as an attempt to distance itself from WikiLeaks.[216] WikiLeaks in turn changed the wording of its website from "Submitting documents to WikiLeaks is safe, easy and protected by law" to "Submitting

[205] Domscheit-Berg: 40-41
[206] The New York Times: 315; Bradbury: 22
[207] The New York Times: 317
[208] The New York Times: 316
[209] The Guardian: 94, 245
[210] The Guardian: 209
[211] Benkler: 26, 33-34; The New York Times: 324
[212] Crovitz
[213] The New York Times: 316; Der Spiegel: 176; Crovitz
[214] The New York Times: 15, 234
[215] The New York Times: 8
[216] Der Spiegel: 230, 232

documents to our journalists is protected by law in better democracies" as well as the statement "WikiLeaks accepts a range of material, but we do not solicit it" and the 'most wanted' list of materials no longer includes the reference to classified material.[217]

Overall, the Obama administration has charged five government employees for leaking classified information to the media, no other president has overseen more than one such prosecution[218]

Harvard professor Jack Goldsmith, former Assistant Attorney General in the Office for Legal Council under President George W. Bush, and expert on cyber-security warns that a WikiLeaks prosecution is likely to fail, a view shared by Benkler[219] and that "Succeeding will harm First Amendment press protections, make a martyr of Assange and invite further chaotic Internet attacks. The best thing to do – I realize that is politically impossible – would be to ignore Assange and fix the secrecy system so this does not happen again".[220]

However, the actual ruling is only one effect of law. The process leading to the ruling has important political effects in itself and constitutes a separate policy option. Mathews, for example, was so impressed by the case brought against him that he decided to end his involvement with WikiLeaks shortly thereafter.[221] A legal response can therefore have powerful deterrent effects as highlighted in the section on public relations.

(III) Technological response. The U.S. government is not known to have engaged in a cyber attack against WikiLeaks. Nevertheless, 2010 might have been the first global cyber-conflict of its kind. While the DDoS attack against Estonia in 2007 or the Google incident and Stuxnet attack in 2010 are reported to have been mainly bilateral – Estonia/Russia, Google/China, Israel/Iran – the activities in cyberspace after the Cablegate release included American hackers targeting WikiLeaks, multinational companies cancelling their business relationship with WikiLeaks in the US, France, and Switzerland, the hacktivist group Anonymous attacking those companies in return, while mirror sites of WikiLeaks sprung up all over the world. In the words of Der Spiegel, "It constitutes the biggest international revolt in the net up to date."[222] It is a powerful example of what Nye describes in his most recent book *The Future of Power* as a diffusion of power to nongovernmental actors explicitly mentioning WikiLeaks.[223]

With regard to government involvement, the possibility of an offensive cyber attack against WikiLeaks' infrastructure has been discussed by Steven Bradbury, the head of the Department of Justice's Office of Legal Council under President George W. Bush.[224] However, the only evidence of government involvement is reduced to Senator Lieberman stating "I call on any

[217] Domscheit-Berg: 262
[218] The New York Times: 340
[219] Benkler: 3
[220] The New York Times: 340-341
[221] Der Spiegel: 91
[222] Der Spiegel: 279
[223] Nye: 118
[224] Bradbury: 21-22

other company or organization that is hosting WikiLeaks to immediately terminate its relationship with them. WikiLeaks' illegal, outrageous, and reckless acts have compromised our national security and put lives at risk around the world. No responsible company – whether American or foreign – should assist WikiLeaks in its efforts to disseminate these stolen materials."[225] Another indication that government pressure induced the companies' behavior was revealed by a PayPal manger speaking at a conference in Paris saying that "The State Department told us, the activities are illegal" despite previous denials.[226]

At the same time, Secretary Clinton declared in her speech on February 15, 2011 *Internet Rights and Wrongs: Choices & Challenges in a Networked World,*

> "There were reports in the days following these leaks that the United States Government intervened to coerce private companies to deny service to WikiLeaks. That is not the case. Now, some politicians and pundits publicly called for companies to disassociate from WikiLeaks, while others criticized them for doing so. Public officials are part of our country's public debates, but there's a line between expressing views and coercing conduct. Business decisions that private companies may have taken to enforce their own values or policies regarding WikiLeaks are not at the direction of the Obama administration". [227]

So what happened? On November 29, 2010, after the Cablegate release, a Distributed Denial of Service attack (DDoS) was launched against WikiLeaks' website by the hacktivist "The Jester" ("th3j35t3r" since hackers tend to substitute the letter 'e' with number '3' and 's' with '5').[228] Peaking at 18Gbps, this DDoS attack was eight times larger than any previous DDoS attack on WikiLeaks.[229] The hacktivist group Anonymous, which had become famous previously for its activities against Scientology, decided to launch a counterattack. It also targeted companies like Amazon, PayPal, MasterCard among others.[230]

After the statement by Senator Lieberman, Amazon, whose server WikiLeaks was using, decided to end the business relationship. WikiLeaks responded by publishing its new URL via Twitter and when the French government cracked down on the new French server, a server in Sweden was eventually chosen where it enjoyed one of the strongest free speech protections.[231] The new URL became wikileaks.ch and while it is the Swiss country domain name, the website is actually hosted by the Swedish Pirate Party.

Within days 1,200 mirror sites had sprung up over the Internet making the DDoS attack and companies' actions largely ineffective.[232] In the words of Domscheit-Berg, "It was virtually

[225] The Guardian: 205; Benkler: 21
[226] Der Spiegel: 275
[227] www.stage.gov/secretary/rm/2011/02/156619.html
[228] Der Spiegel: 271
[229] The Guardian: 203
[230] Der Spiegel: 273
[231] Benkler: 28, 29
[232] Der Spiegel: 278

impossible to take us off the Internet"[233]. However, the actions of PayPal and other financial service providers successfully restricted WikiLeaks access to existing funds and new donations while raising important questions regarding net neutrality. A further escalation of the cyber-conflict could have taken place if WikiLeaks would have decided to release the password to decrypt the 'insurance file', a highly encrypted file posted on the Internet on July 30, 2010, and sent to a dozen of people saved on USB sticks containing all cables in unredacted form. [234]

With a physical response not really being an option, the challenges of a legal prosecution, and the decision not to escalate the cyber-conflict, the most effective piece of the government's response was arguably the public relations element. The four components are not mutually exclusive and any action relating to the former three certainly reinforce the fourth.

(IV) Public relations. In March 2008, an Army analyst prepared a 32-page report on WikiLeaks in response to the release of a document on the battle of Fallujah in November 2007. The report not only mentions WikiLeaks controversial status as a media organization, but more importantly identifies as a key vulnerability the trust WikiLeaks tries to convey to potential sources by ensuring an anonymous submission.[235]

The first release on Afghanistan did not yet produce a major public response by the Obama administration. Some argue that this is because that release largely dealt with the war strategy of President Obama's predecessor.[236] However, the Department of Defense set up an "Information Review Task Force" consisting of 120 people led by General Robert A. Carr from the Defense Intelligence Agency to review the cables but also to find evidence not only against source but also against Assange and WikiLeaks.[237]

The response to the release of the Iraq cables was similar, but the media reaction was more critical of the information revealed.[238] As a result and with the Cablegate release including many cables of the Obama administration itself, the government's response became more aggressive. The State Department set up a task force after learning about the impending release a few days in advance.[239] Secretary of State declared the release to be "not just an attack on America's foreign policy interests. It is an attack on the international community".[240] Vice President Biden stated that Assange is "more like a high-tech terrorist than the Pentagon Papers".[241] And Peter King,

[233] Domscheit-Berg: 21
[234] Domscheit-Berg: xiv+193
[235] Der Spiegel: 25
[236] Der Spiegel: 173
[237] Der Spiegel: 175-176
[238] Der Spiegel: 223
[239] Der Spiegel: 225; The Guardian: 199
[240] Der Spiegel: 2; Benkler: 15
[241] http://huffingtonpost.com/2010/12/19/joe-biden-wikileaks-assange-high-tech-terrorist_n_798838.html quoted in Benkler: 2

incoming Homeland Security Committee chair suggested to designate WikiLeaks as a "foreign terrorist organization".[242]

According to Der Spiegel, the government argued two ways: First, the cables reveal nothing new as mentioned in the President's speech in the Rose Garden, but that the information puts people's lives at risk.[243] The New York Times adds a third element with the government making the argument that by working with WikiLeaks, news organizations "compromised their impartiality and independence".[244] That fact that Assange considered himself to be a puppet master[245] with the news organizations as his puppets would underline this latter point.

With regard to the administration's relationship with the mainstream media itself, the White House sent an email to media organizations stating that WikiLeaks is not objective but against US.[246] The administration requested to withhold information to protect (i) informants, (ii) sensitive American programs, and (iii) counterterrorism efforts. Other than that, the administration focused on Manning who was already under arrest and on WikiLeaks.[247] However, the White House later added the request that any information relating to the national interest as well as the names of foreign dignitaries be withheld.[248] The New York Times reports to have "almost always agreed" to the first, "withheld some of the information" relating to the second and third, and to the fourth added later, having been "mostly unconvinced".[249]

Some have argued that the government's response stands in contrast to Secretary's Clinton Internet freedom speech at the Newseum in Washington in January 2010, describing the Internet as "a new nervous system for our planet […] In many respects, information has never been so free […] Even in authoritarian countries, information networks are helping people discover new facts and making governments more accountable".[250] Clinton's speech on February 15, 2011 was a response to this criticism reaffirming the administration's commitment to a free Internet explaining that "The fact that WikiLeaks used the internet is not the reason we criticized its actions. WikiLeaks does not challenge our commitment to internet freedom".[251]

(4) Alternative views. An alternative perspective on the government's response was given by Ron Paul, Republican Congressman from Texas and Presidential candidate, raising nine critical questions relating to WikiLeaks on the House floor on December 9, 2010.[252] In addition, The New York Times describes a discussion with Richard Holbrooke regarding WikiLeaks stating

[242] The Guardian: 202; The New York Times: 340
[243] Der Spiegel: 179-182
[244] The New York Times: 18
[245] The New York Times: 20
[246] Der Spiegel: 173
[247] Der Spiegel: 227
[248] Der Spiegel: 228-229
[249] The New York Times: 13
[250] http://www.state.gov/secretary/rm/2010/01/135519.htm
[251] www.stage.gov/secretary/rm/2011/02/156619.html
[252] The New York Times: 228-229

that “one of Holbrooke’s many gifts was his ability to make pretty good lemonade out of the bitterest lemons; he was already spinning the reports of Pakistani duplicity as leverage he could use to pull the Pakistanis back into closer alignment with American interests”.[253]

One could imagine a PR campaign that would target WikiLeaks while at the same time emulating Holbrooke’s thinking of actively using the information now publicly available as additional leverage for specific US foreign policy goals. The challenges of a PR campaign as a policy response are illustrated by the difficulty of separating Assange’s actions as a private individual and the charges against him in Sweden and his actions as a public figure. Another more questionable example are the various references to Manning’s homosexuality in the discussions of his role. (Those commentators seem to forget that his homosexuality did not prevent Alan Turing from serving his country and to break the Nazi’s Enigma code.)

I would add that the PR campaign against the naked transparency movement represented by Assange could have been stronger, if the government’s campaign would have included more elements to reassure its support for more balanced transparency initiatives and the open government project. This would have highlighted that the issue is not simply government vs. transparency or a binary transparency good/bad. Instead it could have encouraged people to a more nuanced assessment of transparency by underlining the government’s general commitment to transparency while focusing its counteractions on particular extreme case such as WikiLeaks.

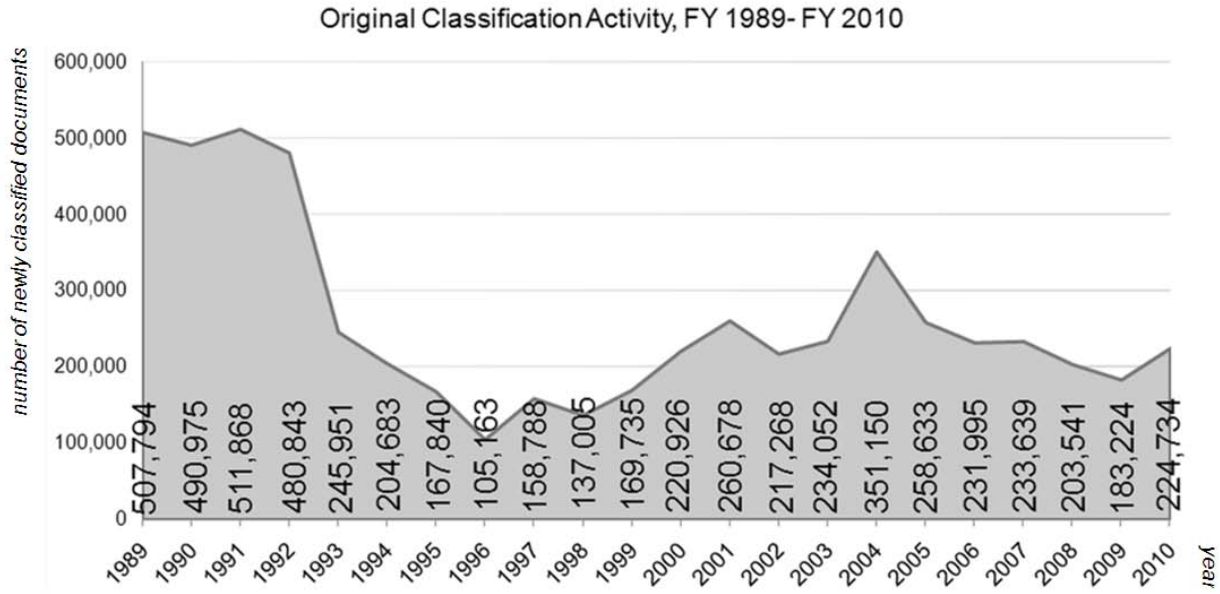
Such elements could have been, for example, an initiative to examine and possibly strengthen existing whistleblowing provisions and Congressional oversight. Or, a new commission looking at the issue of overclassification similar to the work of the bipartisan 1997 report of Commission on Protecting and Reducing Government Secrecy and the work of Senator Daniel Patrick Moynihan in the 1990s.[254] The tendency of government to overclassify has been extensively discussed in Moynihan’s book *Secrecy – The American Experience.* The commission’s main conclusion is that the government classifies “far too many documents at every stage, at far too great a cost, and that vital secrets were not adequately protected because of the vast volume of needlessly classified materials”[255]. This is explained by secrecy being an organizational asset and the interactions between governmental departments and agencies as the market in which secrets are exchanged.[256]

It is no secret that overclassification is still an issue today. In the context of WikiLeaks, for example, David Sanger from The New York Times raised the question, “when embassies compile clippings from the newspapers of the country that they are serving in, and send excerpts to the State Department, it is classified as secret?”[257] (unless you consider the selection itself to

[253] The New York Times: 9
[254] Moynihan
[255] Powers in Moynihan: 11
[256] Moynihan: 73
[257] Sanger - Shorenstein: 16

be sensitive information). In its most recent report, the Information Security Oversight Office published the figure of 183,224 new secrets for the fiscal year 2009. The trend overtime is shown in Figure 2 below.

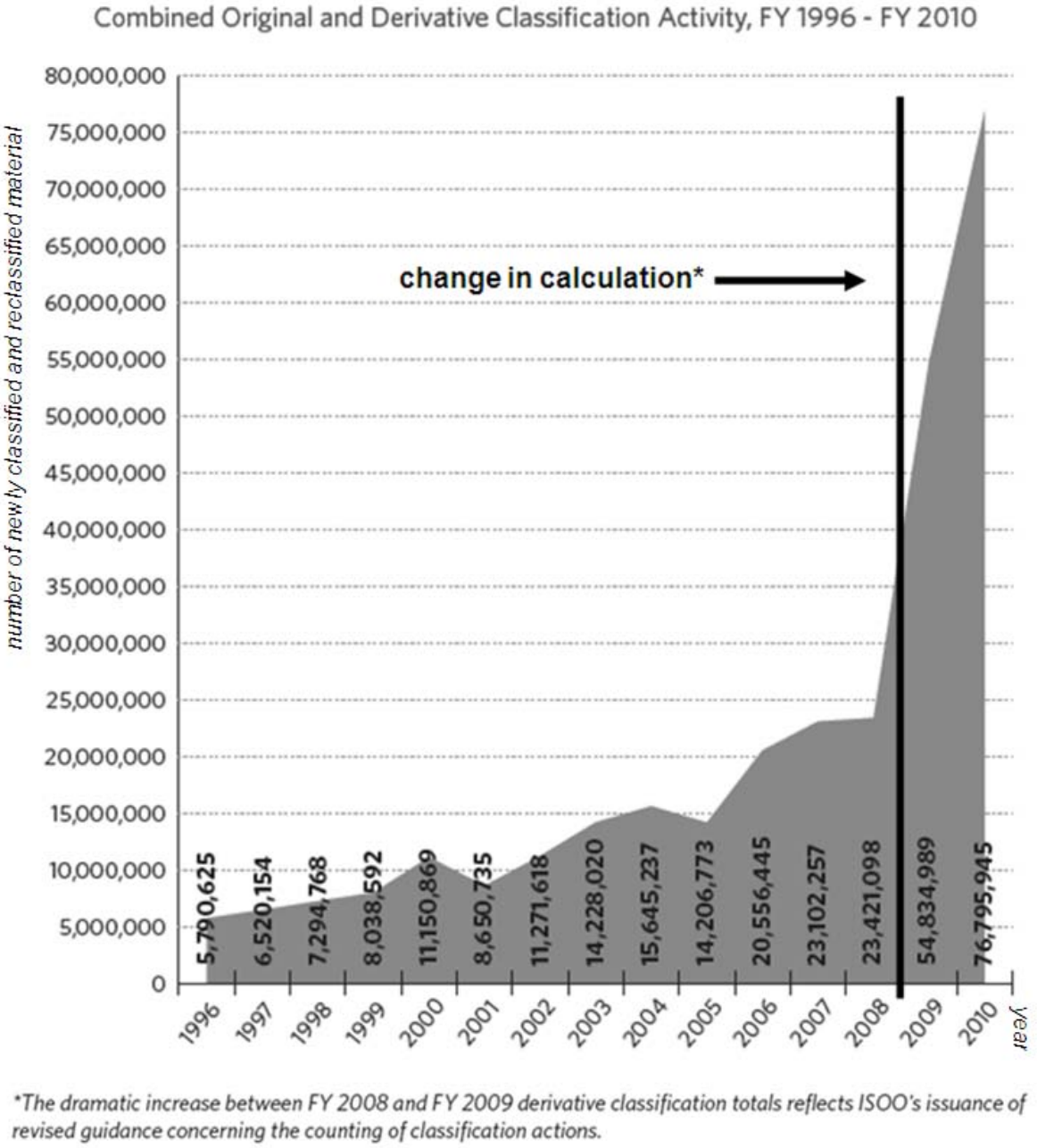
Figure 2



Combined with derivative classification, 'old secrets', the total amount of classified material stands at 54,834,989 illustrated in Figure 3. "Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form information that is already classified and, therefore, are not considered new 'secrets' "[258].

[258] ISOO: 7

Figure 3



**The dramatic increase between FY 2008 and FY 2009 derivative classification totals reflects ISOO's issuance of revised guidance concerning the counting of classification actions.*

[259]

A new commission would therefore not only have been a useful additional element of the PR campaign to prevent to alienate traditional supporters of the transparency and open government movement, but as outlined in the aforementioned conclusion of the commission would have also enabled the government to strengthen the protection of its vital secrets even more as it has already successfully done for its top secret material.

[259] ISOO: 9; ISOO (2010): 12

III. Is it a New Phenomenon?

In Nye's assessment, "If Assange had never been born, something like this would have happened anyway […] as Jonathan [Zittrain] said, it was in the DNA of the net".[260] That is why the real news of 2010 might have been WikiLeaks itself and not the cables. Interestingly, in their recent publications, two out of the three mainstream media outlets, The Guardian and Der Spiegel, involved in the 2010 releases did focus on WikiLeaks and their interaction with WikiLeaks rather than the content of cables themselves while The New York Times in its book *Open Secrets – WikiLeaks, War, and American Diplomacy* focuses mostly on the analysis of the cables.[261]

The Internet is also new in a different aspect. While in 1970s the government did nothing when a magazine published an article on how to build a nuclear bomb anticipating that it would simply disappear in the "fog of information"[262], the Internet somewhat lifts this fog by tools such as Google's search engine that pulls up anything ever published if searched.

Another important aspect of this new environment is highlighted by David Gordon, the former head for policy planning at the State Department, in a contribution for the Harvard Business Review.[263] He points out that WikiLeaks is not only a threat to governments but also to companies that might see their internal information exposed. Assange prominently announced a release exposing a financial institution in 2010, which has yet to become public.

Another indication of the new reality is the fact that WikiLeaks itself suffered from a leak.[264] Batches of the cables appeared in Lebanon, Australia, and Norway.[265] At the end of 2010 there are said to have been at least four additional individuals in possession of all the cables: Heather Brooke, a London-based American journalist and freedom of information activist, Daniel Ellsberg, Smari McCarthy, Icelandic former WikiLeaks programmer[266] and Holocaust-denying Israel Shamir.[267] Moreover, newspaper editors are said to have been very careful about saving documents in electronic form while preparing stories because they had correspondents all over the world working on it and were concerned it would be monitored.[268]

This shows that the key element to leaking is the human component. WikiLeaks is the first instance where this human activity was coupled with new technology and the transfer of information from the private network, SIPRNet, to the public network, the Internet. The fact that President Obama has overseen more charges against government officials for leaking classified material than any of his predecessors speaks to this new reality. That is why delinking Assange

[260] Nye - Shorenstein: 26
[261] The New York Times; The Guardian; Der Spiegel
[262] Nye - Shorenstein: 28
[263] Gordon
[264] Der Spiegel: 230
[265] The New York Times: 11, 243
[266] The Guardian: 165
[267] The Guardian: 174
[268] Male - Shorenstein: 108

from WikiLeaks as a technological platform is so important. Assange represents the potential revival of anarchists as a political force in the 21st century, while WikiLeaks stands for a new technology that can be used by anarchists, terrorists, or democrats alike.

The New York Times Max Frankel, Bill Keller's predecessor, wrote during the Pentagon Papers case

> "For the vast majority of 'secrets', there has developed between the government and the press (and Congress) a rather simple rule of thumb: The government hides what it can, pleading necessity as long as it can, and the press pries out what it can, pleading a need and a right to know. Each side in this 'game' regularly 'wins' and 'loses' a round or two. Each fights with the weapons at its command. When the government loses a secret or two, it simply adjusts to a new reality".[269]

WikiLeaks represents a significant shift in this balance of power. The sheer quantity of the material is no longer simply losing "a secret or two" making it much more painful for the government to adjust. The President of the New American Foundation, Steve Coll though states that "I'm skeptical about whether a release of this size is ever going to take place again […] in part because established interests and the rule of law tend to come down pretty hard on incipient movements. Think of the initial impact of Napster and what subsequently happened to them".[270]

This analogy to the music industry is very insightful and one also made by Zittrain. At the same time, Coll seems to neglect how the period of Napster and its aftermath of peer-to-peer networks have changed the music industry dramatically, with traditional data storage systems in rapid decline while iTunes enjoys further growth.[271]

Lessig's assessment therefore seems more accurate,

> "The network disables a certain kind of control. The response of those who benefitted from that control is a frantic effort to restore it. Depending on your perspective, restoration seems justified or not. But regardless of your perspective, restoration fails. Despite the best efforts of the most powerful, the control – so long as there is 'an Internet' – is lost".[272]

[269] The New York Times: 18
[270] The New York Times: 235
[271] The New York Times: 235
[272] Lessig: 41

Cyber-security implications. Lessig, however, goes on to say

> "But then what? If we can't go back, how do we go forward? For each of these problems, there have been solutions proposed that do not depend foolishly upon breaking the network. These solutions may not produce a world as good as the world was before (at least for some). They may not benefit everyone in the same way. But they are solutions that remove an important part of the problem in each case, and restore at least part of the good that is recognized in the past"[273]

The WikiLeaks affair has been described as an unintended consequence of the policy post 9/11 with its push to share more information. It has become clear that this policy shift neglected the protection of those information systems.[274] Consequently, in an immediate response to the release the State Department disconnected from SIPRNet.[275] The Air Force blocked access to The New York Times, 25 other news organizations and blogs having posted cables and to WikiLeaks itself.[276] The Department of Defense eventually changed its policy allowing no USB sticks, CD/DVDs on its systems and introducing new software monitoring data patterns to detect unusual activity as well as requiring two people to sign off if material is to be moved over the airgap from classified to unclassified networks.[277] An additional enhancement, Zittrain has suggested, is to design system that watermarks every document accessed by authorized system with your identity as tracking and real deterrent.[278]

The Office of Management and Budget, which is part of the White House, informed governmental agencies on December 3 that "Classified information, whether or not already posted on public websites or disclosed to the media, remains classified, and must be treated as such by federal employees and contractors, until it is declassified by an appropriate U.S. Government authority" declassify information.[279] This instruction includes the Library of Congress and according to Der Spiegel "There has never been something similar".[280] In addition, three senators proposed an "anti-leak" law declaring institutions like WikiLeaks to be a transnational threat providing a new legal basis.[281]

Yet, building on the aforementioned assessment and the net's DNA, even if cyber-security is significantly enhanced in the future, the architecture of the Internet always provides the possibility for a similar event from happening. We can therefore reduce the probability of its occurrence but not its inevitability statistically speaking. Using encryption is fairly easy and more or less simply a mouse click if the user downloaded the software. Using the Tor network

[273] Lessig: 41
[274] The New York Times: 339
[275] Ryan - Shorenstein: 66
[276] The New York Times: 237
[277] The New York Times: 340; Der Spiegel: 311
[278] Zittrain - Berkman
[279] The New York Times: 238; Benkler: 24
[280] Der Spiegel: 276
[281] Der Spiegel: 269

requires some conceptual knowledge for effective use but is also accessible to the layman. The key hurdle for any similar future incident is therefore less dependent on the technological skill level than the psychological barrier to enter the world of hacking and using and combining the publicly available tools and knowledge.[282]

Importantly, we must bear in mind the early days of WikiLeaks. The first documents released by WikiLeaks were obtained by hackers inside the Tor network.[283] They monitored Chinese hackers, who were reportedly tracked back to Guangzhou province in China, using the Tor network to secretly transfer material. According to Assange writing to Young in early 2007

> "Hackers monitor Chinese and other intel s they burrow into their targets, when they pull, so do we. Inexhaustible supply of material. Near 100,000 documents/emails a day. We're going to crack the world open and let it flower into something new… We have all of pre 2005 afghanistan. Almost all of india fed. Half a dozen foreign ministries. Dozens of political parties and consultes, worldbank, opec, UN sections, trade groups, Tibet and falun dafa associations and … Russian phishing mafia who pull data everywhere. We're drowning. We don't even know a tenth of what we have or who it belongs to. We stopped storing it at 1Tb (one terabyte, or 1,000 gigabytes)"[284]

These data flows were discovered by people associated with WikiLeaks in January 2007. (This was apparently unknown to many people inside WikiLeaks itself until the news broke in June 2010.[285]) It is a detail that so far has been largely neglected in the public debate. It shows that WikiLeaks made information public which we can assume foreign governments can or might already have accessed through secretive hacking.

[282] I thank Philipp Schroegel for his comments.
[283] The Guardian: 56
[284] The Guardian: 55; Der Spiegel 68-69
[285] Der Spiegel: 70

Conclusion

Assuming that the Internet will not be subject to a major redesign, something like WikiLeaks will always be part of it. How this new technology is used, for good or bad, depends on its human users. That is why it is important to delink Assange from WikiLeaks, in particular as some of the former member have left WikiLeaks to start their own projects such as Domscheit-Berg with openleaks.org[286]. It remains to be seen whether they will attract similar attention as the now established brand WikiLeaks.

Technology has always had an effect. When television entered the stage and C-SPAN Congress, the 'real' negotiations and deals in parliaments all over the world or at the United Nations no longer took place in the assembly halls now shown on TV but moved into the corridors instead. Maybe something similar will take place in diplomacy, and conversations will move from cables to emails or cell phones.

A serious concern highlighted by Harvard Professor Graham Allison addresses how to calibrate the policy response.[287] One of the reasons why such a leak was possible was the increase in information sharing after the attacks on September 11, 2001, in order to prevent future attacks. If this is simply replaced by the old system again in response to WikiLeaks, the question is what is likely to trigger greater harm: a future leak possibly including top secret material or a future terrorist attack that could not be prevented because crucial pieces of information did not come together?

A better response would be to learn from the past. After 9/11, the government focused on sharing more information while neglecting the protection of its information systems. Information sharing is still needed to more effectively prevent terror attacks by overcoming bureaucratic fragmentation. However, the protection of the information systems must not be neglected and the two are not mutually exclusive. Overall, the events of 2010 highlighted gaps in cyber-security and cyber-law which are likely to result in policy changes including President Obama's recent proposal for legislation in this context.[288]

If we like it not, the fact that the leaker, allegedly Bradley Manning, decided to submit the material to someone like Assange rather than channels within the military or traditional media shows that there are people who do not trust established mechanisms. Moreover, Domscheit-Berg points out that "What connected Julian [Assange] and me was the belief in a better world. In the world we dreamed of, there would be no more bosses or hierarchies, and no one could achieve power by withholding from the others the knowledge needed to act as an equal player. That was the idea for which we fought […] I still believe in the idea. I'm convinced the project

[286] Der Spiegel: 99
[287] Allison - Shorenstein
[288] http://www.nytimes.com/2011/05/13/us/politics/13obama.html?_r=1&ref=technology

itself was brilliant. Perhaps it was too brilliant to work the first time around"[289] Building on Der Spiegel's earlier observation linking Assange's hacktivism to anarchism, this might be the first public sign of a new international anarchist movement similar to the one Europe experience at the end of the 19th century. Last but not least, an entirely different discussion is needed to analyze governmental espionage since WikiLeaks has shown the public only what seems to be already secretly accessed by foreign governments.

[289] Domscheit-Berg: 4

Works Cited

Benkler, Yochai. “A Free Irresponsible Press: WikiLeaks and the Battle over the Soul of the Networked Fourth Estate”. *Harvard Civil Rights-Civil Liberties Law Review*. (forthcoming)

Berkman Center for Internet and Society. *Radio Berkman 171: WikiLeaks and the Information Wars - Transcript*. December 7, 2010. Last accessed April 21, 2011. <http://blogs.law.harvard.edu/mediaberkman/2010/12/08/radio-berkman-171/>

Bradbury, Steven G. “The Developing Legal Framework for Defensive and Offensive Cyber Operations – Keynote Address Harvard National Security Journal Symposium ‘Cybersecurity: Law, Privacy, and Warfare in a Digital World’ March 4, 2011”. 2.2 *Harvard National Security Journal*. (forthcoming)

Chiesa, Raoul. *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*. Turin: UNICRI, 2008.

Clarke, Richard A. and Robert Knake. *Cyber War : The Next Threat to National Security and What To Do About It*. Ecco, April 2010.

Clinton, Hillary Rodham. *Internet Rights and Wrongs: Choices and Challenges in a Networked World*. Washington, DC: 15 February 2011. Last accessed May 14, 2011. <www.stage.gov/secretary/rm/2011/02/156619.html>

Crovitz, L. Gordon. “WikiLeaks and the Espionage Act”. *The Wall Street Journal* (April 25, 2011) Last accessed May 14, 2011. < <http://online.wsj.com/article/SB10001424052748703387904576278883412892972.html >

Davis, Michael “Whistleblowing,” in Hugh LaFollette, ed., *The Oxford Handbook of Practical Ethics* (2003), pp. 539-63.

Department of Defense. News Briefing with Secretary of Defense Donald Rumsfeld and Gen. Peter Pace. (November 29, 2005). Last accessed June 12, 2011. <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=1492>

Der Spiegel - Rosenbach, Marcel and Holger Stark. *Staatsfeind WikiLeaks – Wie eine Gruppe von Netzaktivisten die maechtigsten Nationen der Welt herausfordert*. Deutsche Verlags-Anstalt: Muenchen, 2011.

Domscheit-Berg, Daniel. *Inside WikiLeaks – My Time with Julian Assange at the World’s Most Dangerous Website*. Crown Publishers: New York, 2011.

Goldsmith , Jack. “Seven Thoughts About WikiLeaks”. *Lawfareblog* (December 10, 2010) Last accessed May 14, 2011. <www.lawfareblog.com/2010/12/seven-thoughts-on-wikileaks>

Gordon, David and Sean West. “Could WikiLeaks Expose Your Corporate Brain?” *Harvard Business Review (*December 13, 2010). Last accessed April 21, 2011. <http://blogs.hbr.org/cs/2010/12/could_wikileaks_expose_your_co.html>

Information Security Oversight Office. *Annual Report to the President 2009*. Last accessed May 14, 2011. <http://www.archives.gov/isoo/reports/>

--. *Annual Report to the President 2010*. Last accessed May 14, 2011. <http://www.archives.gov/isoo/reports/>

Fitzpatrick, John Fitzpatrick. *Hearing on Security Clearance Policy Subcommittee on Intelligence Community Management House Permanent Select Committee on Intelligence* (December 1, 2010). Last accessed May 14, 2011. <www.fas.org/sgp/news/2010/12/clearances.html>

Frontline. *Bradley Manning’s Facebook Page*. Last accessed June 12, 2011. <http://www.pbs.org/wgbh/pages/frontline/wikileaks/manning-facebook-page/>

Lessig, Lawrence. “Against Transparency – The perils of openness in government”. *The New Republic* (October 21, 2009).

March, James G. and Johan P. Olsen. “The Institutional Dynamics of International Politics” *International Organization* 52.4 (Autumn 1998)

Masnick, Mike. “Since When Is It Illegal To Just Mention A Trademark Online?” techdirt (January 5, 2005). Last accessed June 12, 2011. <http://www.techdirt.com/articles/20050105/0132239.shtml>

McConnell, Terrance. “Whistle-blowing,” in R. G. Frey and Christopher Heath Wellman, eds., *A Companion to Applied Ethics* (2003), pp. 570-582.

Moynihan, Daniel Patrick. *Secrecy – The American Experience*. Yale University Press: New Haven & London, 1998.

Nye Jr, Joseph S.. “WikiLeaks and Internet Freedom”. *The Financial Times* (March 9, 2011) Last accessed May 14, 2011. <http://www.ft.com/cms/s/595fd0c4-49bd-11e0-acf0-00144feab49a,Authorised=false.html?_i_location=http%3A%2F%2Fwww.ft.com%2Fcms%2Fs%2F0%2F595fd0c4-49bd-11e0-acf0-00144feab49a.html&_i_referer=http%3A%2F%2Fyaleglobal.yale.edu%2Fcontent%2Famerica-should-not-prosecute-julian-assange >

--. *The Future of Power*. PublicAffairs: New York, 2011.

Oxford Dictionaries. “Hacktivist&Cypherpunk”. Last accessed August 10, 2011. <http://oxforddictionaries.com/definition/hacktivist?region=us>

Poulsen, Kevin and Kim Zetter. “U.S. Intelligence Analyst Arrested in WikiLeaks Video Probe” *Wired* (6 June 2010) Last accessed May 14, 2011. <http://www.wired.com/threatlevel/2010/06/leak/>

Shorenstein Center on the Press, Politics and Public Policy. *Executive Session on WikiLeaks.* Cambridge: Joan Shorenstein Center on the Press, Politics and Public Policy, Harvard Kennedy School, February 3, 2011.

Sifry, Micah L. *WikiLeaks and the Age of Transparency*. Counterpoint: Berkeley, California, 2011.

The Guardian – Leigh, David and Luke Harding. *WikiLeaks – Inside Julian Assange’s War on Secrecy*. PublicAffairs: New York, 2011.

The New York Times. Jolly, David and Raphael Minder. *Spain Detains 3 in PlayStation Cyberattacks.* (June 10, 2011). Last accessed June 12, 2011. < http://www.nytimes.com/2011/06/11/technology/11hack.html?scp=4&sq=anonymous&st=cse>

--. Reuters. *Ex-Official for N.S.A. Accepts Deal in Leak Case*. (June 10, 2011). Last accessed June12, 2011. < http://www.nytimes.com/2011/06/11/us/11justice.html?_r=1&scp=1&sq=leak&st=cse>

--. Share, Scott. *Ex-N.S.A. Aide Gains Plea Deal in Leak Case; Setback to U.S.* (June 9, 2011). Last accessed June 12, 2011.<http://www.nytimes.com/2011/06/10/us/10leak.html>

--. Star, Alexander. *Open Secrets – WikiLeaks, War and American Diplomacy*. Grove Press: New York, 2011.

The Times. “Man named by WikiLeaks ‘war logs’ already dead’ (July 29, 2010) Last accessed May 14, 2011. <http://www.thetimes.co.uk/tto/news/world/asia/afghanistan/article2664166.ece>

U.S Code / Title 10 – Armed Forces / Subtitle A – General Military Law / Part II – Personnel / Chapter 53 – Miscellaneous Rights and Benefits / Section 1034 – Protected communications; prohibition of retaliatory personnel actions

Wall Street Journal. *SafeHouse*. Last accessed May 16, 2011. < https://www.wsjsafehouse.com/>

--. *Wall Street Journal Statement Regarding SafeHouse Security Measures and Anonymity*. Last accessed May 16, 2011. < http://www.dowjones.com/pressroom/presskits/safehouse.asp>

Wikipedia.org. *United States diplomatic cables leak*. Last accessed May 16, 2011. <http://en.wikipedia.org/wiki/United_States_diplomatic_cables_leak#cite_note-5>

--. *Streisand effect*. Last accessed June 12, 2011. <http://en.wikipedia.org/wiki/Streisand_effect>

Wu, Tim and Jack Goldsmith. *Who Controls the Internet – Illusions of a Borderless World*. Oxford: Oxford University Press, 2008.

Zittrain, Jonathan. *The Future of the Internet – And How To Stop It*. New Haven: Yale University Press, 2008.

Figure 4 copyright reference:

GNU Free Documentation License. Last accessed May 15, 2011. <http://commons.wikimedia.org/wiki/File:Globe.png>

Appendix: Known Members of WikiLeaks

2006 Julian Assange claims WikiLeaks consists of 22 people but only half a dozen are known[i]: 'The Nanny', an old friend of Assange's around 40 years old[ii]; a South African; a German volunteer; Assange's girlfriend; [iii] Daniel Mathews, an Australian political activist[iv]; and Ben Laurie, the prominent British developer of the Apache software[v]

2007 Daniel Domscheit-Berg meets Assange at 24th Chaos Communication Congress in Berlin in December[vi]

2008 'The Technician' joins[vii]

2009 Domscheit-Berg, leaves his full-time job on January 31 to become WikiLeaks second speaker for WikiLeaks under the pseudonym Daniel Schmitt[viii]; 'The Architect', a German programmer, joins in early 2009[ix]; Jacob Appelbaum[x]; Birgitta Jonsdottir, Icelandic Member of Parliament, joins in the summer as a result of WikiLeaks release of documents from the Kaupthing Bank in July[xi]; Rop Gonggrijp, Dutch hacker, meets Assange at a conference in Malaysia[xii]

2010 (Icelandic Modern Media Initiative) Icelandic journalist Kristinn Hrafnasson and cameraman Ingi Ragnar Ingason travel to Baghdad to factcheck video[xiii] promoted to regular members of WikiLeaks team[xiv]; Smari McCarthy, Icelandic former WikiLeaks programmer[xv]; Herbert Snorrason, Icelander[xvi]

August 25: The Architect and Technician put WikiLeaks into maintenance mode without Assange's prior approval[xvii]; August 26: Assange suspends Domscheit-Berg[xviii]

September 15: Birgitta Jonsdottir[xix] leaves WikiLeaks and subsequently a dozen others[xx] including the Icelandic Herbert Snorrason[xxi] and The Architect[xxii]

September 17: Domscheit-Berg registers the domain openleaks.org[xxiii], The Architect joins him to work on OpenLeaks[xxiv], and Domscheit-Berg reveals his real name in an interview at the end of September[xxv]

2011 WikiLeaks includes new members from Assange's time in London such as Joseph Farrell from Swaziland and Sarah Harrison, both recent journalistic interns[xxvi] as well as a person from the French La Quadrature du Net[xxvii]; James Ball, a former reporter for Grocer trade magazine who is reported to be the new WikiLeaks spokesman[xxviii] although Domscheit-Berg says Hrafnsson is the new spokesman[xxix]; and the controversial Israel Shamir[xxx]

[i] Der Spiegel: 61
[ii] Domscheit-Berg: 80
[iii] Der Spiegel: 72
[iv] Der Spiegel: 61
[v] Der Spiegel : 73
[vi] Domscheit-Berg: xi
[vii] Domscheit-Berg: 122-123
[viii] Domscheit-Berg: xii+93; Der Spiegel: 95
[ix] Domscheit-Berg: 122-123; Der Spiegel: 207
[x] Der Spiegel: 116
[xi] The Guardian: 68; Domscheit-Berg: 119
[xii] Domscheit-Berg: xiii
[xiii] Der Spiegel: 121
[xiv] Domscheit-Berg: 154
[xv] The Guardian: 165
[xvi] The Guardian: 167
[xvii] Domscheit-Berg: 222
[xviii] Domscheit-Berg: xiv+227
[xix] Der Spiegel: 115
[xx] Domscheit-Berg: xiv; The New York Times: 41; Der Spiegel: 199
[xxi] Der Spiegel: 205-206
[xxii] Der Spiegel: 207
[xxiii] Domscheit-Berg: xiv+239
[xxiv] Domscheit-Berg: 240
[xxv] Der Spiegel: 204
[xxvi] Der Spiegel: 208; The Guardian: 14, 17
[xxvii] Der Spiegel: 209
[xxviii] The Guardian: 16
[xxix] Domscheit-Berg: 154
[xxx] The Guardian: 174

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138
Fax: (617) 495-8963
Email: belfer_center@harvard.edu
Website: http://belfercenter.org