Archives for the Dark Web: A Field Guide for Study

Robert W. Gehl

[This chapter will appear in a forthcoming book, *Research Methods for Digital Humanities*, edited by Levenberg, Neilson, and Rheams. This is a pre-proofed version.]

This chapter is the result of several years of study of the Dark Web, which culminated in my book project *Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P* (MIT Press, 2018). *Weaving the Dark Web* provides a history of Freenet, Tor, and I2P and details the politics of Dark Web markets, search engines, and social networking sites. In the book, I draw on three main streams of data: participant observation, digital archives, and the experience of running the routing software required to access the Dark Web.

Throughout the course of my time on the Dark Web, a curious term kept coming up: *legit*. People would use variations on the word "legitimate" in a wide range of contexts. For example, on a forum dedicated to the art of making and passing counterfeit American money, one participant described a technique to make fake $20 bills "look legit." In another context, business writers lamented the fact that the Silk Road drug market wasn't considered "legitimate," because it was an incredibly profitable startup that grew at a fantastic pace. And in yet another context, security researchers argued that the Tor Project has a responsibility to get more "legitimate" (i.e., legal) users onto their network. After seeing this curious word come up again and again, I chose to do a keyword-based inquiry into the Dark Web, similar to Nicholas John's book *The Age of Sharing*,[1] where I considered three key meanings of "legitimacy": states' claims to a monopoly on violence; organizations' claims to resources and respect; and practices of inclusion and exclusion. In other words: violence, propriety, and authenticity. Through interviews, participant observation, and archival research, I trace these claims and practices through a range of Dark Web sites.

This chapter draws on the three streams of data I engaged with to provide a field guide for other digital humanists who want to study the Dark Web. In order to focus the chapter, I emphasize my belief that, in order to study the cultures of Dark Web sites and users, the digital humanist must engage with these systems' technical infrastructures. I will provide specific reasons why I believe that understanding the technical details of Freenet, Tor, and I2P will benefit any researchers who study these systems, even if they focus on end users, aesthetics, or Dark Web cultures. To this end, I offer a catalog of archives and resources researchers could draw on and a discussion of why researchers should build their own archives. I conclude with some remarks about ethics of Dark Web research.

What is the Dark Web?

As I define the Dark Web in my book, the "Dark Web" should actually be called "Dark Webs," because there are multiple systems, each relatively independent of one another. I write about three in my book: Freenet, Tor, and I2P. With these systems installed on a computer, a user can access special Web sites through network topologies that anonymize the connection between the client and the server. The most famous of these systems is Tor, which enables Tor hidden services (sometimes called "onions" due to that system's Top Level Domain, .onion). But there is an older system, Freenet, which allows for hosting and browsing freesites. Freenet was quite influential on the Tor developers. Another system that drew inspiration from Freenet, the Invisible Internet Project or I2P, allows for the anonymous hosting and browsing of eepsites. Tor hidden services, freesites, and eepsites are all built using standard Web technologies, such as HTML, CSS, and in some cases server- and client-side scripting. Thus, these sites can be seen in any standard browser so long as that browser is routed through the accompanying special software. Thus, what makes them "dark" is their anonymizing capacities. A way to think of this

1 Nicholas A. John, *The Age of Sharing* (Malden, MA: Polity, 2017).

is in terms of the connotation of "going dark" in terms of communications, of moving one's communications off of open networks and into more secure channels.[2]

Thus, I resist the definitions of "Dark Web" that play on the negative connotations of "dark," where the Dark Web is anything immoral or illegal that happens on the Internet. To be certain, there are illegal activities occurring on the Tor, Freenet, or I2P networks, including drug markets, sales of black hat hacking services or stolen personal information, or child exploitation images. However, there are also activities that belie the negative connotations of "dark," including political discourses, social networking sites, or news services. Even Facebook now has a Tor hidden service. The Dark Web – much like the standard World Wide Web – includes a rich range of human activity.

Approaches Previously Taken to the DW

Indeed, it's the presence of a wide range of activities on the Dark Web which leads me to my call: the Dark Web is in need of more humanistic inquiry. Currently, academic work on the Dark Web is dominated by computer science[3] and automated content analysis[4] approaches. The former is dedicated to developing new networking and encryption algorithms as well as testing the security of the networks. The major questions that computer science/network security researchers ask include: how well does this network encrypt data? How well does it dissociate user identities from their activities? The latter tends to use automated crawling software and large-scale content analysis to classify content

2 Thus, the connotation of “dark” I draw on to define the Dark Web is quite similar to that of former FBI director James Comey. See James Comey, “Encryption, Public Safety, and ‘Going Dark,’” Blog, *Lawfare*, (July 6, 2015), http://www.lawfareblog.com/encryption-public-safety-and-going-dark.

3 For examples, see Ian Clarke et al., “Freenet: A Distributed Anonymous Information Storage and Retrieval System,” in *Designing Privacy Enhancing Technologies*, ed. Hannes Federrath (Springer, 2001), 46–66, http://link.springer.com/chapter/10.1007/3-540-44702-4_4; Ian Clarke et al., “Protecting Free Expression Online with Freenet,” *Internet Computing, IEEE* 6, no. 1 (2002): 40–49; Jens Mache et al., “Request Algorithms in Freenet-Style Peer-to-Peer Systems,” in *Peer-to-Peer Computing, 2002.(P2P 2002). Proceedings. Second International Conference On* (IEEE, 2002), 90–95, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1046317; Hui Zhang, Ashish Goel, and Ramesh Govindan, “Using the Small-World Model to Improve Freenet Performance,” in *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 3 (IEEE, 2002), 1228–1237, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1019373; Karl Aberer, Manfred Hauswirth, and Magdalena Punceva, “Self-Organized Construction of Distributed Access Structures: A Comparative Evaluation of P-Grid and FreeNet,” in *The 5th Workshop on Distributed Data and Structures (WDAS" 2003)*, 2003, http://infoscience.epfl.ch/record/54381; Jem E. Berkes, “Decentralized Peer-to-Peer Network Architecture: Gnutella and Freenet,” *University of Manitoba Winnipeg, Manitoba, Canada*, 2003, http://www.berkes.ca/archive/berkes_gnutella_freenet.pdf; Ian Clarke et al., “Private Communication through a Network of Trusted Connections: The Dark Freenet,” *Network*, 2010, http://www.researchgate.net/profile/Vilhelm_Verendel/publication/228552753_Private_Communication_Through_a_Network_of_Trusted_Connections_The_Dark_Freenet/links/02e7e525f9eb66ba13000000.pdf; Mathias Ehlert, “I2P Usability vs. Tor Usability A Bandwidth and Latency Comparison,” in *Seminar. Humboldt University of Berlin. Berlin, Germany*, 2011, http://userpage.fu-berlin.de/semu/docs/2011_seminar_ehlert_i2p.pdf; Peipeng Liu et al., “Empirical Measurement and Analysis of I2P Routers,” *Journal of Networks* 9, no. 9 (2014): 2269–2278; Gildas Nya Tchabe and Yinhua Xu, “Anonymous Communications: A Survey on I2P,” *CDC Publication Theoretische Informatik–KryptographieundComputeralgebra (Https://Www. Cdc. Informatik. Tu-Da Rmstadt. De)*, 2014, https://www.cdc.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_CDC/Documents/Lehre/SS13/Seminar/CPS/cps2014_submission_4.pdf; Matthew Thomas and Aziz Mohaisen, “Measuring the Leakage of Onion at the Root,” 2014, 11.

4 Symon Aked, “An Investigation into Darknets and the Content Available via Anonymous Peer-to-Peer File Sharing,” 2011, http://ro.ecu.edu.au/ism/106/; Hsinchun Chen, *Dark Web - Exploring and Data Mining the Dark Side of the Web* (New York: Springer, 2012), http://www.springer.com/computer/database+management+%26+information+retrieval/book/978-1-4614-1556-5; Gabriel Weimann, “Going Dark: Terrorism on the Dark Web,” *Studies in Conflict & Terrorism*, 2015, http://www.tandfonline.com/doi/abs/10.1080/1057610X.2015.1119546; Clement Guitton, “A Review of the Available Content on Tor Hidden Services: The Case against Further Development,” *Computers in Human Behavior* 29, no. 6 (November 2013): 2805–15, doi:10.1016/j.chb.2013.07.031; Jialun Qin et al., “The Dark Web Portal Project: Collecting and Analyzing the Presence of Terrorist Groups on the Web,” in *Proceedings of the 2005 IEEE International Conference on Intelligence and Security Informatics* (Springer-Verlag, 2005), 623–624, http://dl.acm.org/citation.cfm?id=2154737.

on the various networks (predominantly on Tor). Very often, a goal of the latter is to demonstrate that Tor (or I2P or Freenet) is mostly comprised of "unethical" activity.[5]

More recently, given the explosion of interest in Dark Web drug markets, specifically the Silk Road during its run between 2011 and 2013, there is a growing body of research on Dark Web exchanges.[6] A significant part of this work is ethnographic, especially from Alexia Maddox and Monica Barrett, who have not only engaged in ethnographies of markets[7] but also have written about ethnographic methods in those environments.[8] Key questions these researchers ask include: How do Dark Web markets function? What are the patterns of social interaction that occur as Dark Web users seek to buy and sell goods and services? What sort of discursive patterns do they develop to describe their activities? This latter thread of Dark Web ethnography is, I would suggest, a key starting point for digital humanist work.

Thus, as should be clear, there are many underutilized approaches to the Dark Web, including political economy and semiotic and textual interpretation. The ethnographic work has mainly been directed at Dark Web markets and not at other types of sites, including forums and social networking sites.[9] Moreover, most of the attention is paid to Tor Hidden Services; far less to I2P, Freenet, or newer systems such as Zeronet. Although the Dark Web is relatively small in comparison to the "Clear Web," there is much more work to be done, and critical humanists ought to be engaged in it.

Why Study Technical Infrastructures?

This leads me to a somewhat unusual point. To engage in critical humanist work on the Dark Web, I suggest that the potential researcher consider studying Dark Web infrastructures and technologies. I suggest this for a pragmatic reason: any qualitative inquiry into the Dark Web will inevitably have to grapple with their technical capacities. As Barratt and Maddox argue, "Conducting digital ethnography in the dark net requires a strong working knowledge of the technical practices that are used to maintain anonymous communications."[10] Many of the discussions and interactions among Dark Web participants have to do with the technical details of these systems. Marshall McLuhan famously said "the medium is the message," and in the case of the cultures of the Dark Web, this is profoundly true. Those who administer and use Dark Web sites often engage in highly technical discussions about anonymizing networks, cryptography, operating systems, and Web hosting and browsing software (which also means a researcher's literature review ought to include much of the computer science work cited above). This is not to say that there are no other discourses on the Dark Web, but it is to say that the vast majority of

5 See especially Guitton, “A Review of the Available Content on Tor Hidden Services”; Weimann, “Going Dark.”

6 Nicolas Christin, “Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace,” in *Proceedings of the 22Nd International Conference on World Wide Web*, WWW ’13 (New York, NY, USA: ACM, 2013), 213–224, doi:10.1145/2488388.2488408; Marie Claire Van Hout and Tim Bingham, “‘Silk Road’, the Virtual Drug Marketplace: A Single Case Study of User Experiences,” *International Journal of Drug Policy* 24, no. 5 (September 2013): 385–91, doi:10.1016/j.drugpo.2013.01.005; Marie Claire Van Hout and Tim Bingham, “‘Surfing the Silk Road’: A Study of Users’ Experiences,” *International Journal of Drug Policy* 24, no. 6 (November 2013): 524–29, doi:10.1016/j.drugpo.2013.08.011; James Martin, *Drugs on the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs*, 2014; James Martin, “Lost on the Silk Road : Online Drug Distribution and the ‘Cryptomarket,’” *Criminology & Criminal Justice* 14, no. 3 (2014): 351–367, doi:10.1177/1748895813505234; Amy Phelps and Allan Watt, “I Shop Online – Recreationally! Internet Anonymity and Silk Road Enabling Drug Use in Australia,” *Digital Investigation* 11, no. 4 (2014): 261–272, doi:10.1016/j.diin.2014.08.001; Alois Afilipoaie and Patrick Shortis, “From Dealer to Doorstep–how Drugs Are Sold on the Dark Net,” GDPO Situation Analysis (Swansea University: Global Drugs Policy Observatory, 2015), http://www.swansea.ac.uk/media/Dealer%20to%20Doorstep%20FINAL%20SA.pdf; Jakob Johan Demant and Esben Houborg, “Personal Use, Social Supply or Redistribution? Cryptomarket Demand on Silk Road 2 and Agora,” *Trends in Organized Crime*, 2016, http://www.forskningsdatabasen.dk/en/catalog/2304479461; Rasmus Munksgaard and Jakob Demant, “Mixing Politics and Crime – The Prevalence and Decline of Political Discourse on the Cryptomarket,” *International Journal of Drug Policy* 35 (September 2016): 77–83, doi:10.1016/j.drugpo.2016.04.021; Alice Hutchings and Thomas J. Holt, “The Online Stolen Data Market: Disruption and Intervention Approaches,” *Global Crime* 18, no. 1 (January 2, 2017): 11–30, doi:10.1080/17440572.2016.1197123.

interactions there involve these technical discourses in one way or another.

A political economist, for example, will have to understand cryptocurrencies (including Bitcoin, but also new systems such as Monero and Zcash), Web market software, and PGP encryption in order to fully trace circuits of production, exchange, distribution, and consumption. Scholars of visual culture will see images and visual artifacts that are directly inspired by computer science, network engineering, and hacker cultures. Thus, understanding the technical elements of the networks – or more precisely how the artists and participants are interpreting these technical details – will be important. Textual analysts, including those engaged in new digital humanities techniques of distant reading and large corpus analysis, will need understanding of infrastructures and networking technologies in order to uncover the politics and cultures of Dark Web texts.[11] Participant observers will need to learn the languages of Dark Web users, which relies heavily on technical terms and ideas, in order to be included in conversations and practices. Just as in previous ethnographies, as the anthropologist Hugh Gusterson notes, the researcher's identity is a key aspect of the work.[12] Of course, the anonymizing properties of the Dark Web are predominantly used by people who hide markers of identity such as race, class, and gender.[13] Often instead of those identity markers, Dark Web participants use technical knowledge of encryption, routing, network protocols, or Web hosting as substitutes for the markers that would be more prevalent in face-to-face settings. Ultimately, then, I recommend humanist researchers familiarize themselves with technical details and language. This will aid in dealing with the inevitable "disorientation," which "is one of the strongest sensations of the researcher newly arrived in the field."[14]

For a humanist to study these networks and their participants on their own terms, then, it is necessary to have a solid grasp of the underlying technical infrastructures. This chapter is in large part a guide to resources to enable the study of those infrastructures. While I have selected these archives with this recommendation in mind, these archives also have the advantage of providing rich insights into many aspects of Dark Web cultures and practices.

Archives to Draw On

Generally speaking, the materials a researcher would draw on to study Dark Web infrastructures includes

- software repositories

7 Monica J. Barratt, Jason A. Ferris, and Adam R. Winstock, “Safer Scoring? Cryptomarkets, Social Supply and Drug Market Violence,” *International Journal of Drug Policy* 35 (September 2016): 24–31, doi:10.1016/j.drugpo.2016.04.019; Monica J. Barratt et al., “‘What If You Live on Top of a Bakery and You like Cakes?’—Drug Use and Harm Trajectories before, during and after the Emergence of Silk Road,” *International Journal of Drug Policy* 35 (September 2016): 50–57, doi:10.1016/j.drugpo.2016.04.006; Alexia Maddox et al., “Constructive Activism in the Dark Web: Cryptomarkets and Illicit Drugs in the Digital ‘Demimonde,’” *Information, Communication & Society* 0, no. 0 (October 15, 2015): 1–16, doi:10.1080/1369118X.2015.1093531.

8 Monica J. Barratt and Alexia Maddox, “Active Engagement with Stigmatised Communities through Digital Ethnography,” *Qualitative Research*, May 22, 2016, 1468794116648766, doi:10.1177/1468794116648766.

9 Robert W. Gehl, “Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network,” *New Media and Society*, October 16, 2014, 1–17.

10 Barratt and Maddox, “Active Engagement with Stigmatised Communities through Digital Ethnography,” 6.

11 Munksgaard and Demant, “Mixing Politics and Crime – The Prevalence and Decline of Political Discourse on the Cryptomarket.”

12 Hugh Gusterson, “Ethnographic Research,” in *Qualitative Methods in International Relations*, ed. Audie Klotz and Deepa Prakash, Research Methods Series (Palgrave Macmillan UK, 2008), 96, doi:10.1007/978-0-230-58412-9_7.

13 This is definitely not to say that such markers don't emerge, or that racialized/gendered/classed discourses do not appear on the Dark Web. As I show in my book, such discourses do emerge, highlighting the overall arguments put forward by Lisa Nakamura that the Internet is not a perfectly "disembodied" medium. See Lisa Nakamura, *Cybertypes: Race, Ethnicity, and Identity on the Internet* (New York: Routledge, 2002).

14 Gusterson, “Ethnographic Research,” 97.

- mailing lists
- forums
- hidden sites

In terms of software repositories, as I have written about elsewhere, lines of code can offer a great deal of insight into how developers conceive of their software system's uses and users.[15] Many Dark Web systems are open source, meaning their code is available for inspection in software repositories. Each and every contribution to the software is recorded, meaning software repositories provide an opportunity to study software evolution, tracing production from initial lines of code to full-blown software packages. Most important for the digital humanist, this code is accompanied by comments, both within the code itself and added by developers as they upload new versions, so a researcher can trace the organizational discourses and structures that give rise to the software.[16]

Beyond code, however, the software developers engage in rich debates in mailing lists and forums. For example, since it dates back to 1999, Freenet has nearly two decades of mailing list debates that certainly engage in the technical details of routing algorithms and encryption protocols, but also discuss the role of spam in free speech,[17] the politics of post-9/11 surveillance states,[18] and network economics.[19] Tor also has highly active mailing lists.[20] I2P developers use Internet Relay Chat, archiving their meetings on their home page,[21] as well as a development forum hosted as an eepsite (at zzz.i2p*).[22] For my book, I focused on how these projects deployed the figure of "the dissident" as an ideal user to build for as well as a political and economic justification for the projects' existence (this relates back to the Weberian concept of the state's claim to a monopoly on violence). Future researchers might draw on these archives to discover other such organizing concepts and discourses.

And of course, Dark Web sites themselves can provide rich streams of data, including archives that can help a researcher understand technical structures and the histories of these systems. For example, Freenet's Sone (SOcial NEtworking) plugin is an active, searchable microblog system with posts dating back several years. I2P's wiki (i2pwiki.i2p) retains records of previous edits to wiki pages. Hidden Answers (on the Tor network and on I2P, at http://answerstedhctbek.onion and hiddenanswers.i2p, respectively), has tens of thousands of categorized questions and answers, dominated by questions on computer networking and hacking. These archives provide rich insight into the cultural practices of Dark Web network builders, administrators, and users. Because these sites are "Web 2.0"-style interactive platforms, a researcher can participate in them, making posts to Sone, editing the I2P wiki, or posing or answering questions on Hidden Answers. In fact, each of these sites/systems would make a good starting point for broader forays into the Dark Web.

In what follows, I provide links to specific archives. This catalog is not exhaustive.

15 Robert W. Gehl, “(Critical) Reverse Engineering and Genealogy,” *Foucaultblog*, August 16, 2016, doi:10.13095/uzh.fsw.fb.153.

16 Ahmed Hassan, “Mining Software Repositories to Assist Developers and Support Managers,” 2004, 2, https://uwspace.uwaterloo.ca/handle/10012/1017.

17 Glenn McGrath, “[Freenet-Chat] Deep Philosophical Question,” January 2, 2002, https://emu.freenetproject.org/pipermail/chat/2002-January/000604.html.

18 colbyd, “[Freenet-Chat] Terrorism and Freenet,” January 9, 2002, https://emu.freenetproject.org/pipermail/chat/2002-January/001353.html.

19 Roger Dingledine, “[Freehaven-Dev] Re: [Freenet-Chat] MojoNation,” August 9, 2000, http://archives.seul.org//freehaven/dev/Aug-2000/msg00006.html.

20 See https://lists.torproject.org/cgi-bin/mailman/listinfo for a list of them.

21 See https://geti2p.net/en/meetings/ for the archived chat logs.

22 All URLs marked with an * require special routing software to access. URLs ending in .i2p require I2P software; .onions require Tor, and Freesites require Freenet. For instructions on how to download, install, and run these routers, see each project's respective home pages.

Tor Hidden Services

Tor Project and Related Archives

The Tor Project home page (torproject.org) contains links to many of specifications documents and public relations documents associated with Tor. Their blog (https://blog.torproject.org/) is now a decade old, with thousands of posts and tens of thousands of comments archived. Tor now uses Github as its software repository (https://github.com/TheTorProject/gettorbrowser). This repository provides the sorts of data described above: bugs, comments, and of course lines of code.[23]

Prior to the Tor Project, key Tor people (including Roger Dingledine) worked on another, called Free Haven. Free Haven was to be an anonymous document storage system. It was never implemented, but the technical problems Dingledine and his colleagues encountered led them to onion routing and, from there, to what would become the Tor Project. The Free Haven site (freehaven.net) contains an archive of technical papers and the freehaven-dev mail list. Similarly, onion routing creator Paul Syverson maintained a Web site dedicated to onion routing and the early years of Tor: https://www.onion-router.net/

Research projects engaging with these archives might include historical analysis of the development of the Tor project as an organization, its peculiar relationship to state agencies, and how the culture of Tor becomes embedded in the technical artifacts it produces.

Darknet Market Archives

Because of sites such as the Silk Road, a great deal of attention has been paid to Tor-based markets. Several researchers have used Web scraping software to download large portions of Dark Web market forums. These forums are important because they are where buyers, vendors, and market administrators discuss market policies and features, settle disputes, and engage in social and political discussion. A compressed, 50GB archive of the results of this Web scraping, dating between 2011 – 2015, can be found at https://www.gwern.net/DNM%20archives. The page also includes suggested research topics, including analysis of online drug and security cultures.

Key Tor Hidden Services

Although a researcher can draw on the Gwern.org archives, they halt in 2015. To gather more recent data – as well as engage in participant observation or find interview subjects, one ought to spend time on market forums. For example, DreamMarket* is a long-running market, and its forum can be found at http://tmskhzavkycdupbr.onion/. For any researcher working on these forums, I highly recommend studying their guides to encryption and remaining anonymous. I also highly recommend Barratt and Maddox's guide to doing research in such environments, particularly because engaging in such research raises important ethical considerations (more on this below).[24] With practice, a researcher can start to engage Dark Web market forum participants in conversations about the state of markets, market practices, and the codes of social interaction.

As one of the longest-running Tor hidden service social networking sites, Galaxy2* (http://w363zoq3ylux5rf5.onion/) is an essential site of study. As I have written about elsewhere, such Dark Web social networking sites replicate many of the features of corporate sites such as Facebook, but of course do so within anonymizing networks.[25] Galaxy2 has over 17,000 registered accounts, which is of course very small compared to Facebook, but is quite large compared to many other Dark Web social networking systems. It features blogs, social groups, and a microblogging system, dating back to early 2015. The vast majority of my own participant observation during my research occurred on sites such as Galaxy2. Because they are social networking sites, they replicate many of the practices

23 Achilleas Pipinellis, *GitHub Essentials* (Packt Publishing, 2015).
24 Barratt and Maddox, “Active Engagement with Stigmatised Communities through Digital Ethnography.”
25 Gehl, “Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network.”

of corporate social media, such as Facebook: friending, liking, and commenting. I actively engaged with these sites for several years, collaborating on the development of a privacy policy, commenting on others' posts, helping to moderate a group forum, and sharing links to other Dark Web sites. Eventually, as I got to know members of these sites better, I was able to interview them to explore their perceptions of the Dark Web's legitimacy (or lack of). Of course, I did these interviews while adhering to the standards set forth by my university's Institutional Review Board (a point I will return to below).

Ultimately, such social networks provide important windows into the broader Dark Web cultures. By delving into market forums and Galaxy2, a researcher can begin to discover other key sites and services on the Tor network. Comparative work on the social dynamics of market forums versus social networking software would be a fruitful research project.

Freenet Freesites

Freenet Project

Starting with Ian Clarke's master's thesis in 1999, Freenet is the oldest of the Dark Web systems discussed in this chapter. The Freenet Project home page (freenetproject.org) is similar to the Tor Project's in that it contains software specifications documents, guides on installation and use, and mailing lists. Mailing lists (both at https://freenetproject.org/pages/help.html#mailing-lists) date back to the year 2000. Unfortunately, the Freenet-chat mail list is no longer online (contact me for an archive).

The Freenet Project also operates a user survey site at https://freenet.uservoice.com/forums/8861-general, where Freenet users suggest features and the developers discuss possible implementations of them.

One of the unique aspects of Freenet is its data storage structure. Freenet was designed to "forget" (i.e., delete) less-accessed data from its distributed data stores. This "forgetting" practice precedes contemporary discussions of "the right to be forgotten" or self-destructing media by over a decade, and thus a researcher may draw insights from Freenet's unique place in the genealogy of forgetful media.

On Freenet

Freenet's home page currently lists directories as the first links. These directories – Enzo's Index,* Linkaggedon,* and Nerdaggedon* – are key ways into the network, but they are archives in their own right due to the structure of Freenet. Freenet's data storage system is distributed across every computer that participates in the network, leading much of the data on the network, including Freesites, to be stored for long periods of time. Thus, these directories, which offer links to Freesites, are a good way to get a sense of the content of the network. Enzo's Index is useful because it is categorized, with Freesites grouped by topic. Unfortunately, it is not being updated. Nerdaggedon, however, is still active.

Two key resources, FMS* and Sone,* are additional plugins for Freenet. This means they do not come with the stock installation of Freenet, but have to be added to the base software. FMS – the Freenet Messaging System – is a bulletin board-style system with boards based on topics. Sone, mentioned above, is a microblogging system similar to Twitter in that it is structured in follower/followed relationships. However, unlike Tor and I2P, Freenet's file structure means that, in order to access older posts on either FMS or Sone, one has to run these systems for some time while they download older posts from the network. After doing so, a researcher has large archives of posts to examine.

I2P eepsites

Invisible Internet Project

As I discuss in my book, the Invisible Internet Project (I2P) is somewhat different from Tor and Freenet in that the latter two organizations decided to become registered nonprofits in the United States, which required them to disclose information about their founders and budgets. I2P, on the other hand, is what

I call an "anonymous nonprofit" in that it did not formally file with the U.S. I.R.S. for nonprofit status and it avoided revealing the real identities of its developers for most of its history. This organizational difference is reflected in how I2P developers do their work. Developer meetings are held predominantly over IRC. Their logs are archived at the I2P home page (https://geti2p.net/en/meetings/). In addition, I2P uses a forum hosted as an eepsite: zzz.i2p,* where developers consult about the project. While they have a public Github software repository (https://github.com/i2p), some development also occurs on another eepsite, http://git.repo.i2p/w?a=project_list;o=age;t=i2p.*

I2P did use a mailing list for several years, but Web-based access to it has been lost. Instead, researchers can access them via NNTP (Network News Transfer Protocol) from Gmane: news://news.gmane.org:119/gmane.network.i2p and news://news.gmane.org:119/gmane.comp.security.invisiblenet.iip.devel. These have not been used since 2006, but both provide insights into the early years of I2P (including its predecessor, the Invisible IRC Project).

Key Eepsites

As described above, the I2P Wiki (i2piwiki.i2p*) is a collaboratively-written guide to I2P, including eepsite directories and how to search the network. Moreover, it is built on MediaWiki (the same software as Wikipedia) and thus a researcher can see edit histories and discussion pages.

Echelon.i2p* provides downloads of I2P software. Notable is the archive of older versions of I2P, stretching back to version 0.6.1.30. Because I2P (like Tor and Freenet) is open source, a researcher can trace changes to the software through these versions. Of particular interest are the readme files, hosts.txt (which includes lists of eepsites), and changelogs.

Like Tor and Freenet, I2P has social networking sites. The oldest is Visibility.i2p*, which dates back to 2012. Visibility is a relatively low-traffic site, but its longevity allows a researcher to track trends in I2P culture over a period of years.

Finally, in addition to running the developer forum (zzz.i2p*), I2P developer zzz runs stats.i2p,* which includes data on I2P routers and network traffic (http://stats.i2p/cgi-bin/dashboard.cgi).* In addition, for a glimpse into zzz's early years as an I2P developer, visit http://zzz.i2p/oldsite/index.html.*

Unfortunately, one of the largest archives on I2P, the user forum forum.i2p,* is no longer operational as of early 2017. There are discussions on the developer forum of bringing it back, archives intact. Any I2P researcher would want to watch – and hope – for the return of forum.i2p. If it does not, a major resource will be lost forever.

Building Your Own Archives

The disappearance of forum.i2p is not the only major Dark Web site to go offline and take its archives with it. For example, in my time on the Dark Web, I have seen dozens of social networking sites come and go.[26] The Darknet Market archives show that many markets have appeared and disappeared over the last five years, with the most recent victim being the largest market to date, Alphabay. Dark Web search engines and directories also appear online for a few months and then leave without a trace. My point here is this: there is no archive.org for the Dark Web. A site can be online one minute and gone the next. Therefore, my final recommendation for any digital humanities scholar studying the Dark Web would be: build your own archives. The Firefox plugin Zotero is a good option here: it is a bibliographic management tool which includes a Web page archiver, and it is compatible with the Tor Browser. It must be used with caution, however: the Tor Project recommends avoiding the use of plugins with the Tor Browser due to security considerations, because plugins are not audited by the Tor Project and they could leak a browser's identifying information. This includes other plugins, such as

26 For an archive of screenshots of many of them, see https://socialmediaalternatives.org/archive/items/browse?tags=dark+web.

screenshot plugins. Such security considerations must be weighed against the researcher's need to document Dark Web sites.

As more digital humanities scholars engage with the Dark Web, they will develop their own archives on their local computers. I would also suggest that we researchers begin to discuss how such archives could be combined into a larger archival project, one that can help future researchers understand the cultures and practices of these anonymizing networks. This effort would be similar to what Gwern et al achieve with the Darknet Markets archive (described above): the combination of ad-hoc research archives into one larger, more systematized archive.

Ethical Considerations

Of course, given that many users of Dark Web sites do so to avoid revealing their personal information, any such combined archive – indeed, any Dark Web research – much be done only after deep consideration about research ethics.

There are several guides to the ethics of Internet research, including the invaluable AOIR guidelines.[27] In addition, the Tor Project provides a research ethics guideline,[28] although it is geared towards large-scale analysis of the Tor network itself, does not say anything about research on Dark Web content, and thus is less valuable to humanistic work. Current Dark Web researchers are tackling ethical questions from a variety of disciplinary perspectives, including computer science and ethnography. Two important guides here are by James Martin and Nicholas Christin[29] and by Monica Barratt and Alexia Maddox,[30] both of which I draw on here.

The key takeaway of the AOIR ethics guide and the work of James and Christin and Barratt and Maddox is that the ethical quandaries faced by a researcher exploring anonymizing networks will vary greatly from site to site and from research project to research project. Thus, rather than laying out hard-and-fast rules for ethical research practices, Martin and Christin suggest that the researcher develop

> localised research practices that are cognizant of broader ethical norms and principles... while also remaining sufficiently flexible to adapt to the various contingencies associated with Internet research.[31]

They draw on Natasha Whiteman's *Undoing Ethics*, which suggests four domains to draw upon for ethical insights: academic/professional bodies and their norms, the researcher's own institution, the researcher's own politics and beliefs, and the "ethics of the researched." Due to space considerations, I will focus on the last to suggest ethical considerations arising from social norms I've observed in my time on the Dark Web.

One of the social norms of many, if not all, Dark Web sites is a prohibition against doxing individuals. Doxing refers to the publication of a person's personal details. In terms of research ethics, this cultural prohibition means that the researcher should not seek to connect online personas to their offline counterparts. It may be tempting to use small pieces of information – say, a subject's favorite food, ways of speaking, comments on the weather, or political stances – to develop a detailed profile of that person. It may be tempting to use these data to identify the person. But this would violate a fundamental aspect of the Dark Web: it is designed to anonymize both readers and producers of texts,

27 Annette Markham and Elizabeth Buchanan, “Ethical Decision-Making and Internet Research: Recommendations from the Aoir Ethics Working Committee (Version 2.0)” (Association of Internet Researchers, 2012), https://pure.au.dk/ws/files/55543125/aoirethics2.pdf.

28 “Ethical Tor Research: Guidelines,” Blog, *The Tor Blog*, (November 11, 2015), https://blog.torproject.org/blog/ethical-tor-research-guidelines.

29 James Martin and Nicolas Christin, “Ethics in Cryptomarket Research,” *International Journal of Drug Policy* 35 (September 2016): 84–91, doi:10.1016/j.drugpo.2016.05.006.

30 Barratt and Maddox, “Active Engagement with Stigmatised Communities through Digital Ethnography.”

31 Martin and Christin, “Ethics in Cryptomarket Research,” 86.

and thus its users seek to dissociate their reading and writing from their real-world identities. For examples of such small bits of information and how they could link pseudonymous people to real-world identities, as well as guidance about how to handle this information, see Barratt and Maddox.[32]

Another cultural norm is distrust, if not outright loathing, of the state. The Dark Web is largely comprised of persons with varying anarchist or libertarian political leanings, and along with these views comes a hatred of the state. Moreover, many of the activities that happen on Dark Web sites are illegal, and therefore participants in these sites fear law enforcement. In addition, Freenet, Tor, and I2P have all been developed by people who fear state censorship and repression. Thus, a research ethics developed in light of "the ethics of the researched" would call for the researcher to refuse active sponsorship from or collaboration with state agencies. To be certain, given the gutting of support for humanities research, it may be tempting to accept military/police/defense funding for Dark Web research, but such funding directly contradicts the ethical positions held by not only Dark Web participants, but many of the people who contribute to developing Dark Web technologies.

Finally, a very sticky issue: should researchers reveal their own identities to Dark Web site administrators and participants? This has direct bearing on the ethical approaches of Institutional Review Boards (IRB), because IRBs often require the researcher to provide potential participants with contact information, which of course means the researcher cannot maintain pseudonymity/anonymity. The goal is to provide research participants with an avenue to hold the researcher accountable if the researcher violates their confidentiality or security. Following this standard, Barratt and Maddox revealed their identities to participants on the Silk Road drug market and other Tor hidden services, seeking to allay anxieties that they were undercover law enforcement agents. However, they note that this choice led to concerns for their own safety; Maddox received graphic death threats from a member of a forum.[33] Unfortunately, another cultural practice that emerges on some anonymous online spaces is harassment and trolling, and such harassment is far more effective if the victim's identity is known. Thus there is a conflict between standard IRB practice and contemporary online research. As Martin and Christin note, IRBs may not have the domain knowledge to help researchers navigate this issue.[34]

Very early into my initial foray into the Dark Web, I was told by one participant that revealing personal information was taboo. This included revealing my own identity as a researcher to interviewees. However, IRB standards require the researcher to identity themselves. I was in a bind. However, in my research leading to my book project, I was fortunate to work with the University of Utah IRB, which recommended that I *offer* to provide my contact details to potential participants, which allowed them to decide whether or not they wanted this information. The vast majority of participants I spoke to declined to know who I am.[35] This may have reduced the likelihood of incidents such as the one Maddox described. But then again, it does raise the specter that Dark Web participants will find themselves feeling betrayed by me after I publish (especially if I am critical of them). To alleviate this issue, where possible, prior to submitting my manuscript to the press, I shared (anonymized) drafts of my work with interviewees and received their feedback.

Conclusion

As Ian Bogost and Nick Montfort argue, "people make negotiations with technologies as they develop

32 Barratt and Maddox, “Active Engagement with Stigmatised Communities through Digital Ethnography,” 10.
33 Ibid., 11.
34 Martin and Christin, “Ethics in Cryptomarket Research,” 88.
35 However, I should note that I was interviewing the builders of Dark Web search engines and the administrators and users of Dark Web social networking sites. These formats have different legal stakes than drug markets, the object Maddox and Barratt were studying. Thus, there may have been less anxiety among my participants that I was an undercover law enforcement agent. Again, this points to the difficulty of establishing hard-and-fast ethical rules for this line of research. I should also note that the Dark Web is a highly masculinized space. In the few cases where participants asked for my identity, they learned I identify as a cisgender male. In contrast, Maddox and Barratt discuss the specific harassment they received due to their female gender identities.

cultural ideas and artifacts, and people themselves create technologies in response to myriad social, cultural, material, and historical issues."[36] This is decidedly the case with Freenet, Tor, and I2P, the Dark Web systems I've discussed here. Although my suggestion that digital humanities scholars must engage with Dark Web technical infrastructures may strike some as a form of techno-elitism – the privileging of technical knowledge over other knowledges – for better or worse, technical knowledge is the lingua franca of these systems. I hope this collection of resources will be valuable for future researchers as they explore the relationship between Dark Web technology and culture.

Glossary

Tor: The term "Tor" can refer to several things, including the Tor Project, which is a nonprofit software development organization; its key software product, The Onion Router, which enables anonymous Internet use; and Tor hidden services, which are hidden Web sites only accessible by people using The Onion Router. The Onion Router works by linking a series of computers, called relays. If a user connects to a Web site, that connection is routed through the relays. Each hop between relays is encrypted, resulting in layers of encryption (hence the term "onion."). The router can be used to anonymously connect to standard Web sites, or to Hidden Services, whose physical locations are hidden.

Tor Browser: This is a modified version of the open source Firefox browser with The Onion Router built in. It is specifically modified to protect user identities as they browse the Web. It also allows for access to Tor Hidden Services, or hidden Web sites that end in the top-level name .onion. For example, one can access a copy of my homepage via the Tor browser at http://347k6hepharlncwb.onion/.

Freenet: This is a distributed network created in 1999 by Irish computer scientist Ian Clarke. Freenet's structure is as a peer to peer, distributed data storage system. This means that each computer that connects to the network is a peer, taking responsibility for moving data across the network. In addition, each peer also stores a portion of the data for the network. Thus, there are no centralized data stores, making it very hard to remove data from the network. Some of the data includes "freesites," or HTML and CSS files that can be viewed in a standard browser.

I2P: The Invisible Internet Project, started in 2003, is an encrypted network of peer-to-peer computers. Peer computers become parts of "tunnels", or chains of computers, enabling two computers to connect without either knowing the others' IP address. Using this system, one can host an "eepsite" (a hidden Web site, with an address ending in .i2p) on one's computer. For example, one can visit a version of my homepage at legitimate.i2p.

Topologies of anonymity: This is a term I use to describe Freenet, Tor, and I2P anonymizing networks. They anonymize Web browsing and publishing by dissociating users' identities from their activities. This is done using network topologies that hide IP addresses from each node in the network but still allow for data to pass through and find its intended recipient.

Software repositories: As open source projects, Freenet, Tor, and I2P rely on global networks of software coders to make their software. In order to coordinate this activity, they use software repositories, such as Github, which store computer code. If want to edit the code, I visit the repository, download the code, modify it, and then upload my modified version. If my modifications are accepted by the project, they are integrated into the main codebase, and the process can repeat. If at a later time my modification is found to be faulty, the code can be reverted back to a previous version. Hence, software repositories are archives of code changes, complete with comments from developers. This means they are a rich source of information about the projects being studied.

36 I. Bogost and N. Montfort, “Platform Studies: Frequently Questioned Answers,” in *Digital Arts and Culture 2009* (After Media: Embodiment and Context, UC Irvine, 2009), 3.

References

Aberer, Karl, Manfred Hauswirth, and Magdalena Punceva. “Self-Organized Construction of Distributed Access Structures: A Comparative Evaluation of P-Grid and FreeNet.” In *The 5th Workshop on Distributed Data and Structures (WDAS" 2003)*, 2003. http://infoscience.epfl.ch/record/54381.

Afilipoaie, Alois, and Patrick Shortis. “From Dealer to Doorstep–how Drugs Are Sold on the Dark Net.” GDPO Situation Analysis. Swansea University: Global Drugs Policy Observatory, 2015. http://www.swansea.ac.uk/media/Dealer%20to%20Doorstep%20FINAL%20SA.pdf.

Aked, Symon. “An Investigation into Darknets and the Content Available via Anonymous Peer-to-Peer File Sharing,” 2011. http://ro.ecu.edu.au/ism/106/.

Barratt, Monica J., Jason A. Ferris, and Adam R. Winstock. “Safer Scoring? Cryptomarkets, Social Supply and Drug Market Violence.” *International Journal of Drug Policy* 35 (September 2016): 24–31. doi:10.1016/j.drugpo.2016.04.019.

Barratt, Monica J., Simon Lenton, Alexia Maddox, and Matthew Allen. “‘What If You Live on Top of a Bakery and You like Cakes?’—Drug Use and Harm Trajectories before, during and after the Emergence of Silk Road.” *International Journal of Drug Policy* 35 (September 2016): 50–57. doi:10.1016/j.drugpo.2016.04.006.

Barratt, Monica J., and Alexia Maddox. “Active Engagement with Stigmatised Communities through Digital Ethnography.” *Qualitative Research*, May 22, 2016, 1468794116648766. doi:10.1177/1468794116648766.

Berkes, Jem E. “Decentralized Peer-to-Peer Network Architecture: Gnutella and Freenet.” *University of Manitoba Winnipeg, Manitoba, Canada*, 2003. http://www.berkes.ca/archive/berkes_gnutella_freenet.pdf.

Bogost, I., and N. Montfort. “Platform Studies: Frequently Questioned Answers.” In *Digital Arts and Culture 2009*, 8. UC Irvine, 2009.

Chen, Hsinchun. *Dark Web - Exploring and Data Mining the Dark Side of the Web*. New York: Springer, 2012. http://www.springer.com/computer/database+management+%26+information+retrieval/book/978-1-4614-1556-5.

Christin, Nicolas. “Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace.” In *Proceedings of the 22Nd International Conference on World Wide Web*, 213–224. WWW ’13. New York, NY, USA: ACM, 2013. doi:10.1145/2488388.2488408.

Clarke, Ian, Scott G. Miller, Theodore W. Hong, Oskar Sandberg, and Brandon Wiley. “Protecting Free Expression Online with Freenet.” *Internet Computing, IEEE* 6, no. 1 (2002): 40–49.

Clarke, Ian, Oskar Sandberg, Matthew Toseland, and Vilhelm Verendel. “Private Communication through a Network of Trusted Connections: The Dark Freenet.” *Network*, 2010. http://www.researchgate.net/profile/Vilhelm_Verendel/publication/228552753_Private_Communication_Through_a_Network_of_Trusted_Connections_The_Dark_Freenet/links/02e7e525f9eb66ba13000000.pdf.

Clarke, Ian, Oskar Sandberg, Brandon Wiley, and Theodore W. Hong. “Freenet: A Distributed Anonymous Information Storage and Retrieval System.” In *Designing Privacy Enhancing Technologies*, edited by Hannes Federrath, 46–66. Springer, 2001. http://link.springer.com/chapter/10.1007/3-540-44702-4_4.

colbyd. “[Freenet-Chat] Terrorism and Freenet,” January 9, 2002. https://emu.freenetproject.org/pipermail/chat/2002-January/001353.html.

Comey, James. “Encryption, Public Safety, and ‘Going Dark.’” Blog. *Lawfare*, July 6, 2015. http://www.lawfareblog.com/encryption-public-safety-and-going-dark.

Demant, Jakob Johan, and Esben Houborg. “Personal Use, Social Supply or Redistribution? Cryptomarket Demand on Silk Road 2 and Agora.” *Trends in Organized Crime*, 2016. http://www.forskningsdatabasen.dk/en/catalog/2304479461.

Dingledine, Roger. “[Freehaven-Dev] Re: [Freenet-Chat] MojoNation,” August 9, 2000. http://archives.seul.org//freehaven/dev/Aug-2000/msg00006.html.
Ehlert, Mathias. “I2P Usability vs. Tor Usability A Bandwidth and Latency Comparison.” In *Seminar. Humboldt University of Berlin. Berlin, Germany*, 2011. http://userpage.fu-berlin.de/semu/docs/2011_seminar_ehlert_i2p.pdf.
“Ethical Tor Research: Guidelines.” Blog. *The Tor Blog*, November 11, 2015. https://blog.torproject.org/blog/ethical-tor-research-guidelines.
Gehl, Robert W. “(Critical) Reverse Engineering and Genealogy.” *Foucaultblog*, August 16, 2016. doi:10.13095/uzh.fsw.fb.153.
———. “Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network.” *New Media and Society*, October 16, 2014, 1–17.
Guitton, Clement. “A Review of the Available Content on Tor Hidden Services: The Case against Further Development.” *Computers in Human Behavior* 29, no. 6 (November 2013): 2805–15. doi:10.1016/j.chb.2013.07.031.
Gusterson, Hugh. “Ethnographic Research.” In *Qualitative Methods in International Relations*, edited by Audie Klotz and Deepa Prakash, 93–113. Research Methods Series. Palgrave Macmillan UK, 2008. doi:10.1007/978-0-230-58412-9_7.
Hassan, Ahmed. “Mining Software Repositories to Assist Developers and Support Managers,” 2004. https://uwspace.uwaterloo.ca/handle/10012/1017.
Hout, Marie Claire Van, and Tim Bingham. “‘Silk Road’, the Virtual Drug Marketplace: A Single Case Study of User Experiences.” *International Journal of Drug Policy* 24, no. 5 (September 2013): 385–91. doi:10.1016/j.drugpo.2013.01.005.
———. “‘Surfing the Silk Road’: A Study of Users’ Experiences.” *International Journal of Drug Policy* 24, no. 6 (November 2013): 524–29. doi:10.1016/j.drugpo.2013.08.011.
Hutchings, Alice, and Thomas J. Holt. “The Online Stolen Data Market: Disruption and Intervention Approaches.” *Global Crime* 18, no. 1 (January 2, 2017): 11–30. doi:10.1080/17440572.2016.1197123.
John, Nicholas A. *The Age of Sharing*. Malden, MA: Polity, 2017.
Liu, Peipeng, Lihong Wang, Qingfeng Tan, Quangang Li, Xuebin Wang, and Jinqiao Shi. “Empirical Measurement and Analysis of I2P Routers.” *Journal of Networks* 9, no. 9 (2014): 2269–2278.
Mache, Jens, Melanie Gilbert, Jason Guchereau, Jeff Lesh, Felix Ramli, and Matthew Wilkinson. “Request Algorithms in Freenet-Style Peer-to-Peer Systems.” In *Peer-to-Peer Computing, 2002.(P2P 2002). Proceedings. Second International Conference On*, 90–95. IEEE, 2002. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1046317.
Maddox, Alexia, Monica J. Barratt, Matthew Allen, and Simon Lenton. “Constructive Activism in the Dark Web: Cryptomarkets and Illicit Drugs in the Digital ‘Demimonde.’” *Information, Communication & Society* 0, no. 0 (October 15, 2015): 1–16. doi:10.1080/1369118X.2015.1093531.
Markham, Annette, and Elizabeth Buchanan. “Ethical Decision-Making and Internet Research: Recommendations from the Aoir Ethics Working Committee (Version 2.0).” Association of Internet Researchers, 2012. https://pure.au.dk/ws/files/55543125/aoirethics2.pdf.
Martin, James. *Drugs on the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs*, 2014.
———. “Lost on the Silk Road : Online Drug Distribution and the ‘Cryptomarket.’” *Criminology & Criminal Justice* 14, no. 3 (2014): 351–367. doi:10.1177/1748895813505234.
Martin, James, and Nicolas Christin. “Ethics in Cryptomarket Research.” *International Journal of Drug Policy* 35 (September 2016): 84–91. doi:10.1016/j.drugpo.2016.05.006.
McGrath, Glenn. “[Freenet-Chat] Deep Philosophical Question,” January 2, 2002. https://emu.freenetproject.org/pipermail/chat/2002-January/000604.html.
Munksgaard, Rasmus, and Jakob Demant. “Mixing Politics and Crime – The Prevalence and Decline of Political Discourse on the Cryptomarket.” *International Journal of Drug Policy* 35 (September

2016): 77–83. doi:10.1016/j.drugpo.2016.04.021.
Nakamura, Lisa. *Cybertypes: Race, Ethnicity, and Identity on the Internet*. New York: Routledge, 2002.
Phelps, Amy, and Allan Watt. “I Shop Online – Recreationally! Internet Anonymity and Silk Road Enabling Drug Use in Australia.” *Digital Investigation* 11, no. 4 (2014): 261–272. doi:10.1016/j.diin.2014.08.001.
Pipinellis, Achilleas. *GitHub Essentials*. Packt Publishing, 2015.
Qin, Jialun, Yilu Zhou, Guanpi Lai, Edna Reid, Marc Sageman, and Hsinchun Chen. “The Dark Web Portal Project: Collecting and Analyzing the Presence of Terrorist Groups on the Web.” In *Proceedings of the 2005 IEEE International Conference on Intelligence and Security Informatics*, 623–624. Springer-Verlag, 2005. http://dl.acm.org/citation.cfm?id=2154737.
Tchabe, Gildas Nya, and Yinhua Xu. “Anonymous Communications: A Survey on I2P.” *CDC Publication Theoretische Informatik–KryptographieundComputeralgebra (Https://Www. Cdc. Informatik. Tu-Da Rmstadt. De)*, 2014. https://www.cdc.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_CDC/Documents/Lehre/SS13/Seminar/CPS/cps2014_submission_4.pdf.
Thomas, Matthew, and Aziz Mohaisen. “Measuring the Leakage of Onion at the Root,” 2014, 11.
Weimann, Gabriel. “Going Dark: Terrorism on the Dark Web.” *Studies in Conflict & Terrorism*, 2015. http://www.tandfonline.com/doi/abs/10.1080/1057610X.2015.1119546.
Zhang, Hui, Ashish Goel, and Ramesh Govindan. “Using the Small-World Model to Improve Freenet Performance.” In *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, 3:1228–1237. IEEE, 2002. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1019373.