TERRORIZING WIKILEAKS: WHY THE EMBARGO AGAINST WIKILEAKS WILL FAIL

SAMUEL C. CANNON*

> *[W]hat steps were taken to stop Wikileaks director Julian Assange from distributing this highly sensitive classified material especially after he had already published material not once but twice in the previous months?*
>
> *He is an anti-American operative with blood on his hands . . . . Why was he not pursued with the same urgency we pursue al-Qaeda and Taliban leaders?*[1]

* The author is a J.D. candidate in the class of 2013 at the University of Colorado Law School. He thanks Professor Paul Ohm and David Cline for their comments that helped develop this paper.

1. Martin Beckford, *Sarah Palin: hunt WikiLeaks founder like al-Qaeda and Taliban leaders*, THE TELEGRAPH (Nov. 30 2010),

INTRODUCTION

The self-styled whistle-blowing website WikiLeaks blazed to international prominence in April of 2010 by releasing a video titled *Collateral Murder*. This video allegedly shows a United States apache attack helicopter firing into a crowd of people, killing many, including two members of the Reuters News agency.[2] Eight months later, WikiLeaks along with its mainstream media partners began to release over 250,000 classified cables written by American diplomats.

Since beginning to publish the embassy cables, WikiLeaks has been under attack. The website was targeted by distributed denial of service ("DDOS") attacks, American companies stopped providing network services to WikiLeaks, and financial services companies stopped processing donations to WikiLeaks.[3] At least some of these actions seem to have come at the request of the United States government.[4] In addition, as the above quote shows, politicians publically condemned WikiLeaks. Some even described the website as a terrorist organization and a threat to national security.[5] On October 24, 2011, WikiLeaks announced that it was suspending publication of leaked documents to concentrate on raising money.[6]

Professor Yochai Benkler has suggested that this public-private partnership in censorship is inconsistent with the type of freedom to which the United States is committed. He argues that this process circumvents traditional First Amendment protections because the speech-chilling actions are taken by private actors, not the government.[7]

---

http://www.telegraph.co.uk/news/worldnews/wikileaks/8171269/Sarah-Palin-hunt-WikiLeaks-founder-like-al-Qaeda-and-Taliban-leaders.html (quoting posts from Palin's Facebook page).

2. *Collateral Murder Overview*, WIKILEAKS, https://www.collateralmurder.com/ (last visited Nov. 24, 2012).

3. Elissa Fink, *Why we removed the WikiLeaks visualizations*, TABLEAU SOFTWARE (Dec. 1, 2010), http://www.tableausoftware.com/about/blog/2010/12/why-we-removed-WikiLeaks-visualizations; Charles Arthur & Josh Halliday, *WikiLeaks fights to stay online after US company withdraws domain name*, THE GUARDIAN (Dec. 3, 2010), http://www.guardian.co.uk/media/blog/2010/dec/03/wikileaks-knocked-off-net-dns-everydns?INTCMP=SRCH.

4. Charles Arthur & Josh Halliday, *WikiLeaks fights to stay online after US company withdraws domain name*, THE GUARDIAN (Dec. 3, 2010), http://www.guardian.co.uk/media/blog/2010/dec/03/wikileaks-knocked-off-net-dns-everydns?INTCMP=SRCH.

5. *See, e.g.*, Beckford, *supra* note 1; *Lieberman Condemns New WikiLeaks Disclosures*, JOE LIEBERMAN UNITED STATES SENATOR FOR CONNECTICUT (Nov. 28, 2010), http://lieberman.senate.gov/index.cfm/news-events/news/2010/11/lieberman-condemns-new-wikileaks-disclosures.

6. Esther Addley & Jason Deans, *WikiLeaks suspends publishing to fight financial blockade*, THE GUARDIAN (Oct. 24, 2011), http://www.guardian.co.uk/media/2011/oct/24/wikileaks-suspends-publishing.

7. Yochai Benkler, *A Free Irresponsible Press: WikiLeaks and the Battle Over the Soul of the Networked Fourth Estate*, 46 HARV. C.R.-C.L. L. REV. 311, 330-31 (2011).

Benkler further asserts that the rhetoric linking WikiLeaks to the "War on Terror" greatly enhanced the pressure felt by private actors to cease dealing with WikiLeaks.[8] This note further explores the connections between the treatment of terrorist organizations in the wake of the September 11, 2001 attacks on New York and Washington D.C. and the disruption felt by WikiLeaks after the publication of the embassy cables.

Part I describes the attacks on terrorist websites in the wake of the September 11, 2001 terrorist attacks on the World Trade Center, showing how websites can be censored through attacks or pressure on the intermediaries of Internet communication. Part II details the history of WikiLeaks and the subsequent attempts to prevent the website from publishing leaked documents. Part III discusses the differences between WikiLeaks and terrorist organizations and predicts that attempts to shut down WikiLeaks using tactics from the fight against terrorist websites will fail.

I. ATTACKS ON TERRORIST WEBSITES

> *We'll have to deal with the networks. One of the ways to do that is to drain the swamp they live in. And that means dealing not only with the terrorists, but those who harbor terrorists. This will take a long, sustained effort. It will require the support of the American people as well as our friends and allies around the world.*[9]

In the aftermath of the September 11, 2001 terrorist attacks on the World Trade Center, terrorist websites were removed from the Internet by the combined efforts of the government and private actors. Professor Gregory S. McNeal has described the multi-step process that has resulted in the failure of these websites.[10] Step 1, US organizations that provide services to the terrorist website are pressured into cutting their ties to the terrorist website by a combination of public shaming and the threat of criminal action under the "Material Support for Terrorist Organizations" statutes. Step 2, once the website has been forced to seek out foreign service providers, the foreign companies must be pressured by their non-terrorist customers to cease dealing with the terrorist website.[11] This process relies on an implicit Step 0: that operating a terrorist website is criminal and that offering material support to such a website is also criminal.

---

8. *Id.* at 333.

9. Press Release, U.S. Dep't of Def., DoD News Briefing - Secretary Rumsfeld (Sep. 18, 2001), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=1893.

10 Gregory S. McNeal, *Fighting Back Against Terrorist Websites*, 13 No. 2 J. Internet L. 1 (2009) [hearinafter McNeal, *Terrorist Websites*].

11. *Id.* at 1-2.

Two recent examples show how this process can succeed in removing terrorist websites from the web: (A) the campaign against Palestinian Islamic Jihad's website, and (B) the attack on Al Qaeda's website, alneda.com.

A. Palestinian Islamic Jihad (PIJ)

According to the U.S. State Department, PIJ is a foreign terrorist organization.[12] PIJ aims to establish a sovereign Islamic Palestinian state in the area covered by pre-1948 mandate Palestine. As part of this aim, PIJ is devoted to the destruction of the state of Israel and eschews negotiation with Israel in favor of violence.[13] Since the year 2000, PIJ has claimed involvement in at least six bombings in Israel, which together killed 80 people.[14] In 2006, PIJ boasted that the FBI was incapable of shutting the organization's websites down.[15]

After PIJ's boast, a private organization, Internet Haganah, posted information to its own website detailing three US companies that were providing Internet services to PIJ. In addition, Internet Haganah encouraged readers to contact the US companies and demand that they stop doing business with terrorist organizations.[16] Because materially supporting terrorists carries significant criminal liability,[17] US companies are unwilling to knowingly provide services to organizations listed as foreign terrorist organizations. Shortly after this shaming campaign, the PIJ Web site shifted its operation to overseas Internet service providers (ISPs) that are beyond the reach of US laws.[18]

Although the private shaming campaign did not remove PIJ from the web completely, McNeal suggests that a second stage embargo against foreign ISP's might have succeeded. If the US were to maintain a list of foreign companies who provide services to terrorist websites, the government might be able to shame US organizations from dealing with the listed companies. Thus, no company who wanted to do business with US entities would be willing to provide Internet services to terrorist groups.[19]

---

12. *Foreign Terrorist Organizations*, U.S. DEPARTMENT OF ST., http://www.state.gov/j/ct/rls/other/des/123085 htm (last visited Nov. 25, 2012).

13. *See* Holly Fletcher, *Palestinian Islamic Jihad*, COUNCIL ON FOREIGN REL. (Apr. 10, 2008), http://www.cfr.org/israel/palestinian-islamic-jihad/p15984#8.

14. *Id.*

15. *See* Gregory S. McNeal, *Cyber Embargo: Countering the Internet Jihad*, 39 CASE W. RES. J. ITN'L L. 789, 791 (2007) [hearinafter McNeal, *Cyber Embargo*].

16. McNeal, *Terrorist Websites*, *supra* note 10, at 1.

17. *See* 18 U.S.C. § 2339B (2006) (effective Dec. 1, 2009) (punishing knowing provision of material support, including communication services, by up to fifteen years imprisonment).

18. McNeal, *Cyber Embargo*, *supra* note 15, at 9.

19. *See* McNeal, *Terrorist Websites*, *supra* note 10, at 793.

The campaign against PIJ was primarily a private one. Internet Haganah carried out the shaming campaign, and McNeal's suggested embargo would have relied on private companies deciding not to deal with the foreign companies who provide services to terrorists. The removal of Al Qaeda's primary website from the Internet also displays the power private actors can wield in disrupting terrorist organizations' online activities.

B. Al Qaeda

While it existed, alneda.com was Al Qaeda's Internet headquarters. The site first appeared in March 2001 and was active until July 2002.[20] The website contained editorials from major Al Qaeda leaders, videos of Osama Bin Laden, calls for terrorist action, and a message board containing coded messages for members of Al Qaeda.[21] Alneda.com was hosted by a Malaysian ISP: Malaysia Technology Development Corporation.[22]

Nearly a year after the September 11, 2001 attacks in New York and Washington D.C., an American Internet entrepreneur decided to attack Islamic extremists online. Jon Messner owned an amateur-housewife-next-door-style pornography website.[23] Shocked by the attacks on the World Trade Center, Messner began researching Al Qaeda and translating extremist websites.[24] Seeing that some of the sites were focused entirely on terrorism and killing Americans, Messner used skills he had acquired running his website to interfere with Al Qaeda's online presence.[25]

Rather than illegally take down the website, Messner decided to target alneda.com's ISP to take control of the website legally.[26] Realizing that a website dedicated to terrorism could not use genuine contact information in its registration, Messner formed a two-step plan. First, Messner registered for the alneda.com domain name with a service called snapname, which registers a domain name to the customer if the current domain name registration expires. Next, Messner contacted the Malaysian ISP the site was using and reported alneda.com for using false

20 Patrick Di Justo, *How Al-Qaida Site Was Hijacked*, WIRED (Aug. 10, 2002), http://www.wired.com/culture/lifestyle/news/2002/08/54455?currentPage=all.

21. *Id.*

22. *Id.*

23. Mike Boettcher, *Pornographer says he hacked al Qaeda*, CNN (Aug. 8, 2002), http://articles.cnn.com/2002-08-08/us/porn.patriot_1_qaeda-internet-site-web-site?_s=PM:US.

24. Jon Messner, *Al-qaeda and the rest of the story as you may not know or care*, ALNEDA.COM, http://www.alneda.com/ (last visited November 27, 2012) (site redirects to www.itshappening.com shortly after loading).

25. Boettcher, *supra* note 23.

26. Di Justo, *supra* note 20.

contact information in violation of the ISP's terms of service. On July 12, 2002, the ISP dropped the alneda.com registration, and Messner became the new owner of the domain name. [27]

In one of the stranger episodes of the war on terror, the FBI failed to capitalize on Messner's control of one of the largest terrorist websites in the world. Once Messner was in control of the alneda.com domain name, he uploaded a duplicate version of the website so it appeared to outsiders that there had just been a brief outage on the site.[28] Messner's server was then logging the IP addresses of every visitor to Al Qaeda's website, most of which were from Saudi Arabia.[29] Aware of how important this information could be, Messner contacted the FBI. According the Messner, the agent who came to his house was not an Internet expert, and by the time an Internet expert was reached, Messner's ruse had been discovered.[30] A message appeared on another extremist website, "The infidels have taken over the site. They are tracking you. The man doing this is an infidel, a pornographer."[31] In response, Messner changed the homepage of alneda.com to an image of the great seal of the United States above the text, "Hacked, tracked, and NOW 0wned [sic] by the U.S.A.," and a description of what he had done.[32]

For some time after Messner's attack, the website formally known as alneda.com existed as a parasite buried within subdirectories of other websites.[33] The websites of a fourteen-year-old student, a security consultancy, a fan page of horror movie director Clive Baker, and a Dutch educational consultancy have all unwittingly hosted the site at one time or another.[34] According to the ISP that hosted some of the commandeered sites, the National Security Agency ("NSA") had requested they temporarily leave the site alone so that the NSA could monitor it.[35] It is unclear whether alneda.com still exists in some form. But, when it existed as a parasite, updates were far less frequent than before Messner's attack.[36]

The attacks on PIJ and alneda.com both show how effective private action against a website can be when there is the implicit threat of criminal liability for supporting terrorist websites. This use of private

27. Messner, *supra* note 24.
28. Di Justo, *supra* note 20.
29. *Id.*
30. *Id.*
31. Boettcher, *supra* note 23.
32. *See* Messner, *supra* note 24.
33. Michelle Delio, *Al Qaeda Website Refuses to Die*, WIRED (Apr. 7, 2003), http://www.wired.com/techbiz/it/news/2003/04/58356?currentPage=1.
34. *Id.*
35. *Id.*
36. *Id.*

pressure, as described by McNeal, has thus been very successful. Accordingly, it is no surprise that similar methods have been used against WikiLeaks.

II. WIKILEAKS

> *It is unfortunate that it took Amazon five months to terminate its relationships with WikiLeaks, and only after having political pressure applied. While I wish that Amazon had taken this step when U.S. soldiers' lives were first put in danger by WikiLeaks back in July, I am heartened that the company has finally corrected its action.*[37]

WikiLeaks's stated goal is to bring important news and information to the public by providing a secure and anonymous electronic drop box where sources can leak information.[38] WikiLeaks is a project of the Sunshine Press,[39] which is incorporated in Iceland,[40] and it is run by a mostly unknown group operating from a number of countries around the world. Julian Assange, WikiLeaks's founder and editor-in-chief, is an Australian citizen, but he claims to have no fixed address.[41]

The story of WikiLeaks can be broken into three sections: (A) the website's publications, (B) the backlash against the publication of US diplomatic cables, and (C) the reaction to this backlash.

A. WikiLeaks' Publications

Although WikiLeaks was formed in late 2006, WikiLeaks did not begin publishing US government material until December 2007. First came the Standard Operating Procedures for Camp Delta from the prison operated by the US Navy in Guantanamo Bay, Cuba.[42] The manual allowed prisoners to be denied access to the Red Cross for up to four weeks and detailed how toilet paper could be used as a reward for good

37. *Rep. Peter King Statement on WikiLeaks-Amazon.com Relationship*, CONGRESSMAN PETER KING (Dec. 1, 2010), http://www house.gov/apps/list/hearing/ny03_king/wikileaksamazon html.

38. *About*, WIKILEAKS, http://wikiLeaks.org/About html (last visited Mar. 9, 2012) [hereinafter WikiLeaks].

39. *Id.*

40. Certificate of Incorporation Sunshine Press Productions, *available at* http://www.scribd.com/WikileaksCrimeGroup/d/47601520-SUNSHINE-PRESS-PRODUCTIONS-EHF-FOR-PROFIT-LIMITED-COMPANY-DOCUMENTS.

41. *WikiLeaks' Assange Jailed While Court Decides on Extradition*, CNN (Dec. 7, 2010), http://articles.cnn.com/2010-12-07/world/uk.wikileaks.investigation_1_wikileaks-founder-julian-assange-extradition-european-arrest-warrant?_s=PM:WORLD.

42. *WikiLeaks: a timeline of the site's top scoops*, THE TELEGRAPH, http://www.telegraph.co.uk/news/worldnews/7911497/WikiLeaks-a-timeline-of-the-sites-top-scoops html (last visited Mar. 9, 2012) [hereinafter WikiLeaks Timeline].

behavior.[43] This was followed by publication of emails from then-vice-presidential candidate Sarah Palin's private email account that showed that Palin was using her private account for official business, supposedly to circumvent Freedom of Information Act requests.[44]

In 2008, WikiLeaks was awarded the Economist Index on Censorship Freedom of Expression award, and in 2009, it won the Amnesty International Human Rights Reporting award for the "New Media" category.[45] However, few of its publications during this time were directed at the US.[46] Instead, WikiLeaks's publications in this period included the so-called "secret bible" of Scientology,[47] an internal report by Trafigura discussing the health effects of waste dumping in Africa, emails from the Climate Research Unit at the University of East Anglia in the UK,[48] and reports of an accident at a nuclear facility in Iran.[49]

WikiLeaks published the *Collateral Murder* video in April 2010. The video shows an attack by two Apache helicopters on a group of suspected insurgents in Baghdad on July 12, 2007. The attack, however, killed twelve people including Reuters photographer Namir Noor-Eldeen and his driver, Saeed Chmagh, and wounded two children.[50] The video consists of footage from the gunsight-target-acquisition system from one of the Apache helicopters and contains audio of the helicopter pilots talking to each other during the attack.[51] The video prompted a response from US Secretary of Defense Robert Gates, who stated, "These people can put out anything they want, and they're never held accountable for it. There's no before and there's no after."[52]

Between June and November, 2010, Assange entered into agreements with El Pais, La Monde, The New York Times, Der Spiegel,

43. *Id.*

44. *Id.*

45. WikiLeaks, *supra* note 38.

46. WikiLeaks Timeline, *supra* note 42.

47. Cade Metz, *Scientology threatens WikiLeaks with injunction*, THE REGISTER (Apr. 8, 2008), http://www.theregister.co.uk/2008/04/08/church_of_scientology_contacts_wikileaks/.

48. WikiLeaks Timeline, *supra* note 42.

49. *Serious nuclear accident may lay behind Iranian nuke chief's mystery resignation*, WIKILEAKS (July 16, 2009), http://mirror.wikileaks.info/wiki/Serious_nuclear_accident_may_lay_behind_Iranian_nuke_chief%27s_mystery_resignation/.

50. Elisabeth Bumiller, *Video Shows U.S. Killing of Reuters Employees*, N.Y. TIMES (Apr. 5, 2010), http://www nytimes.com/2010/04/06/world/middleeast/06baghdad html.

51. David Alexander & Phillip Stewart, *Leaked U.S. video shows deaths of Reuters' Iraqi staffers*, REUTERS (Apr. 5, 2010, 8:39 PM), http://www reuters.com/article/2010/04/06/us-iraq-usa-journalists-idUSTRE6344FW20100406.

52. Phil Stewart & Deborah Zabarenko, *Gates assails Internet group over attack video*, REUTERS (Apr. 13, 2010, 7:00 PM), http://www.reuters.com/article/2010/04/13/us-iraq-usa-journalists-idUSTRE63C53M20100413.

and The Guardian, leading newspapers in Spain, France, the US, Germany, and the UK to publish over 250,000 cables between the US state department and US embassies around the world.[53] These media organizations began to publish selected cables on November 29, 2011, over the objection of the US Department of State.[54] The cables disclosed, among other things, that a team of American Special Forces had been operating inside Pakistan, that Saudi Arabia had pressured the United States to attack Iran, and that American diplomats believed Russia to be a "virtual mafia state."[55] In total, WikiLeaks published 251,287 cables between 274 embassies, including over 100,000 classified documents, of which 15,652 were given the higher classification "secret."[56]

The reaction to WikiLeaks' publication of the Cables was instant. On the first day the cables were published, Hilary Clinton, US Secretary of State stated, "This disclosure is not just an attack on America – it's an attack on the international community."[57] Sarah Palin responded by stating that Assange had "blood on his hands" and asked the rhetorical question, "Why was he not pursued with the same urgency we pursue al Qaeda and Taliban leaders?"[58] Not all reaction was so severe. Defense Secretary Gates summed up the incident as follows, "Is this embarrassing? Yes. Is it awkward? Yes. Consequences for U.S. foreign policy? I think fairly modest.''[59] The reactions of Clinton and Palin were more representative of the US government's response to Wikileaks,

53. Bill Keller, *Dealing With Assange and the WikiLeaks Secrets*, N.Y. TIMES (Jan. 26, 2011), http://www nytimes.com/2011/01/30/magazine/30Wikileaks-t html?ref=world; Javier Moreno, *Why EL PAÍS chose to publish the leaks*, EL PAIS (Dec. 23, 2010), http://www.elpais.com/articulo/english/Why/PAIS/chose/to/publish/the/leaks/elpepueng/20101223elpeng_3/Ten.

54. Letter from Harold Koh, Legal Advisor, United States Dep't of State, to Jullian Assange, Founder of WikiLeaks, and Jennifer Robinson, Julian Assange's Attorney (Nov. 27, 2010), *available at* http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CC0QFjAA&url=http%3A%2F%2Fmedia.washingtonpost.com%2Fwp-srv%2Fpolitics%2Fdocuments%2FDept_of_State_Assange_letter.pdf&ei=_bqZUIqFLdPcqAGY9oDoDA&usg=AFQjCNFK6TfrXgitEemmT5TaOiFBnstIog.

55. *WikiLeaks embassy cables: the key points at a glance*, THE GUARDIAN (Dec. 7, 2010, 10:28 AM), http://www.guardian.co.uk/world/2010/nov/29/wikileaks-embassy-cables-key-points.

56. *Secret US Embassy Cables*, WIKILEAKS, http://WikiLeaks.org/cablegate.html# (last visited Mar. 9, 2012).

57. Scott Neuman, *Clinton: WikiLeaks 'Tear At Fabric' Of Government*, NPR (Nov. 29, 2010), http://www npr.org/2010/11/29/131668950/white-house-aims-to-limit-wikileaks-damage.

58. Daniel Foster, *Palin on WikiLeaks*, NATIONAL REVIEW ONLINE (Nov. 29, 2010, 3:22 PM), http://www nationalreview.com/corner/254062/palin-wikileaks-daniel-foster.

59. Elisabeth Bumiller, *Gates on Leaks, Wiki and Otherwise*, N.Y. TIMES (Nov. 30, 2010), http://thecaucus.blogs nytimes.com/2010/11/30/gates-on-leaks-wiki-and-otherwise.

however, and soon Wikileaks found itself under attack.

B. Backlash Against WikiLeaks

In March 2008, the US Army Counterintelligence Center issued a special report on the threat posed to the US Army by WikiLeaks.[60] The document identified WikiLeaks' reliance on trust as the website's major weakness. WikiLeaks relies on insiders and whistleblowers to trust that they will maintain their anonymity. The report concluded that identifying leakers and exposing them to employment termination or legal action could shake the trust on which WikiLeaks relies. As a result, others would be deterred from leaking documents to WikiLeaks.[61]

Although this report existed in 2008, no overt action was taken against WikiLeaks until the publication of the embassy cables. The first action taken against the website involved members of the US government expressing their outrage at Wikileaks's publication of the cables. In addition to Sarah Palin's description of Assange as a terrorist, then incoming chairman of the House of Representatives Homeland Security Committee, Peter King, described the leak as, "Worse than a military attack."[62]

Next, several congressmen informally asked companies to stop providing services to WikiLeaks. Joe Lieberman, then Chairman of the Senate Homeland Security Committee, publically asked Tableau Software to stop providing visualization services to WikiLeaks. Further, Lieberman persuaded Amazon to stop hosting WikiLeaks on its cloud server service. Soon, EveryDNS, the company that routed requests for the www.WikiLeaks.org domain to the servers hosting WikiLeaks, also terminated its relationship with WikiLeaks.[63] Media organizations speculated that this too was a result of government pressure.[64] In addition, the WikiLeaks.org domain name was hit with a distributed denial of service ("DDOS") attack devised by a political hacker.[65] In

60. Iain Thomson, *US military plan to destroy Wikileaks leaked*, V3 (Mar. 15, 2010), http://www.v3.co.uk/v3-uk/news/1946337/us-military-plan-destroy-wikileaks-leaked.

61. *Id.*

62. James Chapman, Gerri Peev, & Ian Drury, *WikiLeaks are a bunch of terrorists, says leading U.S. congressman as No10 warns of threat to national security*, MAIL ONLINE (Nov. 30, 2010), http://www.dailymail.co.uk/news/article-1333879/WikiLeaks-terrorists-says-leading-US-congressman-Peter-King html.

63. Charles Arthur & Josh Halliday, *WikiLeaks fights to stay online after US company withdraws domain name*, THE GUARDIAN (Dec. 3, 2010, 2:54 PM), http://www.guardian.co.uk/media/blog/2010/dec/03/wikileaks-knocked-off-net-dns-everydns?INTCMP=SRCH.

64. *Id.* (mentioning pressure from Senator Lieberman immediately after noting that WikiLeaks.org website was down).

65. Angela Moscaritolo, *Political hacker takes credit for Wikileaks DDoS attack*, S. C. MAGAZINE (Nov. 29, 2010), http://www.scmagazine.com/political-hacker-takes-credit-for-wikileaks-ddos-attack/article/191669.

response, WikiLeaks moved to a Swiss domain name, WikiLeaks.ch, and restarted operations.[66]

Perhaps, the most significant reaction to WikiLeaks, however, was that financial institutions stopped processing donations to WikiLeaks, cutting off the website's funding stream.[67] On December 3, 2010, PayPal ended its relationship with WikiLeaks, and the next day PayPal froze assets in an account being used by WikiLeaks. On December 7, 2010, MasterCard followed PayPal's lead and stopped allowing funds to transfer to WikiLeaks. Later that month, Bank of America removed all services from WikiLeaks followed by Western Union.[68] As a result of this banking embargo, WikiLeaks ceased publishing new information on October 24, 2011.[69] However, on February 27, 2012, WikiLeaks began publishing emails obtained from Stratfor, a global intelligence company.[70] As of the writing of this note, though, it is unclear whether this marks WikiLeaks's return to actively seeking out and publishing leaked material.

Since the Embassy Cables release, a grand jury has been convened in Maryland to investigate WikiLeaks's release of the embassy cables. The existence of the investigation came to light when Twitter won its battle to quash a gag order attached to a subpoena for subscriber information related to the official WikiLeaks twitter feed.[71] Assange has stated that the grand jury is investigating him and WikiLeaks for violations of the Espionage Act of 1917 and the Computer Fraud and Abuse Act of 1986.[72]

The response to WikiLeaks has followed the process that McNeal suggested to combat terrorist websites. WikiLeaks was publically called a criminal organization, and a criminal case is being built against the website. Private companies have been shamed into cutting ties to Assange and WikiLeaks, forcing the website to find foreign providers of technical services. Finally, an economic embargo has been established to prevent WikiLeaks from receiving funds, forcing the website to cease publishing new information. However, WikiLeaks is not a terrorist

66. Arthur & Halliday, *supra* note 63; *Donate*, WIKILEAKS, http://WikiLeaks.org/support html (last visited Oct. 16, 2011).

67. *Banking Blockade*, WIKILEAKS, http://wikileaks.org/Banking-Blockade.html (last visited Nov. 27, 2012).

68. *Id.*

69. *Id.*

70. *The Global Intelligence Files*, WIKILEAKS.ORG (Feb. 27, 2012), http://wikileaks.org/the-gifiles html (last visited Mar. 26, 2012).

71. Scott Shane & John F. Burns, *U.S. Subpoenas Twitter Over WikiLeaks Supporters*, N.Y. TIMES (Jan. 8, 2011), http://www nytimes.com/2011/01/09/world/09wiki html? pagewanted=all.

72. Michael Hastings, *Julian Assange: The Rolling Stone Interview*, ROLLING STONE (Jan. 18, 2012, 8:00 AM), http://www rollingstone.com/politics/news/julian-assange-the-rolling-stone-interview-20120118.

organization, so these tactics will fail to permanently incapacitate the website.

III. THE IMPENDING FAILURE OF THE CAMPAIGN AGAINST WIKILEAKS

> *As an initial matter, there is no doubt that WikiLeaks is very unpopular right now. Many feel that the WikiLeaks publication was offensive. But being unpopular is not a crime, and publishing offensive information is not either. And the repeated calls from politicians, journalists, and other so-called experts crying out for criminal prosecutions or other extreme measures make me very uncomfortable.*[73]

The actions taken against WikiLeaks do not rise to the level of state action. Thus, WikiLeaks cannot bring a case against the Government and demand an end to the embargo. Nevertheless, the attack on WikiLeaks will fail for two reasons: (A) WikiLeaks is not a criminal enterprise in the same way terrorist websites are, and (B) private actors do not support the campaign against WikiLeaks in the way they supported the attacks on terrorist websites.

A. Criminalization of WikiLeaks will Fail

US Army Private First Class Bradley Manning has been accused of passing the *Collateral Murder* video and other documents to WikiLeaks.[74] On May 29, 2010, Manning was charged under the Uniform Code of Military Justice ("UCMJ") articles 92 and 134 for transferring a classified video to his personal computer, and exceeding authorized access on a Secret Internet Protocol Router Network ("SIPRnet") computer and transmitted protected information to someone not entitled to receive it.[75] The UCMJ applies only to current or past members of the military, military cadets, reserve forces, prisoners of war, and people accompanying the armed forces in the field.[76] As such, Assange may not be charged under the same provisions as Manning. However, there are two civilian statutes that are analogous to the charges leveled against Manning: the Espionage Act of 1917,[77] and the Computer

73. Sahil Kapur, *Wikileaks did not commit a crime, House Judiciary chairman says*, THE RAW STORY (Dec. 16, 2010, 1:14PM), http://www.rawstory.com/rs/2010/12/16/wikileaks-did-not-commit-crime-conyers/ (quoting Rep. John Conyers (D-MI), then-chairman of House Judiciary Committee).

74. CHARGE SHEET OF BRADLEY MANNING (2010), *available at* http://anthropoliteia files.wordpress.com/2010/12/manning-charge.pdf.

75. *Id.*

76. Uniform Code of Military Justice art. 2, 10 U.S.C. § 802 (2006).

77. 18 U.S.C. §§ 792–799 (2006).

Fraud and Abuse Act ("CFAA").[78] Since December 2010, a grand jury has been empanelled in Virginia to investigate these charges against Assange.[79]

To see why Government attempts to criminalize WikiLeaks and its supporters will fail, I will break the discussion into four sections: (i) an examination of whether an Espionage Act prosecution of WikiLeaks is possible, (ii) a look at the problems of an Espionage Act prosecution, (iii) a discussion of whether a prosecution under the CFAA would succeed, and (iv) an argument that even if WikiLeaks can be subjected to criminal liability, unlike supporters of terrorist organizations, WikiLeaks' supporters cannot be prosecuted.

1. Espionage Act

The Espionage Act of 1917 is a first-world-war era law that criminalizes a broad range of acts related to disclosure of classified material. Since the release of the embassy cables, most calls for prosecution of Assange have focused on the possibility that he could be indicted under the Espionage Act.[80]

Specifically, 18 U.S.C. § 793(a) (2011) prohibits knowingly and willfully communicating or making available classified information to an unauthorized person, or publishing such information in any manner prejudicial interests of the United States where the classified information concerns intelligence activities of the US or foreign governments. Further, 18 U.S.C. § 793(b) (2011) outlaws copying any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense. Subsection (c) proscribes receiving, obtaining or agreeing to receive or obtain any of the materials from subsection (b) if the receiver knows or has reason to believe the materials were obtained in violation of the act. Subsection (g) makes it a crime to conspire to do something that violates the act. Any violation of these sections is punishable by a maximum of 10 years in prison.[81]

Assange almost certainly violated the plain meaning of the Espionage Act. Under subsection (a), Assange published classified information that concerned military intelligence by posting the *Collateral Murder* video on WikiLeaks. The very title of the video also

78. 18 U.S.C. § 1030 (2006).

79. *Assange Attorney: Secret Grand Jury Meeting in Virginia on WikiLeaks*, CNN (Dec. 13, 2010), http://articles.cnn.com/2010-12-13/justice/wikileaks.investigation_1_julian-assange-wikileaks-case-grand-jury?s=PM:CRIME.

80. *See, e.g.*, Letter from Rep. Peter T. King to Att'y Gen. Eric Holder (Nov. 28, 2010), *available at* http://www house.gov/apps/list/hearing/ny03_king/kingsupportsprosecutionofwikileaks.html

81. *See* 18 U.S.C. § 793(a)-(g) (2006).

demonstrates that the video was prejudicial to US interests because it accuses the US military of killing civilians. Further, Assange received documents and writings that he certainly had reason to believe were classified by the US government. As such he broke subsection (c) of the act. It could be argued that he also conspired to violate subsection (b) as well by offering to publish any materials he was given. Through a conspiracy charge, Assange would fall a foul of subsection (g) of the Act as well.

Although the prima facie case against Assange for violating the Espionage Act is strong, the government will face serious problems securing a conviction of Assange using this theory.

2. Problems with Espionage Act Prosecution

In *New York Times Co. v. United States*,[82] the US government tried to prosecute the New York Times for publishing the Pentagon Papers. The Supreme Court ruled that prior restraint of publication was not valid under the First Amendment.[83] But, the Court suggested that the government could pursue the paper for violations of the Espionage Act without violating freedom of speech.[84] Thus, Assange will probably not be able to make out a First Amendment defense against an Espionage Act Charge. However, the government must still overcome serious practical and political obstacles to prosecute Assange for violating the Espionage Act.

The primary problem arises because WikiLeaks published the Embassy Cables in conjunction with other newspapers. As such, if WikiLeaks violated the Espionage Act, then every media organization that published material provided by Manning to WikiLeaks also violated the Act. Because Assange organized the group of prominent newspapers to publish the embassy cables simultaneously with Wikileaks, he has set up a public relations trap for the government. The government has taken no steps towards prosecuting the New York Times for publishing the embassy cables and seems unlikely to do so.

Further, in another recent Espionage Act prosecution, federal prosecutors did not charge the journalist who received classified information from a source.[85] In that case, James Risen, a New York Times writer, was given information about a CIA operation against Iran's nuclear program.[86] When Risen included the information in a 2006

82. 403 U.S. 713 (1971).

83. *Id.* at 714.

84. *Id.* at 722 (Douglas, J., concurring).

85. Josh Gerstein, *Feds Spy on Reporter in Leak Probe*, POLITICO (Feb. 24, 2011, 11:06 PM), http://www.politico.com/news/stories/0211/50168 html.

86. *Id.*

book, State of War, the source was prosecuted under the Espionage Act. Although Risen was subpoenaed during the investigation of his source, he has not been charged in connection with the leak.[87] So, if Assange is prosecuted for the leaks, he will be able to point out this disparate treatment and claim he is being persecuted. This is not a strong legal defense, but it will make it politically very hard to charge Assange.

Prosecution of WikiLeaks under the Espionage Act would also leave the government vulnerable to a claim that they were the latest in a long line of administrations that had abused the Act to suppress political opposition. Parts of the Espionage Act have been used to imprison the leader of the Socialist Party of America,[88] to seize a film that portrayed British soldiers in a poor light,[89] and to convict a leaflet distributor.[90] Even if the government can convict Assange of violating the Act, it is quite possible that they would rather not add imprisoning an award-winning journalist to the above list.

3. Conspiracy to Violate Computer Fraud and Abuse Act

The CFAA[91] outlaws a number of activities related to computer hacking. Of particular interest for a potential prosecution of WikiLeaks is 18 U.S.C. §1030(a)(1) (2006). Specifically, this subsection forbids obtaining from a computer without authorization or in excess of authorization information that has been determined by the United States government to require protection against unauthorized disclosure and then willfully communicating, delivering, or transmitting that information to any person who is not entitled to receive the information.[92] 18 U.S.C. § 371 (2011) outlaws conspiring to commit any crime against the United States. This includes conspiring to violate the CFAA.[93] Conspiracy is punishable by up to five years in prison.[94]

Assange did not violate the CFAA as a principle. Although Assange willfully disclosed the information he received from Manning to persons not entitled to receive the information, Assange did not access any computer without authorization or in excess of authorization to obtain the information. Assange may have, however, conspired to

87. *See id.*

88. *See* Debs v. United States, 249 U.S. 211 (1919).

89. *Revive 'Spirit of '76,' Film Barred in 1917*, N.Y. TIMES, July 14, 1921, *available at* http://query nytimes.com/mem/archivefree/pdf?res=9A07E5DC173EEE3ABC4C52DFB166838A639EDE.

90. *See* Abrams v. United States, 250 U.S. 616 (1919).

91. 18 U.S.C. § 1030 (2006).

92. 18 U.S.C. § 1030(a)(1) (2006).

93. *See* United States v. Schaffer, 586 F.3d 414, 422 (6th Cir. 2009).

94. 18 U.S.C. § 631 (2006).

violate the CFAA with Manning. To show that Assange conspired to violate § 1030(a)(1), the government must prove that Assange and Manning agreed to the leak of the information before Manning accessed the computer illegally. There is no publically available information indicating that Assange and Manning had any contact prior to Manning's access of the computers. Unless there is evidence of this that has not been released, it seems unlikely that the government can secure a CFAA conviction of Assange. It has, however, been suggested that Assange may be vulnerable to a conspiracy charge because he actively encouraged the leaking of classified information.[95] However, conspiracy liability usually only extends to agreements to commit a specific crime and other crimes that are reasonably foreseeable consequences of the original crime. As such, a prosecution of Assange premised on the theory that he generally agreed to receive classified information is unlikely to succeed.

4. Lack of a "Material Support" Prohibition

18 U.S.C. § 2339A (2011) forbids anyone from providing "material support" to someone knowing or intending that the support will be used to violate any of the federal statutes designed to fight terrorism.[96] 18 U.S.C. § 2339B (2011) is similar in that it prohibits providing material support to any organization listed in the State Department's list of Foreign Terrorist Organizations.[97] The crimes that fall within the material support prohibition in § 2339A include production or use of biological or chemical weapons as prohibited by 18 U.S.C § 175 (2011) and 18 U.S.C. § 229 (2011), respectively; attacks on US or foreign officials as criminalized by 18 U.S.C § 1114-1116 (2011); and crimes involving aircraft piracy under 49 U.S.C. § 46502 (2011).[98] Sentences under the material support provision range for 15 years in prison for violations that do not cause someone's death, to life in prison for material support to actions that cause death through a violation of a listed statute.[99] Violations of the Espionage Act, the CFAA, and conspiracy are not included in the list of offenses that trigger the material support prohibition.[100]

Even if WikiLeaks violated the law, providing support for violators of the Espionage Act and the CFAA is not illegal like providing material support for terrorists is. Despite the rhetoric from some politicians,

95. King, *supra* note 80.
96. 18 U.S.C. § 2339(a) (2006).
97. 18 U.S.C. § 2339(b) (2006).
98. 18 U.S.C. § 2339(a) (2006).
99. *Id.*
100. *See id.*

implying that Assange and WikiLeaks should be treated like terrorists, WikiLeaks has not been added to the State Department list of Foreign Terrorist Organizations necessary for a prosecution under § 2339B.[101] Neither has there been serious consideration to adding illegal publication of classified material to the list of offenses that justify the punishment available under § 2339A. Thus, there is no potential for criminal liability for companies and organizations that support WikiLeaks.

As can be seen from this discussion, the potential for criminal liability related to WikiLeaks' publications is limited. Assange may be venerable directly for violations of the Espionage Act, but charges cannot be brought against anyone else. As a result, the public does not support the campaign against WikiLeaks as it did the campaign against terrorist websites.

B. Lack of Support from Private Actors

Public opinion about WikiLeaks in 2011 is far less negative than attitudes towards terrorist organizations in the early 2000's. In fact it is hard to imagine any organization being more reviled than al Qaeda at present, let alone an award-winning media website. As a result of this lack of animas towards WikiLeaks, organizations and individuals have begun to resist government attempts to attack WikiLeaks.

Since WikiLeaks was first attacked, people have set up mirror sites of the website so that it is still accessible if the wikileaks.org domain is unavailable. A mirror site is a copy of a website that has been uploaded onto a server separate from the original one. That way, people can access the information on the original website even when that website is down. At present there are 12 mirror sites of the full WikiLeaks website site located in 11 different countries.[102] In addition, there are approximately 400 sites currently mirroring some or all of the Embassy Cables.[103]

Even some mainstream corporations are refusing to cooperate with the government against WikiLeaks. On December 14, 2010, a subpoena was sent to the microblogging website Twitter by the United States attorney for the Eastern District of Virginia. The Subpoena invoked the Stored Communications Act[104] and demanded that Twitter produce account information of five people connected to WikiLeaks: Assange, Manning, Birgitta Jonsdottir, a former WikiLeaks activist and current

101. *Foreign Terrorist Organizations*, U.S. DEPT. OF STATE (Sept. 28, 2012), http://www.state.gov/j/ct/rls/other/des/123085 htm.

102. WIKILEAKS MIRRORS (Aug. 24, 2012), http://wikileaks.info/.

103. WHERE IS WIKILEAKS?, http://www.whereiswikileaks.org (last visited Nov. 28, 2012).

104. 18 U.S.C. § 2702–03 (2006).

member of the Icelandic Parliament, and two computer programmers, Rop Gonggrijp and Jacob Appelbaum. The request covered addresses, screen names, telephone numbers, and credit card and bank account numbers. The subpoena did not ask for the content of private messages sent using Twitter. The subpoena was accompanied by an order requiring Twitter to not notify the owners of the accounts.[105]

Rather than simply comply with the subpoena, Twitter challenged the gag order as its own policy is to notify users of any demands for their information.[106] The subpoena was unsealed on January 5, 2011, and Twitter notified the targets of the subpoena about the request. Subsequently, Appelbaum, Gonggrijp, and Jonsdottir challenged the subpoena in federal court, but the subpoena was upheld on November 10, 2011.[107] Although Twitter was eventually ordered to hand over the requested information, that the subpoena spent almost a year in legal limbo demonstrates that private actors are not willing to abandon WikiLeaks at the first sign of government pressure in the same way they abandoned terrorist websites in the face of Internet Haganah's shaming campaign.

Further, private organizations that support WikiLeaks have been resisting attempts to shut down the website. Days after WikiLeaks began to publish the Embassy Cables, Anonymous, a collective of computer hackers loosely connected to the website 4Chan.org, began attacking companies that had removed services from WikiLeaks.[108] In response to Visa and MasterCard refusing to process donations to WikiLeaks, Anonymous performed distributed denial of service ("DDOS") attacks on the websites of those companies. Next, the organization targeted Paypal's payment delivery system when transfers to WikiLeaks fundraising account were stopped.[109] Unlike most DDOS attacks, which use computers infected with a virus against the users' wishes, the Anonymous attacks used computers owned by people who had signed up to join the attacks.[110] Anonymous released a statement describing the attacks as a blow for freedom of speech. The group said, "Anonymous is peacefully campaigning for freedom of speech everywhere in all forms.

105. Shane & Burns, *supra* note 71.

106. *Id.*

107. Somini Sengupta, *Twitter Must Provide Data on Three Users, Judge Rules*, N.Y. TIMES, Nov. 11, 2011, at B8, *available at* http://www nytimes.com/2011/11/11/technology/twitter-ordered-to-yield-data-in-wikileaks-case html.

108. Andy Bloxham & Steven Swinford, *WikiLeaks Cyberwar: Hackers Target Paypal*, THE TELEGRAPH (Dec. 9, 2010, 2:18 PM), http://www.telegraph.co.uk/news/worldnews/wikileaks/8190871/WikiLeaks-cyberwar-hackers-target-Paypal html.

109. *Id.*

110. *Id.*

Freedom of speech for: the internet, for journalism and journalists, and citizens of the world at large. Regardless of what you think or have to say; Anonymous is campaigning for you."[111]

The resistance to the government's campaign against WikiLeaks and the attacks on those removing services from the website show that public opinion is not behind the government. Individuals around the world are mirroring WikiLeaks to preserve access to the leaked information. Large corporations like Twitter are challenging court orders to produce information related to WikiLeaks. And, Anonymous is attacking the websites of those companies that remove services from WikiLeaks. The actions of Anonymous echo the attacks by Messner and Internet Haganah on terrorist websites, but the attacks have had the opposite aim and effect. They hinder the government's attempt to remove WikiLeaks from the Internet rather than helping the removal of terrorist websites as Messner and Internet Haganah did. The refusal of private actors to help the government attack WikiLeaks demonstrates that there are serious political and practical problems in prosecuting Assange and WikiLeaks.

CONCLUSION

Sarah Palin's comment, quoted at the top of this note, compared Julian Assange to terrorist leaders generated headlines worldwide.[112] But, that since December 2010 the US government has engaged in a campaign against WikiLeaks that is similar to that employed against terrorist organizations after September 11, 2001 has been mostly ignored. Even so, the similarities between the campaigns against terrorist websites and WikiLeaks are unmistakable. Both were ostracized by public declarations that the organizations were criminal, both were targets of shaming campaigns that led companies to remove services from them, and both were attacked by private embargos encouraged by government figures.

Despite these similarities, the campaigns against terrorist websites and WikiLeaks will eventually have very different endings. Despite the technical possibility of an Espionage Act prosecution, the practical difficulties and the lack of public support facing such a prosecution makes comparisons of WikiLeaks to terrorists seem like empty rhetoric. Without successful criminal charges against Assange and WikiLeaks, the embargo on WikiLeaks will not survive. Even if criminal charges are successfully pursued against those associated with WikiLeaks and the website is destroyed, the private actors who have supported WikiLeaks'

111. *Id.*
112. *See, e.g.*, Beckford, *supra* note 1.

campaign for a transparent society will likely step into the void and continue to publish leaked information online.