YALE LAW & POLICY REVIEW

Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service Attacks

Joshua McLaurin[*]

INTRODUCTION 211

I. AN UNASSUMING THREAT 215
  A. *How Denial of Service Works* 216
  B. *One Person's Nuisance, Another's Crisis* 218

II. CRIMINAL LIABILITY FOR DOS ATTACKS IN THE UNITED STATES 222
  A. *State Cybercrime Statutes: Defining "Access"* 224
  B. *The Computer Fraud and Abuse Act: Defining "Damage"* 228

III. A TACTIC IN SEARCH OF A JUSTIFICATION 232
  A. *Doctrinal Obstacles to First Amendment Protection* 234
  B. *A Flawed Comparison to Civil Disobedience* 237
    1. A Tempting Comparison 239
    2. The Moral Legacy of American Civil Disobedience 242
    3. The True Nature of DoS Attacks 245

IV. THE LIMITS OF THE GENERATIVE INTERNET 247
  A. *Knowing What To Punish* 248
  B. *Making Cyberspace Safe for Democracy in a Physical World* 250

CONCLUSION 254

INTRODUCTION

In December 2010, the British government braced itself for a sudden threat: Overnight, tens of thousands of people had acquired a weapon called the Low

* Yale Law School, J.D. expected 2014; University of Georgia, M.P.A., B.A., 2010. My deep gratitude goes to Russell Balikian, Spencer Gilbert, and Ben Cassady for their contributions during the editing process. I would also like to thank Nicholas Bramble, Laura DeNardis, and fellow students in my Spring 2011 Access to Knowledge seminar for their helpful suggestions early in my writing process.

Orbit Ion Cannon (LOIC).[1] The good news for British authorities was that this "cannon" is not actually a space laser or hardly even a weapon; it is an old diagnostic computer program that allows an individual to test a network's capacity to handle traffic by sending information to the network's servers.[2] The bad news was that a nebulous online hacking collective called Anonymous was successfully encouraging these tens of thousands of people to use this tool to disrupt the availability of the websites of a few major corporations.[3] The program allowed individuals to participate in organized attempts to overwhelm each company's servers with information—so much information that those servers could not process other users' normal requests for access.[4] The goal of this type of assault, known as a denial-of-service (DoS) attack, is to disrupt a target organization's online presence for as long as the attacking computers continue to send such information.[5] The immediate consequence of a successful attack is somewhat anticlimactic: The target organization's website simply fails to load upon request. Nevertheless, the idea that thousands of nameless, faceless individuals could have banded together to produce that result adds social significance to what would otherwise be a purely technical problem.

To Anonymous, a group that considers itself a champion of free speech, the DoS attacks that it launched that December were symbolic protests conducted as part of a larger campaign of social activism called Operation Payback.[6] The group targeted PayPal, Visa, and Mastercard, among other entities, to protest the companies' withdrawal of support services from WikiLeaks, the controver-

1. Devin Dwyer, *Foot Soldiers for Wikileaks: 27,000 Download Attack Software Overnight*, ABC News (Dec. 10, 2010), http://abcnews.go.com/Technology/wikileaks-anonymous-cyber-attacks/story?id=12355960; Cahal Milmo & Nigel Morris, *'Prepare for All-Out Cyber War'*, Independent (Dec. 14, 2010), http://www.independent.co.uk/news/media/online/prepare-for-allout-cyber-war-2159567.html.

2. Dwyer, *supra* note 1; Milmo & Morris, *supra* note 1.

3. Dwyer, *supra* note 1.

4. The basic design of the Internet, which utilizes a client-server model, makes this strategy possible. In a client-server exchange, a computer called a server responds to requests by other client computers once it establishes individual connections with each client. Accordingly, a server needs various types of finite resources—processing, memory, and storage capacity—in order to handle clients' requests. *See* Ethan Zuckerman et al., Berkman Ctr. for Internet & Soc'y, Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites 15 (2010), *available at* http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_DDoS_Attacks_Human_Rights_and_Media.pdf.

5. *See* Jelena Mirkovic et al., Internet Denial of Service: Attack and Defense Mechanisms 11 (2005).

6. Anonymous's Operation Payback was a series of actions against a range of organizations alleged by Anonymous to have suppressed free speech. David Sarno, *'Hactivists' Fight for Their Cause Online*, L.A. Times, Dec. 11, 2010, at A1.

sial website that exposed classified U.S. diplomatic cables to the public.[7] In a manifesto posted online around the time of the attacks, a spokesman for Anonymous appealed to the democratic sensibilities inherent in the group's actions, asserting that "Anonymous does not seek to disturb the public peace nor the average Internet citizen; for average Internet citizens are most of us who are Anonymous."[8] The British government had a much different take on the attacks: They were crimes (for which authorities soon arrested five citizens)[9] and a wake-up call for the government to reassess its own cybersecurity.[10] Indeed, for activists interested in WikiLeaks's right to free expression, launching attacks designed to silence their targets was an awkward tactical choice. While a number of activists in addition to Anonymous have argued that DoS attacks are just an online form of political protest,[11] these attacks can do a surprising amount of damage. They exploit basic weaknesses in the architecture of the Internet to produce consequences ranging from the suppression of protest by repressive governments to the unavailability of public services and potentially large losses to the economy.[12]

In a recent editorial, *The Economist* addressed claims that Operation Payback was comparable to civil disobedience or other forms of protest by articulating the intuitive distinction between the two:

> [I]n a free society the moral footing for peaceful lawbreaking must be an individual's readiness to take the consequences, argue in court and fight for a change in the law. . . .
>
> Protesters in cyberspace, by contrast, are usually anonymous and untraceable. The furtive, nameless nature of [DoS] attacks . . . [makes] anonymous perpetrators look like cowardly hooligans, not heroes.[13]

Unfortunately, while American federal and state governments have cybercrime statutes on the books that are broad enough to cover DoS attacks, the text of these statutes often includes no reference to the unique type of harm created when legitimate users cannot access online content. The law largely continues

7. *Id.*; Mark Clayton, *Did WikiLeaks Bring on Cyberwar? Maybe a Cyber Sit-In*, Christian Sci. Monitor (Dec. 23, 2010), http://www.csmonitor.com/USA/2010/1223/Did-WikiLeaks-bring-on-cyberwar-Maybe-a-cyber-sit-in.

8. Dwyer, *supra* note 1.

9. Josh Halliday, *Police Arrest Five over Anonymous WikiLeaks Attacks*, Guardian (London), Jan. 27, 2011, at 15.

10. Milmo & Morris, *supra* note 1.

11. *See, e.g.*, *infra* note 140 and accompanying text.

12. *See infra* Section I.B.

13. Editorial, *The Rights and Wrongs of Hacktivism*, Economist, Dec. 18, 2010, at 16. For another popular commentary arguing that the nonhierarchical nature of social media dilutes their potency as direct causes of change, see Malcolm Gladwell, *Small Change: Why the Revolution Will Not Be Tweeted*, New Yorker, Oct. 4, 2010, at 42, *available at* http://archives.newyorker.com/?i=2010-10-04#folio=042.

to rely on vague, outmoded language to criminalize new types of harmful actions as technology evolves.[14] In the meantime, Anonymous is promoting a new paradigm for protest and democratic community that implicitly calls into question the desirability of statutes with such broad reach. The inattention that courts[15] and academic literature[16] have shown to DoS attacks—and how their perpetrators assign meaning to them—constitutes a missed opportunity to refine how the law comprehends the elements of effective civic engagement as more human interaction takes place online.

This Note analyzes the significance of DoS attacks in four parts. Part I explains what DoS attacks are and the types of harm that they are capable of producing: economic losses, the disabling of critical infrastructure, and the suppression of others' speech.

Part II provides an overview of the current treatment that American law gives to DoS attacks, beginning with a summary of the most common state law approaches to addressing cybercrime in Section A and moving to a discussion of the primary federal cybercrime statute in Section B.

Part III considers the case that has been made by various hacker-activists in support of the prosocial character of DoS attacks. Section A addresses potential First Amendment protections for DoS attacks and concludes that, while these attacks may involve no more than the sending of excessive information to targets, courts would not likely protect them as a form of speech due to the harm that they cause. Section B evaluates the claim that DoS attacks are fundamentally like civil disobedience. It summarizes the similarities that support this claim, reviews the American tradition of civil disobedience, and concludes that DoS attacks lack the elements of legitimacy, grounded in physical space, that are crucial to the role that civil disobedience plays in a healthy democracy.

Part IV discusses the ways in which the DoS phenomenon should inform legal thinking about cyberspace. This Part moves from a particular discussion of DoS attacks to show more generally that overreliance on traditional legal concepts to govern cyberspace puts at risk values such as the consistent application of criminal law and deliberative democracy. Section A emphasizes that the priority of the legal community should be to clarify the essential values that law protects in physical space instead of simply relying on convenient metaphors to expand precedents to cyberspace. Section B demonstrates that moral and legal confusion in classifying DoS attacks arises from a dangerous tendency to presume that pervasive self-expression, uprooted from a legacy of civic engagement

14. *See infra* Part II.

15. There have been very few cases involving DoS attacks in a criminal context. Only in the last few years has the U.S. Department of Justice even begun to indict the perpetrators of major DoS attacks. *See, e.g.*, Press Release, U.S. Att'y's Office for the Cent. Dist. of Cal., Two European Men Charged with Conspiring To Launch Cyberattacks Against Websites of Two U.S. Companies (Oct. 2, 2008), *available at* http://www.justice.gov/criminal/cybercrime/walkerIndict.pdf; *infra* note 44.

16. *See infra* note 40.

grounded in physical space, is the most important component of the "speech" at the heart of our political tradition.

I. An Unassuming Threat

Anonymous was not the only group using DoS attacks to make a statement about WikiLeaks in late 2010. On November 28, 2010, WikiLeaks was itself the target of a DoS attack. The terse "tweet"[17] in which WikiLeaks made this revelation reads like the climax of a presidential wartime speech: "We are currently under a mass distributed denial of service attack."[18] Even so, WikiLeaks's announcement lacked a certain gravity. Words like "attack" make the process sound somewhat intimidating, but even distributed denial-of-service attacks,[19] which are potentially much larger and more effective than the type of attacks that LOIC made possible, do not directly put individuals or computer systems in physical danger. The average news reader is not likely to be alarmed, especially if she learns how widespread these attacks already are: In a leading study on the volume of these attacks, researchers determined that as many as 68,700 attacks had taken place worldwide in the preceding three-year period.[20] The idea of hackers quietly flooding servers with more requests than the servers can handle does not quite measure up intuitively to the kind of threats that a world familiar with terrorism can imagine. Especially when the victim is WikiLeaks, an organization that leaked secret cables that an individual allegedly took illegally from a U.S. government computer,[21] DoS attacks may just appear to be the chosen means by which hackers war with each other and not worth a great deal of attention from law enforcement or analysts.

Contrast this recent episode with events in the spring of 2007, when hackers infected up to a million computers worldwide and instructed them to launch a three-week DoS offensive against media, banking, and government networks in Estonia.[22] The source of the attack was unclear, but analysts believe that in addi-

17. "Tweets" are small bursts of information that users of the website Twitter.com can share with one another over a real-time network. *About*, Twitter, http://www.twitter.com/about (last visited Nov. 24, 2011).

18. WikiLeaks, *Tweet by WikiLeaks*, Twitter (Nov. 28, 2010), http://www.twitter.com/#!/Wikileaks/status/8920530488926208/.

19. *See infra* text accompanying note 29.

20. David Moore et al., *Inferring Internet Denial-of-Service Activity*, 24 ACM Transactions on Computer Systems 115, 116 (2006), *available at* http://www.caida.org/publications/papers/2006/backscatter_dos/backscatter_dos.pdf.

21. Noam Cohen, *Ex-Hacker Who Accused Suspect of Army Leak Is Still Talking*, N.Y. Times, June 28, 2010, at B3.

22. Adrian Blomfield, *Estonia Calls for NATO Cyber-Terrorism Strategy*, Daily Telegraph (London), May 18, 2007, at 18; Mark Landler & John Markoff, *After Computer Siege in Estonia, War Fears Turn to Cyberspace*, N.Y. Times, May 29, 2007, at A1.

tion to knowledgeable hackers who likely planned and executed the attack, thousands of ordinary Russians may have participated in the offensive after reading instructions that were posted on dozens of Russian websites seeking to capitalize on nationalist fervor against Estonia.[23] The attack did not cripple the government's websites or online capabilities for the full three weeks, but the attack was effective in diverting a substantial amount of the government's attention and resources.[24] Small nuisances that by themselves would amount to inconveniences in today's electronic world—a Member of Parliament without access to email for four days or a traveling Estonian businessman without access to his bank accounts—aggregated to become enough of a breach in national security for Estonia to present the issue formally to NATO.[25]

A. How Denial of Service Works

Compared to other categories of crime that involve more physical activity, cybercrime is fairly discreet. Although perpetrators can do a lot of damage, they can do so quietly and from the comfort of their own homes. Pure DoS attacks exemplify the seemingly benign actus reus of cybercrime. A perpetrator need not "break and enter" into any computer systems to gain control of them in order to carry out the attack. The simplest form of a DoS attack is information overload: A single person with sufficient computing resources sends enough "packets"[26] of information to a target server for those packets to deplete the server's resources, preventing it from responding to requests from other users.[27] Some varieties of the basic attack rely on modified packets that can tax a server more effectively by tricking the server into tying up scarce resources.[28]

---

23. Blomfield, *supra* note 22, at 18.

24. Robert Vamosi, *Cyberattack in Estonia—What It Really Means*, CNET News (May 29, 2007), http://news.cnet.com/2008-7349_3-6186751.html (quoting Jose Nazario, Senior Researcher, Arbor Networks).

25. Blomfield, *supra* note 22, at 18; Landler & Markoff, *supra* note 22, at A1.

26. Data travels over the Internet in small, discrete chunks called "packets." Computers send each other these packets as part of a system of communication called TCP/IP (Transmission Control Protocol/Internet Protocol) that serves as the foundation of the Internet. Mirkovic et al., *supra* note 5, at 296, 298.

27. *Id.* at 16.

28. *Id.* at 16-17. One example is a "SYN flood" attack, which exploits communication protocols to deceive the target server. Computers exchanging data using TCP/IP must first open a connection with each other through a process known as a "three-way handshake." The first computer sends a specific type of packet called a "SYN packet" to request a connection, to which the second computer will respond with an acknowledgment. Finally, the first computer establishes the connection with a second packet of its own. In a SYN flood attack, the packet that the attacking computer first sends to request a connection has fake, or "spoofed," source IP address information. The target server therefore sends its acknowledg-

Distributed denial of service, or DDoS, is a type of DoS attack that involves conduct more traditionally understood as "hacking." Preparation for a DDoS attack begins when an individual user gains some degree of control over a number of other computers, usually through the spread of a specially coded computer virus that the user distributes over the Internet to infect vulnerable systems.[29] Computer experts colorfully refer to this process as the "recruitment" of "zombies" for use in an attack.[30] Then, the user is able to instruct the infected systems to engage in a DoS attack against the target server. These attacks can take on a much larger scale than simple DoS attacks because of the rapidity and ease with which the attack's manager can enlarge the network of computers that he controls, called a "botnet," by spreading malicious code over the Internet.[31]

As with a physical war, the outcome of an attack depends in large part on the level of resources available to the target. Target servers with larger bandwidth and more data ports for opening connections with other computers will fare better on average, since a successful attack must deplete one of those resources.[32] When attackers seize additional resources in order to scale up their attacks, targets can respond by implementing algorithms that evaluate incoming packets and filter out illegitimate traffic. The diversity of systems within "zombie" networks makes filtering very difficult, however, since attack managers can make the flood of requests appear to originate from a wide variety of legitimate sources.[33] A savvy attacker can thus manipulate the content of packets to make it much more difficult to trace the packets back to him and to determine his identity.[34]

---

ment to a false return address, and the third part of the "handshake" never happens. As a result, the comparatively few resources that a server dedicates to opening connections are tied up managing "half-open" connections that the attacker never intended to complete. *Id.* at 80-81.

29. *Id.* at 17.

30. *See* Paul Robichaux, *Distributed Denial-of-Service Attacks and You*, Microsoft TechNet, http://technet.microsoft.com/en-us/library/cc722931.aspx (last visited Nov. 25, 2011).

31. *See* Mirkovic et al., *supra* note 5, at 24-27. Microsoft claims to have cleaned up over 9.5 million host computers between August 2003 and April 2004 that had been compromised by this sort of activity. *Id.* at 26.

32. *See* U.S. Computer Emergency Readiness Team, *Denial of Service Attacks*, CERT Coordination Center (June 4, 2001), http://www.cert.org/tech_tips/denial_of_service.html.

33. Tao Peng, Christopher Leckie & Kotagiri Ramamohanarao, *Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems*, 39 ACM Computing Surveys 1, 1-2 (2007), *available at* http://www.cs.mu.oz.au/~tpeng/p1-peng.pdf.

34. The structure of the Internet—which resembles a near-endless switchboard of possible pathways on which information can travel—makes this problem difficult to overcome. *Id.* at 7-8. Network service providers are theoretically capable of

B. *One Person's Nuisance, Another's Crisis*

The U.S. government has developed more capacity to deal with cyberthreats since the 2007 attacks on Estonia,[35] but American targets are by no means immune. In fact, DoS attacks on American targets are fairly common. An annual survey conducted by the Computer Security Institute found that in each of the last six years, between seventeen percent and thirty-two percent of the organizations surveyed were the target of a DoS attack.[36] The attacks can be costly: The survey found that the combined cost of DoS attacks for a group of 269 respondents amounted to about $26 million in 2004 alone.[37] The true cost, however, may be higher after factoring in losses in consumer confidence: After a series of DoS attacks in 2000 on major companies that included Yahoo, eBay, E*Trade, CNN, and Amazon.com, over forty percent of respondents to a PC Data Online poll said that they were less likely to shop online.[38] Further, the

---

tracking the route that a packet of information takes to a destination server, but the large costs and privacy concerns associated with doing so can make retracing that route impracticable. *Id.* at 8; *see also id.* at 15, 31 (listing proposals for technical self-help solutions to attacks that employ spoofing, with cautious optimism only for proposals that address spoofing close to the packets' source).

35. Recent efforts by the United States to promote cybersecurity have included both foreign assistance and domestic policy changes. In May 2011, the United States sent four Secret Service agents to investigate cybercrimes in the Baltic region and to serve as support staff to the governments of Estonia, Latvia, and Lithuania in warding off cybercrime. *United States Secret Service*, Embassy U.S.: Tallinn, Est., http://estonia.usembassy.gov/usss.html (last visited Nov. 25, 2011); *U.S. Secret Service Opens Cybercrime Office in Estonia*, Huffington Post (May 20, 2011), http://www.huffingtonpost.com/2011/05/20/us-secret-service-cybercrime-estonia_n_864946.html. To protect American interests, the Pentagon released a new cyberstrategy in the last year that provides for the use of conventional force in response to some cyberattacks, and accompanying this strategy is a new, classified list of cyberweapons the United States keeps at its disposal. Ellen Nakashima, *Defense Dept. Develops List of Cyber-Weapons*, Wash. Post, June 1, 2011, at A3.

36. Robert Richardson, 2010/2011 CSI Computer Crime and Security Survey 17 (2011), *available at* http://gatton.uky.edu/FACULTY/PAYNE/ACC324/CSISurvey2010.pdf. Survey respondents were executives or computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions, and universities. *See id.* at 4-5.

37. Lawrence A. Gordon et al., 2004 CSI/FBI Computer Crime and Security Survey 1, 10 (2004), *available at* http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf. See CSI Computer Crime and Security Survey Archive, http://gocsi.com/SurveyArchive (last visited Nov. 25, 2011), for reports from 2004 through 2009 in which respondents report less profound losses.

38. Patricia Jacobus, *Poll Shows People Worried About Net Attacks*, ZDNet (Feb. 16, 2000), http://www.zdnetasia.com/poll-shows-people-worried-about-net-attacks-13025577.htm.

costs may be so small to any one business that the trouble is just not worth reporting.[39]

Outside of the news coverage that DoS attacks receive as a result of events like the attacks on Estonia or WikiLeaks, the public remains largely unconcerned with the unique character of the attacks or how they differ from other cybercrimes.[40] The worry for analysts who discuss the dangers of DoS attacks is not the economic cost faced by individual businesses—though those costs are potentially serious in some cases—but rather the threat that ongoing attacks pose to general access to public services or important information.[41] The architects of the Internet made fundamental design choices in favor of connectivity and resource-sharing that provide cause for this worry.[42] Servers, the physical

39. *See* Robert Richardson, 2008 CSI Computer Crime & Security Survey 4, 23 (2008), *available at* http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf.

40. Scholarly literature in particular has very little to say about the special significance of DoS attacks. When academic commentators mention denial of service, it is usually as one of a number of forms of cybercrime. The discussion tends to turn primarily toward practical questions about law enforcement and costs as opposed to the attacks' unique relationship to free speech and associated democratic norms. *See, e.g.*, Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 Santa Clara Computer & High Tech. L.J. 177 (2000); Charlotte Decker, Note, *Cyber Crime 2.0: An Argument To Update the United States Criminal Code To Reflect the Changing Nature of Cyber Crime*, 81 S. Cal. L. Rev. 959 (2008); Note, *Immunizing the Internet, or: How I Learned To Stop Worrying and Love the Worm*, 119 Harv. L. Rev. 2442 (2006).

41. Prior to Estonia, a few isolated but noteworthy events prompted some members of Congress to conclude that some critical online infrastructure was vulnerable enough to DoS attacks to merit more attention. *See Cyber Attack: Roadblocks to Investigation and Information Sharing: Hearing Before the Subcomm. on Tech., Terrorism, & Gov't Info. of the S. Comm. on the Judiciary*, 106th Cong. 7 (2000) [hereinafter *Cyberattack Hearing*] (statement of Louis J. Freeh, Dir., Fed. Bureau of Investigation). For example, in 2000, a DoS attack successfully took down an FBI website for several hours. *Id.* at 3 (statement of Sen. Dianne Feinstein). In 1996, a teenage prankster making telephone calls in a manner analogous to a DoS attack periodically clogged up 911 telephone lines in eleven Florida counties over the course of a few weeks. *Id.* at 7 (statement of Louis J. Freeh, Dir., Fed. Bureau of Investigation); *see also Swedish Teen Fined for Prank Florida Calls*, Tampa Trib., May 2, 1997, at 2. This event made it clear that unsophisticated actors with limited resources were capable of nontrivial interference with networked emergency services. As "traditional operations in essential services, such as banking, transportation, power, health, and defense, are being progressively replaced by cheaper, more efficient Internet-based applications," this type of threat becomes more serious. Peng, Leckie & Ramamohanarao, *supra* note 33, at 2.

42. One fundamental difference between the Internet and telephone networks, for example, is that "circuit-switched" telephone lines allocate channels for each connection that are wholly separate from one another throughout the connection.

machines that store content on the Internet, can host multiple unaffiliated websites in an arrangement called "shared hosting."[43] Thus, even though an attacker's intent is usually to target one particular website, a DoS attack against a server that hosts multiple websites could cause a significant amount of "collateral damage" as users are blocked from accessing websites that themselves were not targeted.[44]

Other special servers called Domain Name System (DNS) root servers are responsible for directing traffic any time an Internet user types in a website's textual web address instead of its numerical IP address.[45] A worst-case scenario in the context of DoS might be what attackers attempted to bring about in a 2002 DDoS attack on all thirteen of the Internet's DNS servers: the disabling of large chunks or all of the Internet's IP address directory system.[46] While the attack was unsuccessful due to the system's resilience, over half of the thirteen servers were seriously affected.[47] Had the attack successfully disabled all of the servers for a period of forty-eight hours—a hypothetical worth considering even if it is highly unlikely—it is possible that Internet users would have been unable to access websites for which they did not know the IP address.[48] The episode made it clear that serious, large-scale DDoS attacks pose a unique threat to DNS root servers and are a primary concern in efforts to secure those servers.[49]

Nonetheless, a survey of attempts at large-scale DoS attacks suggests that the primary significance of such attacks is not their potential to bring about

---

"Packet-switching," by contrast, makes use of shared pathways that can be clogged. Peng, Leckie & Ramamohanarao, *supra* note 33, at 7-8.

43. The reason why an organization would engage in basic shared hosting or an evolved form called "cloud computing" is to avoid the costs of maintaining server hardware in-house. A recent crash in Amazon.com's cloud computing services took down the websites of some major customers, demonstrating the vulnerability of websites hosted on shared servers. *See* Joseph Galante, *Amazon Web Services Disruption Knocks Customer Sites Offline*, BLOOMBERG (Apr. 21, 2011), http://www.bloomberg.com/news/2011-04-21/amazon-com-says-some-web-services-for-businesses-not-available.html.

44. For example, one man received a sentence of thirty months' jail time for aiming DDoS attacks at his business competitors, causing hundreds of thousands of dollars in damage. *See* Press Release, U.S. Att'y's Office for the Dist. of N.J., Michigan Man Gets 30 Months for Conspiracy To Order Destructive Computer Attacks on Business Competitors (Aug. 25, 2006), http://www.justice.gov/criminal/cybercrime/araboSent.htm.

45. Daniel Karrenberg, *DNS Root Name Server FAQ*, INTERNET SOC'Y, http://www.isoc.org/briefings/020 (last updated Feb. 2008).

46. *See* MIRKOVIC ET AL., *supra* note 5, at 5-6.

47. Karrenberg, *supra* note 45.

48. *Id.*

49. *Id.*

doomsday: Experts concede that the vast majority of attacks are small nuisances and that hypothetical catastrophes are unlikely.[50] The highest value of analyzing DoS attacks may be in understanding how and why perpetrators carry them out in cyberspace, where technology continues to pose new questions about the line between self-expression and injury to others. Estonia's experience suggests the presence of a wide array of motives and strategies behind DoS attacks with broad participation. For attackers with particularly disruptive motives and vulnerable targets, however, DoS looks less like protest and more like sabotage. The Kremlin may not have been involved in the attacks on Estonia, but Russian involvement was harder to deny when Georgia's computer systems succumbed to a DoS attack while Russia simultaneously initiated a military operation in South Ossetia in 2008.[51]

Beyond implications for diplomacy between states, politically motivated attempts at online incapacitation pose serious problems for independent media, human rights groups, or other organizations doing advocacy work that rely on their websites to disseminate information.[52] The Russian-Georgian conflict provides a clear example. A 2009 DDoS attack that shut down Twitter for several hours contained a strange twist: The attackers ordered their botnet to send a flood of emails linking to pages on Twitter and Facebook, which in turn linked to the website of a pro-Abkhazia activist.[53] The activist's website was unable to handle the massive traffic and shut down for the duration of the attack.[54] Other threats to oppositional voices can be more direct. The Chinese government is thought to rely on DDoS attacks as part of its arsenal against human rights groups, as evidenced by untraceable yet powerful DDoS attacks in early 2010 that brought down a number of Chinese human rights websites for sixteen

50. *See* Mirkovic et al., *supra* note 5, at 28 ("Even some of the high-profile attacks on major Internet sites were not that difficult to handle once the defenders were aware of the nature of the attack and had a little time to respond to it.").

51. *See* Tom Espiner, *Georgia Accuses Russia of Coordinated Cyberattack*, CNET (Aug. 11, 2008), http://news.cnet.com/8301-1009_3-10014150-83.html.

52. The Berkman Center for Internet and Society at Harvard University released a report in 2010 summarizing its research into the prevalence of DDoS attacks against independent media. *See* Zuckerman et al., *supra* note 4. Researchers discovered reports of 140 attacks against the websites of over 280 different independent media and human rights organizations during the twelve-month period from September 2009 to August 2010. *Id.* at 26.

53. Barbara Ortutay, *Activist Hackers Attack Twitter*, Times Argus (Barre-Montpelier, Vt.), Aug. 7, 2009 (News), at 1, *available at* 2009 WLNR 26949151. Abkhazia is a secessionist region in Georgia that Russia has recognized as independent. Based on the ambiguous intentions behind the attack, it is hard to say which side launched it. *Id.*

54. *Id.*

hours.[55] As recently as April 18, 2011, the servers hosting U.S. website Change.org began experiencing occasional interruptions in service due to an attack originating in China after the website's petition for the release of Chinese prisoner Ai Weiwei gained popularity.[56] Even short attacks pose an appreciable threat if the suppressed content is time sensitive. One example is the DDoS attack that blocked access to opposition newspapers' websites in Kyrgyzstan during the country's 2005 elections.[57] The attacks were traceable back only to Ukrainian "hackers-for-hire," thus leaving open the question of whether the Kyrgyz government covertly sponsored an act of repression.[58]

II. Criminal Liability for DoS Attacks in the United States

The policy argument that government should address the DoS threat responds to a collective action problem inherent in the Internet's nonhierarchical structure. Internet service providers, which oversee the delivery of data from the Internet to end users, do not want to spend resources policing activity over the Internet if such prevention efforts allow other Internet service providers to "free ride" without engaging in such costly efforts themselves.[59] The problem became salient enough for the U.S. government to take notice in early 2000, however, when DoS attacks took down the websites of several major corporations.[60] President Clinton responded by calling an "emergency summit" of government officials, Internet company executives, and security experts to address the threat.[61]

55. *See* Owen Fletcher, *Chinese Human Rights Sites Hit by DDoS Attack*, Computerworld (Jan. 26, 2010), http://www.computerworld.com/s/article/9147938/Chinese_human_rights_sites_hit_by_DDoS_attack.

56. The attacks even prompted a Congresswoman from Connecticut to send an open letter to her colleagues in Congress that asked for the involvement of Secretary of State Clinton in condemning the attacks. Benjamin Joffe-Walt, *Congresswoman Asks Colleagues To Pressure Sec. Clinton over Foreign Cyber-Attack on Change.org*, Change.org Blog (May 11, 2011), http://blog.change.org/2011/05/congresswoman-asks-colleagues-to-pressure-sec-clinton-over-foreign-cyber-attack-on-change-org/.

57. Jonathan Zittrain & John Palfrey, *Internet Filtering: The Politics and Mechanisms of Control*, *in* Access Denied: The Practice and Policy of Global Internet Filtering 41 (Ronald Deibert et al. eds., 2008), *available at* http://www.opennet.net/sites/opennet.net/files/Deibert_03_Ch02_029-056.pdf.

58. *See id.*

59. Karrenberg, *supra* note 45 ("[N]o ISP wants to bear the associated cost first while others profit and do not incur the cost. There is clearly an area for government action here."); *see also* Peng, Leckie & Ramamohanarao, *supra* note 33, at 37.

60. *See supra* text accompanying note 38.

61. C. Satapathy, *Impact of Cyber Vandalism on the Internet*, 35 Econ. & Pol. Wkly. 1059, 1060 (2000).

The FBI promptly began a criminal investigation into the attacks,[62] but it was Canada that eventually prosecuted the youth who went by the pseudonym "Mafiaboy" and was responsible for perpetrating the attacks.[63] After pleading guilty to fifty-five charges of criminal mischief,[64] he received a sentence of only eight months in a youth detention center.[65] Notwithstanding the large-scale response his actions triggered, one expert warned that Mafiaboy's amateur behavior was only the "tip" of the hacker "iceberg" and that thousands of other hackers were learning from his mistakes.[66]

The pervasiveness and potential disruptiveness of DoS attacks give the United States a stake in managing the threat, whether or not the perpetrators of attacks or their targets fall within its jurisdiction. Rather than pursuing a purely regulatory path for each cyberthreat, the federal government and all fifty states have adopted legislation criminalizing actions that threaten the integrity of computers and networks generally.[67] The rationale behind the use of criminal law for this purpose is pragmatic and straightforward: Given the evolving opportunities for individuals to use technology to threaten others' privacy, safety, and material assets, it is appropriate to update criminal laws that already exist to protect against such threats in the physical world.[68]

This Part analyzes the current treatment of DoS attacks under American criminal law. Federal and state statutes succeed in proscribing DoS attacks by

62. *Id.*

63. Dan Verton, *Teen Hacker 'Mafiaboy' Pleads Guilty to 55 Charges*, Computer-World (Jan. 18, 2001), http://www.computerworld.com/s/article/56555/Teen_hacker_Mafiaboy_pleads_guilty_to_55_charges.

64. *Id.*

65. *'Mafiaboy' Sentenced to 8 Months*, Wired (Sept. 13, 2001), http://www.wired.com/techbiz/media/news/2001/09/46791.

66. Verton, *supra* note 63.

67. U.S. Dep't of Justice, Prosecuting Computer Crimes 1-3 (Scott Eltringham ed., 2d ed. 2010), *available at* http://www.justice.gov/criminal/cybercrime/ccmanual/ccmanual.pdf; Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1615 (2003).

68. S. Rep. No. 99-432, at 1 (1986) (explaining that it is important for federal legislation to evolve in response to "a new type of criminal—one who uses computers to steal, to defraud, and to abuse the property of others"), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2480; *see also* Cal. Penal Code § 502 (West 2011) ("It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems."). *See generally* Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. Pa. L. Rev. 1003 (2001) (endorsing an economic theory of cost deterrence as a reason to refocus cybercrime prevention efforts on analyzing the choices of an individual cybercriminal).

relying on a definition of "damage" or "access" that covers the particular effects that an attack has on a server. As a result, perpetrators of attacks would indeed be criminally liable under practically every jurisdiction's generic cybercrime statutes. However, no generic statute provides convincing legal principles that distinguish DoS attacks from lawful use of the Internet because liability under those statutes turns on an inherently ambiguous inquiry into whether use was "authorized." This Part concludes that the only apparent way for criminal statutes to avoid this ambiguity is to identify intent to bring about denial of service as an element of the crime. Such a narrowly drawn statute more effectively communicates the law's condemnation of DoS attacks by isolating the decision to attack as a unique source of harm.

Depending on the attacker's motives and relationship to the target, DoS attacks could fall under a number of categories of criminal conduct involving fraud or extortion and other threats.[69] This Part does not aim to describe all the possible avenues to criminal liability that DoS attacks could create. Rather, it seeks to identify the essentially criminal nature of DoS attacks and the ways in which federal and state statutes could be applied consistently to proscribe attacks without reaching legitimate Internet use.

A. State Cybercrime Statutes: Defining "Access"

States took an early lead in the criminalization of computer misuse.[70] At first, courts mostly relied upon the common law crime of theft to classify and punish any harm done through computers.[71] Due to the difficulty of demarcating property in computer usage, courts were forced to infer a violation of property rights from the presence of a substantial harm even if no principled explanation of how the defendant violated those rights was available.[72] The parallels

69. A few such federal statutes include prohibitions on extortion that affects commerce, threats transmitted in interstate commerce, receipt of proceeds of extortion, and fraud in connection with access devices. MIRKOVIC ET AL., *supra* note 5, at 244-45.

70. Almost half of the states had adopted legislation specific to computer crimes by 1983. Dodd S. Griffith, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 459 (1990). The federal government was actually somewhat reluctant to pass its first cybercrime legislation in the mid-1980s, given concerns about redundancy and overstepping federal authority. *Id.* at 458-59.

71. Kerr, *supra* note 67, at 1607-09.

72. *Id.* at 1610-11 ("[T]he [courts'] reasoning seemed to go something like this: When a person is harmed, the person loses something of value; when a person loses something of value, they are deprived of property. Therefore the infliction of harm triggers a theft.").

between hacking and crimes such as trespass or burglary are hard to ignore,[73] but traditional property crime laws proved to be insufficient to deal with instances of misuse that commentators agreed were criminal even when they did not cause consequential harms.[74] Accordingly, every state responded to this deficiency by developing a criminal statute specific to computer crimes.[75]

In describing the actus reus of computer crime, states primarily rely on the concept of "access," which most states define by statute.[76] Courts' historical concern with the protection of economic interests in property is reflected in an expansive, clear definition of "access" that favors the owner of the computer(s) being accessed. A very common formulation of this definition is to "instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network."[77]

This definition readily enables the criminalization of DoS attacks. Such an all-encompassing definition essentially makes any interaction with a computer network an instance of access and would indisputably categorize DoS attacks as such. Of course, "access" cannot be the basis for liability by itself; otherwise, all Internet use would be unlawful. To distinguish between lawful and unlawful usage, most states establish offenses in terms of access "without authorization."[78] Authorization would presumably serve the same function as permission or consent in the definition of criminal trespass to real property, under which the property owner's wishes ultimately determine whether access is lawful.[79]

---

73. *See, e.g.*, Susan W. Brenner, *Is There Such a Thing as "Virtual Crime"?*, 4 CAL. CRIM. L. REV. 1, ¶¶ 81-82, 84 (2001) ("Conceptually, it makes no difference whether the area that is unlawfully accessed exists in the physical world or in the virtual world; the harm to the owner of that area is logically indistinguishable.").

74. *See* Kerr, *supra* note 67, at 1615.

75. *Id.*

76. Those that do not define "access" do define an alternate word such as "use" to cover essentially the same conduct. *See, e.g.*, COLO. REV. STAT. § 18-5.5-101 (2011); GA. CODE ANN. § 16-9-92 (2011).

77. FLA. STAT. § 815.03 (2011). No fewer than thirty states include a close derivative of this language in their definition of access or use. *See, e.g.*, N.Y. PENAL LAW § 156.00(7) (McKinney 2011) ("'Access' means to instruct, communicate with, store data in, retrieve from, or otherwise make use of any resources of a computer, physically, directly or by electronic means."). Illinois is an example of a state that replaces "resources" with "services." *See* 720 ILL. COMP. STAT. ANN. 5/17-55 (West 2011). The statute goes on to provide that "'[s]ervices' includes but is not limited to computer time, data manipulation, or storage functions." *Id.*

78. Susan W. Brenner, *State Cybercrime Legislation in the United States of America: A Survey*, 7 RICH. J.L. & TECH. 28, ¶ 15 (2001), http://jolt.richmond.edu/v7i3/article2.html.

79. *See* 3 WAYNE R. LAFAVE, SUBSTANTIVE CRIMINAL LAW § 21.2 (2d ed. 2011) ("In the typical criminal trespass case, however, the claim that the defendant's entry or remaining was unlawful will come down to the contention that it was so because a

Assuming that no one would authorize an attack on his own server, any DoS attack would thus be criminal in one of the many jurisdictions wherein unauthorized access to a computer network is itself a criminal offense, regardless of the amount of loss accruing to the target server's owner.[80]

Unfortunately, these statutes retain the fundamental ambiguity plaguing the prosecution of computer crimes at common law: There does not appear to be a principled way to distinguish DoS attacks from lawful conduct since "unauthorized" remains ambiguous.[81] States may attempt to delineate unlawful access by proscribing conduct that causes "disruption" in networks,[82] but this strategy provides little help in elaborating the criminal nature of DoS attacks. A person who accesses a busy ticket-sales website may well know that he is preventing another user from loading the site during times of high traffic, but he is hardly a criminal for wanting to be first in line.

Some states have been able to avoid an overbroad or imprecise prohibition of DoS attacks by making the intent to effectuate denial of service an element of

---

person with a legal interest in the property or an agent of that person had exercised a legal right to forbid such entry or remaining.").

80. For an example of the simplest, least serious form of liability that a state might impose for this conduct, see HAW. REV. STAT. § 708-895.7 (2011) ("A person commits the offense of unauthorized computer access in the third degree if the person knowingly accesses a computer, computer system, or computer network without authorization."). In granting summary judgment to a woman whose husband broke into her protected online information, a federal district court in Arkansas recently noted how little case law exists on an Arkansas computer trespass statute—an observation that makes sense in light of how uncomplicated the analysis in computer trespass cases often is. *See* Miller v. Meyers, 766 F. Supp. 2d 919, 924 (W.D. Ark. 2011) ("While there is little case law interpreting this particular statute, it is clear to the court that Defendant intentionally accessed the MySpace and Yahoo computer networks without authorization and should now be held liable for computer trespass.").

81. Any attempt to define authorization across the board runs into trouble quickly. Tennessee defines authorization as "any and all forms of consent, including both implicit and explicit consent," TENN. CODE ANN. § 39-14-601 (2011), but this definition turns on the meaning of "consent" and could well be void for vagueness as applied in some cases. *See infra* text accompanying notes 107-109. A requirement of express consent might seem promising in tackling the vagueness problem, *see* COLO. REV. STAT. § 18-5.5-101 (2011), but of course an Internet user cannot reasonably expect to have affirmative permission from server owners to load every website she visits. One suggestion for resolving the ambiguity limits the definition of "unauthorized access" to the bypassing of code-based restrictions on system use. *See* Kerr, *supra* note 67, at 1600.

82. Alaska's statute proscribes unauthorized access that causes a disruption in computer networks; however, the statute does not define "disruption." *See* ALASKA STAT. § 11.46.740 (2010).

the crime.[83] The language employed by such prohibitions ranges from a basic description of a perpetrator's design[84] to the direct use of the term "denial of service attack."[85] These provisions may still only cover those actions that are "without authorization,"[86] but the inquiry into whether a DoS attack was specifically authorized is necessarily simpler than determining whether a server owner has authorized any action qualifying as "access." Unlike most Internet use, DoS attacks cause harm by design and are presumptively unwelcome to targets. An organization would likely authorize a DoS attack on its servers only in order to allow computer security practitioners to test the networks that they manage.[87] The phrase "without authorization" in some DoS-specific statutes therefore functions mostly as a limitation on liability for a category of conduct that is only rarely sanctioned in the first place. Consequently, all statutes specific to DoS attacks locate the essential criminal nature of the attacks—the character

83. *See, e.g.*, Md. Code Ann., Crim. Law § 7-302 (West 2010) (requiring intent to interrupt the operation of computers or networks); 18 Pa. Cons. Stat. § 7612 (2011) (prohibiting intentionally or knowingly engaging in a scheme that has denial of service as its design). Knowingly taking part in a purposive, organized attack effectively amounts to an intent to attack, *cf.* United States v. Phillips, 477 F.3d 215, 223 (5th Cir. 2007) (finding that defendant's knowing use of a computer program designed to achieve unlawful ends was substantively the same as intending those unlawful ends), but knowingly denying service to others could be entirely devoid of any intent to deny service, *see infra* text accompanying note 112.

84. La. Rev. Stat. Ann. § 14:73.4 (2010) ("An offense against computer users is the intentional denial to an authorized user, without consent, of the full and effective use of or access to a computer, a computer system, a computer network, or computer services.").

85. 18 Pa. Cons. Stat. § 7612. Some states even have a spyware statute that isolates the distribution of malicious code used in DDoS attacks as an offense separate from simply interfering with others' access through standard DoS attacks. *See, e.g.*, N.H. Rev. Stat. Ann. § 359-H:2 (2011) ("A person . . . who is not an authorized user, shall not knowingly cause a computer program or spyware to be copied onto the computer of a consumer and use the program or spyware to . . . [t]ake control, through intentionally deceptive means, of the consumer's computer by . . . [u]sing the consumer's computer as part of an activity performed by a group of computers for the purpose of causing damage to another computer, including launching a denial of service attack.").

86. *See, e.g.*, N.C. Gen. Stat. § 14-456 (2011) ("Any person who willfully and without authorization denies or causes the denial of computer, computer program, computer system, or computer network services to an authorized user . . . is guilty of a Class 1 misdemeanor.").

87. The LOIC used by Anonymous was originally a tool designed for testing purposes, after all. *See supra* text accompanying note 2.

that separates them consistently from lawful conduct—in the choice to engage in a specific type of harmful conduct, not in a failure to obtain authorization.[88]

B. The Computer Fraud and Abuse Act: Defining "Damage"

The federal government's primary legal response to computer crimes is codified in the Computer Fraud and Abuse Act (CFAA) at 18 U.S.C. § 1030, which has been amended several times since its enactment in 1986 to adapt to newly realized threats.[89] Its prohibitions cover practically any instance of cybercrime nationally because of the statute's expansive definition of "protected computers": The term includes, in addition to certain computers used by financial institutions and the federal government, any computer "used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."[90]

The Act's primary provisions include prohibitions against extracting information from computers,[91] accessing exclusive government computers or especially sensitive information,[92] engaging in threats to perpetrate cybercrime as a means of extortion,[93] committing fraud,[94] and generally taking actions that cause damage to computers.[95] The primary mechanism used by the statute to cover the range of technical means by which computer users could pursue these illegitimate goals is to make "access[ing] a computer without authorization" or "exceed[ing] authorized access" the first element of an offense.[96] Offenses defined according to this mechanism usually require some additional action or interference on behalf of the offender;[97] consequently, these provisions do not apply to the simplest DoS attacks, which only require an attacker to access the resources that a server uses to communicate with other computers.

---

88. The State may never punish an "unlawful intent" absent some sort of action on that intent, but it is fully consistent to suggest that the intent element of a given crime supplies a criminal nature to the accompanying action that it otherwise would not have attained. *See* 1 LaFave, *supra* note 79, § 6.1.

89. U.S. Dep't of Justice, *supra* note 67, at 2-3.

90. 18 U.S.C. § 1030(e)(2)(B) (Supp. 2010); *see* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1577-78 (2010).

91. 18 U.S.C. § 1030(a)(1)-(2) (2006 & Supp. 2010).

92. *Id.* § 1030(a)(1), (3) (2006).

93. *Id.* § 1030(a)(7) (2006 & Supp. 2010).

94. *Id.* § 1030(a)(4), (6) (2006).

95. *Id.* § 1030(a)(5)(A) (2006 & Supp. 2010).

96. *Id.* § 1030(a)(1) (2006); *see* Kerr, *supra* note 90, at 1561-62.

97. *See* sources cited *supra* notes 91-94.

The provision most relevant to DoS attacks, § 1030(a)(5), defines offenses with a greater emphasis on damage than access. The first subparagraph of this provision, § 1030(a)(5)(A), does not even mention access at all: It holds liable anyone who "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer."[98] Of course, DoS attacks are not damaging in a conventional sense because they do not physically harm target servers.[99] Nevertheless, the Act defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information."[100] Based on this definition, it is clear that liability under the CFAA should attach to any perpetrator of a DoS attack who intends the effects that an attack has on a server and has not been authorized to carry out the attack by the server's owner.[101] DDoS attacks would create liability on multiple counts: In addition to decreasing the availability of data on target servers, these attacks rely on unauthorized access to and impair the integrity of every "zombie" computer commandeered without authorization to attack those servers.[102]

It is not a cause for celebration that the statute relies on definitions that are broad enough to criminalize DoS attacks:[103] The language may be too vague to

98. 18 U.S.C. § 1030(a)(5)(A) (Supp. 2010).

99. *See supra* text accompanying note 27.

100. 18 U.S.C. § 1030(e)(8) (2006).

101. In the penalties subsection, the statute provides that felony liability under § 1030(a)(5)(A), with a maximum of ten years' imprisonment, attaches only if the harm caused falls into one of several categories: loss aggregating to $5000 in a year; interference with medical examination, diagnosis, or treatment; physical injury to anyone; a threat to public safety; damage to federal government systems used in furtherance of national security or justice; or damage affecting ten or more protected computers in a year. *Id.* § 1030(c)(4)(A)(i), (B)(i) (2006 & Supp. 2010). The bar for felony liability is thus not very high. Since any number of protected computers might use the resources of a server under attack, there seems to be no reason why this last type of harm would not automatically trigger felony liability for most DoS attacks. Also, $5000 is not a very high threshold: When calculating its "loss," a target can include consequential damages or expenditures related to assessing damage in addition to estimates of lost revenues. *Id.* § 1030(e)(11) (2006). In any event, a DoS attack would always be at least a misdemeanor punishable by a fine and up to one year in prison. *See id.* § 1030(c)(4)(G)(i) (2006 & Supp. 2010).

102. *See* Sinrod & Reilly, *supra* note 40, at 199-202. Given the expansive definition of "damage," unauthorized access to zombie systems would create liability under subparagraphs (B) and (C) as well. *See* § 1030(a)(5)(B)-(C) (2006 & Supp. 2010).

103. The Department of Justice's *Prosecuting Computer Crimes* manual claims that the provision addressing damage to others' data was conceived in part to protect against DoS attacks. *See* U.S. Dep't of Justice, *supra* note 67, at 2.

survive a constitutional due process analysis in some cases.[104] Although provisions involving "access" are not relevant to the prosecution of DoS attacks, it is worth noting that the CFAA does not ever define "access" despite using the word in the text of most of the statute's offenses. More problematic is that the CFAA, like state statutes, fails to define "authorized" and thus leaves open the question of exactly which types of conduct constitute "unauthorized access."[105] The unfortunate consequence is that prosecutors and courts are free to adopt an interpretation of the statute that proscribes more activity than Congress might have intended.[106] In one prominent case, the government sought conviction of someone who created a fake profile on MySpace, arguing that merely violating a "Terms-of-Service" agreement on a website rendered the defendant's access "unauthorized" under the CFAA.[107] Given that the maximum penalty for this single violation would have been five years' imprisonment,[108] the district court's decision to grant the defendant's motion for judgment of acquittal on void-for-vagueness grounds seems eminently reasonable.[109]

---

104. The Supreme Court has made it clear that as-applied constitutional challenges to criminal statutes under the Due Process Clause may succeed where the lack of clarity as to exactly what conduct is unlawful violates "the requirement that a legislature establish minimal guidelines to govern law enforcement." City of Chicago v. Morales, 527 U.S. 41, 60 (1999) (quoting Kolender v. Lawson, 461 U.S. 352, 358 (1983)) (internal quotation marks omitted). This principle holds true "even if an enactment does not reach a substantial amount of constitutionally protected conduct" because it may still "fail[] to establish standards for the police and public that are sufficient to guard against the arbitrary deprivation of liberty interests." *Id.* at 52.

105. Kerr, *supra* note 90, at 1573-78 (drawing on void-for-vagueness case law to suggest that a legitimate constitutional question is raised if the meaning of the words "unauthorized access" controls the scope of the statute). For an overview of theories explicating "unauthorized access" in the context of the CFAA, see Cyrus Y. Chung, Note, *The Computer Fraud and Abuse Act: How Computer Science Can Help with the Problem of Overbreadth*, 24 HARV. J.L. & TECH. 233 (2010).

106. Civil liberties groups recently sent a letter to ranking members of the Senate Judiciary Committee expressing their concern about the potential for prosecutorial abuse under the CFAA due to the vague meaning of "authorized." Letter from Laura W. Murphy, Dir., Wash. Legislative Office, Am. Civil Liberties Union et al., to Sen. Patrick Leahy & Sen. Charles Grassley (Aug. 3, 2011), *available at* http://cdt.org/files/pdfs/CFAA_Sign-on_ltr.pdf.

107. United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

108. The defendant in this case was charged with violating § 1030(a)(2)(C), *id.* at 452, punishable by up to five years' imprisonment, § 1030(c)(2)(B)(ii).

109. *Drew*, 259 F.R.D. at 467 ("It is unclear that every intentional breach of a website's terms of service would be or should be held to be equivalent to an intent to access the site without authorization or in excess of authorization. This is especially the case with MySpace and similar Internet venues which are publically available for access and use.").

The phrase "damage without authorization" threatens similar problems with vagueness. While one could assume that DDoS and simpler DoS attacks would be unauthorized under the statute, there is no consistent principle for distinguishing between harmful, presumptively unauthorized damage and the incidental kind of damage that must be authorized for the Internet to function. The enumerated types of damage that trigger felony liability under § 1030(a)(5)(A) are mostly obvious harms that would presumably be unauthorized, but misdemeanor liability could be predicated on more benign types of unauthorized damage.[110] After all, every attempt to access a website is at least a knowing impairment of the overall availability of the server hosting the site—and thus meets the statutory definition of "damage"—yet no one would suggest that an individual's personal use is unauthorized.

The mens rea provision of § 1030(a)(5)(A) does not resolve the ambiguity inherent in the word "authorization," but the provision does narrow the scope of the offense. The statute prevents plainly lawful Internet use from falling within the scope of the prohibition by requiring that an offender *intentionally* and not just knowingly engage in conduct that causes unauthorized damage.[111] DoS attacks have damage as their design, whereas an ordinary Internet user's purpose is to access information legitimately even as he is aware that he is consuming server resources.[112] Congress even expressly took this distinction into account in drafting one of the amendments to the CFAA.[113] And although the language still allows for the possibility that intentional damage would be authorized, it is hard to imagine that prosecutors would find this ambiguity to be an obstacle in taking on high-profile attacks that cause sizable harm.[114]

110. *See supra* note 101 and accompanying text.

111. 18 U.S.C. § 1030(a)(5)(A) (Supp. 2010).

112. For this reason, the prohibition by some states on "knowingly" or "recklessly" denying service to other users is overbroad and inappropriate. *See* CAL. PENAL CODE § 502 (West 2010) ("[A]ny person who commits any of the following acts is guilty of a public offense: . . . Knowingly and without permission us[ing] or caus[ing] to be used computer services."); DEL. CODE ANN. tit. 11, § 934 (2011) (using the word "intentionally" but also attaching liability for recklessly interrupting service).

113. *See* S. REP. NO. 99-432, at 5 (1986) ("[T]he Committee is concerned that the 'knowingly' standard in the existing statute might be inappropriate for cases involving computer technology."), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2483-84; *see also* United States v. Phillips, 477 F.3d 215, 222 (5th Cir. 2007) (explaining the significance of the amended "intentionally" standard in the context of the damage provisions in § 1030(a)(5)).

114. Losses that reach the $5000 mark trigger a higher level of penalties. *See supra* note 101 and accompanying text. Although proving damages of at least that amount may have been straightforward in one prosecution for a DDoS attack against eBay under the CFAA, *see* Decker, *supra* note 40, at 985-86, measuring damages from DoS attacks is inherently difficult, *see* Sinrod & Reilly, *supra* note 40, at 227.

III. A Tactic in Search of a Justification

No matter how clearly a statute may mandate the attachment of criminal liability to conduct, criminal liability is not a final judgment on the moral legitimacy of the conduct. To the extent that criminal law casts a normative shadow over prohibited conduct, it does so because of the assumption that the State would punish an individual only for a good reason—namely, that the conduct in question is sufficiently antisocial.[115] Nonetheless, our criminal laws may fail to map out with perfect accuracy our collective judgments as to which behaviors are impermissibly antisocial, especially since there is not always agreement about which conduct should fall into that category. A legal prohibition against murder is an easy point of agreement, and likewise most people would agree that it is wise to keep the law *out* of conflicts over immoral conduct that would be difficult or inappropriate for authorities to punish, such as breaking a gratuitous promise that induces no reliance[116] or carelessly hurting someone's feelings.[117] Disputes about the appropriateness of criminal liability may surface in marginal cases, however, where an offender violates a sensible legal rule but lacks moral blameworthiness.[118] It is at these junctures that would-be offenders

115. As used in this Note, the word "antisocial" is intended to carry a moral connotation consistent with ordinary criminal punishment theory. *See* Kyron Huigens, *The Jurisprudence of Punishment*, 48 Wm. & Mary L. Rev. 1793, 1802-06 (2007). While moral disapproval alone is not sufficient to criminalize conduct, Lawrence v. Texas, 539 U.S. 558, 560 (2003) ("[T]he fact that a State's governing majority has traditionally viewed a particular practice as immoral is not a sufficient reason for upholding a law prohibiting the practice . . . ."), the presence of a satisfying moral rationale for criminalizing conduct appears to be almost necessary in the American system of criminal law, *see, e.g.*, John Shepard Wiley, Jr., *Not Guilty by Reason of Blamelessness: Culpability in Federal Criminal Interpretation*, 85 Va. L. Rev. 1021 (1999) (finding that, despite upholding the constitutionality of some strict-liability crimes, the U.S. Supreme Court has tended to honor the longstanding ideal of requiring moral blameworthiness in federal criminal convictions).

116. *See, e.g.*, Mount Sinai Hosp. of Greater Miami, Inc. v. Jordan, 290 So. 2d 484, 486-87 (Fla. 1974).

117. *See* Restatement (Second) of Torts § 46 cmt. d (1965) ("There is no occasion for the law to intervene in every case where some one's feelings are hurt."). The qualifier "carelessly" matters, of course, given the presence of a mens rea requirement in the definition of emotional harm torts. *See* Restatement (Second) of Torts § 46 (1965). To the extent that mens rea matters in making emotional harm actionable, it is evident that considerations of justice are indeed sensitive to the "badness" of someone's intent regardless of the minimal nature of the harm.

118. One commentator writing about small public order offenses notes that lack of moral blameworthiness, rather than a simple lack of legal clarity, may explain why a case falls near the "borderline" of criminal law. Josh Bowers, *Legal Guilt, Normative Innocence, and the Equitable Decision Not To Prosecute*, 110 Colum. L. Rev. 1655, 1666-67 (2010). He recognizes that "First Amendment and vagueness questions tend to raise the toughest legal issues in the context of petty street-sweeping

and their allies have an opportunity to contest the presumption that the criminal law as it stands is an accurate codification of society's ideal restrictions on conduct.[119]

A number of activists have tried to carve out space at the borderline of criminal activity for the legitimate use of DoS attacks as a form of political protest. They argue that the technology, even if disruptive, is a means to the legitimate end of expressing disagreement with the policies of governments or large corporations.[120] One label that has emerged to describe the concept of cybercrimes-as-protest is "hacktivism,"[121] a word that captures the tension between the criminal and democratic elements of such tactics. Indeed, even the first usage of the word "hacker" in modern tech parlance in 1963[122] reflected the conflict between the dangerous consequences of interfering with networks and the creativity inherent in such actions.[123] Creativity does not make criminal conduct any less prohibited, of course, and it is safe to say that some form of expression more nuanced than mere creativity is necessary to begin questioning whether expressive conduct should be immune from criminal sanction.

Proponents of DoS attacks have made a number of arguments to frame the tactic as a legitimate form of expression, ranging from appeals to principles of free speech[124] to the assertion of an extrajudicial authority to punish certain

---

statutes. But in the main, the proposition is somewhat uncontroversial: Greater agreement exists about the wrongfulness of conduct that violates core criminal statutes." *Id.* at 1667.

119. *See* Paul H. Robinson & John M. Darley, *The Utility of Desert*, 91 Nw. U. L. Rev. 453, 475-76 (1997) ("The criminal law's influence as a moral authority has effect primarily at the borderline of criminal activity, where there may be some ambiguity as to whether the conduct really is wrong.").

120. *See infra* text accompanying notes 140-148.

121. *Cyberattack Hearing*, *supra* note 41, at 26-27 (statement of Louis J. Freeh, Dir., Fed. Bureau of Investigation).

122. *See* Posting of Fred R. Shapiro, fred.shapiro@yale.edu, to Am. Dialect Soc'y Mailing List, ADS-L@listserv.uga.edu (June 13, 2003), http://listserv.linguistlist.org/cgi-bin/wa?A2=ind0306B&L=ADS-L&P=R5831.

123. *See* Henry Lichstein, *Services Curtailed: Telephone Hackers Active*, Tech (Cambridge, Mass.), Nov. 20, 1963, at 5c, *available at* http://duartes.org/gustavo/blog/post/first-recorded-usage-of-hacker. A professor at MIT was quoted in the school newspaper saying that he "appreciate[d the] curiosity" of the boys responsible for shutting down certain telephone networks but warned that repeated involvement would expose them to criminal liability and disciplinary action by the school. *Id.*

124. *See infra* Section III.A. The Electronic Disturbance Theater (EDT) justified its DoS attack against the Mexican government in 1998 as "a symbolic gesture in support of Mexico's Zapatistas." Stefan Wray, *Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics*, 4 Switch, no. 2, 1998, http://switch.sjsu.edu/web/v4n2/stefan; *see also*

organizations for operating against principles of freedom and openness of information on the Internet.[125] At the latter extreme, attackers may even be willing to acknowledge that the attacks themselves are "wrong" but nevertheless claim that they are excusable as part of an appropriately measured response to the target group's reprehensible conduct.[126] This radical claim clearly does not provide shelter from the criminal law, but such a claim does point to the resolve of hacktivists who defiantly choose to break the law. This Part addresses the variety of arguments made by proponents of the use of DoS attacks to justify the attacks on legal and moral grounds and concludes that DoS attacks merit neither protection under the First Amendment nor a comparison to civil disobedience.

A. Doctrinal Obstacles to First Amendment Protection

As hacktivism grows in popularity, the likelihood increases that those engaging in less technically invasive attacks such as simple DoS might seek constitutional protection from prosecution. One public defender in California has already stated his intention to make such an argument in one of the first upcoming CFAA prosecutions for political DoS attacks. Commenting on his homeless client's alleged DoS attack against the City of Santa Cruz for its anti-camping law, the lawyer claimed that "[t]here's no such thing as a DDoS 'attack' . . . . A DDoS is a protest . . . . It's not a crime, it's speech."[127] Attackers would be highly unlikely to succeed in a First Amendment challenge to laws prohibiting DoS, however, because of the limited circumstances in which the

Seth F. Kreimer, *Technologies of Protest: Insurgent Social Movements and the First Amendment in the Era of the Internet*, 150 U. PA. L. REV. 119, 159 (2001) ("The argument of the EDT has been that the sending of queries is merely a repeated exercise of free speech rights.").

125. Open Letter from Anonymous to Sony, http://anonnews.org/?p=press&a=item&i=787 (last visited Oct. 26, 2011). In this letter, Anonymous responds to Sony's lawsuit against hackers who provided information about "jailbreaking" PlayStation 3 consoles. The letter states that Sony has committed an "unforgivable offense against free speech and Internet freedom" and asserts that Anonymous is engaging in "disciplinary" actions against a web domain that Sony is only "renting." *Id.* In general, a spectrum of possible justifications from legal to anarchic aligns closely with John Rawls's map of different types of dissent. *See* JOHN RAWLS, A THEORY OF JUSTICE 363 (1971) ("[Forms of opposition to democratic authority] range from legal demonstrations and infractions of law designed to raise test cases before the courts to militant action and organized resistance. A theory specifies the place of civil disobedience in this spectrum of possibilities.").

126. *See, e.g.*, Open Letter from Anonymous to Sony, *supra* note 125 ("Now Anonymous is attacking your private property because we disagree with your actions. And that seems, dare we say it, 'wrong.' Sound familiar?").

127. Ryan J. Reilly, *'Homeless Hacker' Lawyer: DDoS Isn't an Attack, It's a Digital Sit In*, TALKING POINTS MEMO (Sept. 28, 2011), http://idealab.talkingpointsmemo.com/2011/09/homeless-hacker-lawyer-ddos-isnt-an-attack-its-a-digital-sit-in.php.

case law recognizes expressive conduct as protected speech. Two main Supreme Court cases define the extent to which the First Amendment protects expressive conduct: *Spence v. Washington*[128] and *United States v. O'Brien*.[129]

In *Spence*, the Court established that expressive conduct attains the status of symbolic speech if that conduct carries with it an intent to convey a particularized message that the audience is likely to understand.[130] This latter requirement sets a high bar for DoS attacks—it is implausible to suggest that the meaning behind a DoS attack would be apparent to users for whom a website simply fails to load.[131] Even so, the first DoS attack on WikiLeaks in November 2010 is an example of an attack that might satisfy this test. Although the attack was anonymous, opposition to the release of classified State Department cables was motivated by one concern—protecting U.S. troops and assets—that could be presumed to be the rationale of the attacker.[132] It is a stretch to conclude that his intention was to make a symbolic statement about the importance of national security rather than to prevent the release of documents, but at least his cause was clear.

No matter how clear an attacker's message may be, though, a DoS attack would fail under the test that the Court established just a few years prior to *Spence*. In *O'Brien*, the Court ruled that the government may regulate expressive conduct by drafting laws within its constitutional power that serve an important interest and are not aimed at suppressing speech.[133] The core logic of the *O'Brien* holding is found in the Court's declaration that it could not "accept

128. 418 U.S. 405 (1974).

129. 391 U.S. 367 (1968).

130. 418 U.S. at 410-11.

131. *See* Nicholas Bramble, *Ill Telecommunications: How Internet Infrastructure Providers Lose First Amendment Protection*, 17 MICH. TELECOMM. & TECH. L. REV. 67, 89 (2010), *available at* http://www.mttlr.org/volseventeen/bramble.pdf.

132. One hacker in particular, calling himself "Jester," posted on Twitter to claim responsibility for the attack. He explained that he attacked WikiLeaks "for attempting to endanger the lives of our troops and other assets." Angela Moscaritolo, *Political Hacker Takes Credit for Wikileaks DDoS Attack*, SC MAGAZINE (Nov. 29, 2010), http://www.scmagazineus.com/political-hacker-takes-credit-for-wikileaks-ddos-attack/article/191669. Whether "Jester" was responsible for the attack or not, it seems safe to attribute his rationale to whoever was responsible since public opposition was very unified in its concern for U.S. assets. A nationwide McClatchy-Marist poll found that seventy percent of adults who had heard about WikiLeaks believed that WikiLeaks was "doing more harm than good by allowing enemies of the U.S. to see confidential and secret information about foreign policy." Marist Poll, *WikiLeaks: Prosecution Warranted . . . Does More Harm than Good, Say Americans*, MARIST INST. PUB. OPINION (Dec. 13, 2010), http://maristpoll.marist.edu/1213-wikileaks-prosecution-warranted-%e2%80%a6-does-more-harm-than-good-say-americans/.

133. 391 U.S. at 376-77.

the view that an apparently limitless variety of conduct can be labeled 'speech' whenever the person engaging in the conduct intends thereby to express an idea."[134] Even though a political argument such as the one implicated in the November 2010 attacks on WikiLeaks is of a nature that the First Amendment fundamentally encourages, DoS attacks themselves are not as inherently *expressive* as they are *disruptive* (of others' ability to speak, no less). The pure transfer of information is not necessarily pure speech—and thus not necessarily deserving of constitutional protection—if the effect of that transfer is to impose harms that the State has an interest in preventing.[135] While an individual may certainly expect a type of heightened review to be applied to restrictions on speech,[136] expressive conduct must first qualify as speech to receive such protection.

In sum, it seems clear that a governmental interest in preventing harmful interference with the flow of webpage information from a server host to a user would foreclose any First Amendment claim. This interest arises directly from the spirit of the First Amendment itself: In the words of one blogger, "You don't stand up for free speech by using a muzzle."[137] Courts may not use the First Amendment to restrict the behavior of nonstate attackers acting in a private capacity,[138] but they can certainly refuse to call DoS attacks "speech" in the interest of a healthy public sphere and economic well-being.

---

134. *Id.* at 376.

135. In a 2000 case concerning the posting of computer code that would illegally decrypt digitally encrypted videos on proprietary DVDs, one district court reaffirmed that while mere expressiveness may implicate the First Amendment, it does not necessarily command the First Amendment's protection. Suggesting that the extent of harm caused by the computer code is of vital concern, the court noted that simply concluding that the First Amendment is relevant "still leaves for determination the level of scrutiny to be applied in determining the constitutionality of regulation of computer code." Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 304, 327 (S.D.N.Y. 2000).

136. *See, e.g.*, Ysursa v. Pocatello Educ. Ass'n, 555 U.S. 353, 358 (2009) (recognizing that content-based restrictions on speech are "'presumptively invalid' and subject to strict scrutiny" (quoting Davenport v. Wash. Educ. Ass'n, 551 U.S. 177, 188 (2007))); Turner Broad. Sys., Inc. v. FCC, 520 U.S. 180, 213-14 (1997) (outlining the components of "intermediate scrutiny" for content-neutral regulations of speech).

137. Tom Watson, *Denial of Service, Denial of Speech*, Tom Watson (Dec. 12, 2010), http://tomwatson.typepad.com/tom_watson/2010/12/denial-of-service-denial-of-speech.html.

138. The text only speaks of Congress, *see* U.S. Const. amend. I, and the Fourteenth Amendment's incorporation of the First Amendment's restraints applies only to state actors. *See, e.g.*, United States v. Morrison, 529 U.S. 598, 621 (2000).

B. A Flawed Comparison to Civil Disobedience

Another argument in support of the legitimacy of DoS attacks as a form of public protest does not hinge upon the attacks' constitutional merit. Those who consider themselves stakeholders in the use of DoS attacks may make a purely moral argument in support of the tactic and push for public support in pursuit of the tactic's longer-term acceptance as legal or useful.[139] These advocates face quite a challenge: Despite statutes and First Amendment case law that would deny to DoS attacks legal status as protected speech, these people nonetheless seek to articulate the inherent value that DoS attacks have as a form of protest in bringing about desirable change. To be successful, this vision must persuasively distinguish between that which is criminal and that which is immoral, in effect recruiting the public at large to be stakeholders themselves in the effort to frame DoS attacks as prosocial.

Ever since its first DoS attack against the Mexican government in 1998, a group calling itself the Electronic Disturbance Theater (EDT) has taken the lead in touting the prosocial character of DoS attacks.[140] Expressing its disagreement with the treatment of Zapatista rebels in Mexico, the group encouraged the use of a primitive DoS program called FloodNet against the websites of the Mexican president, the Mexican Secretariat of Governance, and even the U.S. White House as acts of so-called "electronic civil disobedience."[141] Instead of using the malicious, invasive code that is characteristic of DDoS attacks, FloodNet was the first deployment of a type of attack called Client-Side Distributed Denial-of-Service (CDoS).[142] This program invited mass participation in a DoS attack but on a *voluntary basis*, by downloading a program that would enable an

139. These stakeholders can include perpetrators themselves or even mere onlookers who express support for the tactic. A good example of someone with this latter profile is a commenter on Amazon's website whose username was the name of a computer hacker heroine from a famous book series and who wrote in support of the Operation Payback attacks. Jane Warren, *Bizarre World of the Hacktivists*, Daily Express (U.K.), Dec. 10, 2010, http://www.express.co.uk/posts/view/216593/Bizarre-world-of-the-hacktivists ("Whilst I will not personally engage in any cyber activities against you, I will lend my wholehearted support to those who do and I will watch on with amusement and gratification as you slowly sink." (quoting the commenter) (internal quotation marks omitted)).

140. *See* Stefan Wray, *The Electronic Disturbance Theater and Electronic Civil Disobedience*, Thing.net (June 17, 1998), http://www.thing.net/~rdom/ecd/EDTECD.html.

141. *Id.*

142. Charles Nelson & Anita Ramasastry, *Cybercrime*, Berkman Ctr. Internet & Soc'y (June 22, 2002), http://cyber.law.harvard.edu/studygroup/cybercrime.html.

individual to direct his computer to send messages in coordination with the rest of the attack.[143]

This characteristic of CDoS attacks is significant because it provides a popular legitimacy to larger-scale attacks that DDoS attacks—which involve taking unauthorized control of computers—could never have. A group of Internet activists calling themselves the "electrohippies collective" celebrated this distinction in 2001 after their own CDoS action against the World Trade Organization, noting:

> [DDoS] actions . . . are created by abusing the routers of web servers to generate huge numbers of incomplete requests. [A DDoS action is] [e]ffective, but the manner of the action, and its covert nature, mean that it does not have any particular democratic legitimacy.
>
> . . .
>
> So, the difference between the two actions is one of popular legitimacy versus individual will. The structure of the client-side distributed actions developed by the electrohippies means that there must be widespread support across a country, or continent in order to make the system work. *Our method has built within it the guarantee of democratic accountability. If people don't vote with their modems (rather than voting with their feet) the action would be an abject failure.*[144]

The attractiveness of CDoS as a means of protest may not be limited to individuals who agree with the particular goals of the electrohippies collective or other activist groups. The creativity and impact of these groups' methods have the potential to inspire any institutional thinkers who are looking for fresh approaches to activism.[145] The EDT even claims to have had an audience with Harvard's Berkman Center for Internet and Society in 1998 to explain its approach to online activism.[146] The most convincing proof of the attractiveness of CDoS is its employment by Anonymous in some of the group's recent high-profile activities.[147] The extent of Anonymous's connections to the EDT or

143. Kreimer, *supra* note 124, at 158.

144. DJNZ & the Action Tool Dev. Grp. of the Electrohippies Collective, *Client-Side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act?*, 34 LEONARDO 269, 270 (2001).

145. Writing in 2006, a professor of sociology specializing in globalization studies at Columbia University extolled the virtues of Internet activism such as the EDT employs as part of her overall discussion of new avenues for women's activism. Saskia Sassen, *Local Actors in Global Politics*, ISIS INT'L (Oct. 2, 2006), http://www.isiswomen.org/index.php?option=com_content&task=view&id=301&Itemid=191 ("There is the vastly expanded repertory of actions that can be taken when electronic activism is also an option.").

146. Posting of Ricardo Dominguez, rdom@thing.net, to post@nettime.free.xs2.net (Oct. 13, 1998, 2:32 AM), http://www.nettime.org/Lists-Archives/nettime-l-9810/msg00079.html.

147. *See supra* text accompanying notes 3-4.

the electrohippies collective is unclear, but the appeal to the individual participant is the same. After visiting an Anonymous chat room, one computer programmer became inspired to join the attack on PayPal because of similarities he saw to "the college sit-ins of the '70s" and Mahatma Gandhi's civil disobedience movement against British rule.[148]

1. A Tempting Comparison

The rhetoric of civil disobedience is useful for DoS attackers because it provides a framework within which to describe DoS as an inherently legitimate activity regardless of whether the law recognizes it as permissible. Civil disobedience, as a category of conduct, is defined by the conflict between a conduct's illegality on the one hand and its supposed moral legitimacy on the other.[149] Ronald Dworkin argued in 1985 that "civil disobedience has a legitimate if informal place in the political culture of [the American] community. Few Americans now either deplore or regret the civil rights and antiwar movements of the 1960s. . . . They concede that these acts did engage the collective moral sense of the community."[150] This moral legitimacy, which may exist independently of a protest's legal status, is ideal for proponents of DoS attacks in search of a convincing, nonlegal basis to oppose the operation of the criminal law as is. Admittedly, the metaphor of civil disobedience is enticing for more than this reason alone. One of the founders of the EDT, Stefan Wray, wrote a manifesto identifying his group's activities as part of a long tradition of civil disobedience beginning with Henry David Thoreau and continuing through the Civil Rights Movement and the Vietnam War, claiming:

> As hackers become politicized and as activists become computerized, we are going to see an increase in the number of cyber-activists who engage in what will become more widely known as Electronic Civil Disobedience. The same principals [sic] of traditional civil disobedience, like trespass and blockage, will still be applied, but more and more these acts will take place in electronic or digital form.[151]

Wray is not wrong to say that cybercrime has components that are analogous to the mechanics of sit-ins historically conducted as civil disobedience. Insofar as

148. Somini Sengupta, *For Suspected Hackers, a Sense of Social Protest*, N.Y. Times, July 26, 2011, at B1.

149. The literature on civil disobedience provides a number of definitions, *see infra* text accompanying notes 171, 176, but the tension between illegality and moral legitimacy is inherent to any formulation of the concept.

150. Bruce Ledewitz, *Perspectives on the Law of the American Sit-In*, 16 Whittier L. Rev. 499, 499 (1995) (quoting Ronald Dworkin, A Matter of Principle 105 (1985)).

151. Stefan Wray, *On Electronic Civil Disobedience*, Thing.net (Mar. 22, 1998), http://www.thing.net/~rdom/ecd/oecd.html (paper presented to the 1998 Socialist Scholars Conference).

unauthorized access and denial of service are analogs for the trespass and blockage that Wray mentions,[152] this "electronic civil disobedience" invokes techniques of protest used in periods of time that our political culture now recognizes as revered moments of social change.

Regardless, the intuitively obvious contrast between physical sit-ins and running programs from a computer terminal calls for pause in making such a comparison. A look at how one of the Civil Rights Movement's iconic grassroots efforts took place may elucidate the difference. On February 1, 1960, four black male students from North Carolina Agricultural and Technical College took seats reserved for whites only at the lunch counter of a Woolworth's department store in Greensboro, North Carolina.[153] Even though they had just bought school supplies from another counter at the store, the waitress told the students, "[W]e don't serve you here." The students replied, "We just beg to disagree with you. We've in fact already been served."[154] A dumbfounded waitress and an angry police officer with no excuse to retaliate could only watch as the students continued to occupy their seats peacefully.[155] Support began to grow for the student-led protest as soon as the local paper picked up the story. Student reinforcements crowded the aisles awaiting their turn to occupy the counter as others took part in nonviolent demonstrations outside.[156] Over the next few months, similar sit-ins began to take place in other North Carolina cities and other segregationist states.[157]

Trespass, blockage, and an overall strategy of attrition were the tactics that won the day in Greensboro. The black community's boycott of Greensboro department stores, coupled with lost sales as customers avoided the ongoing tension inside stores that the protestors occupied, eventually convinced store owners to change their policies.[158] The ignition of a new spark in the whole Civil Rights Movement,[159] however, had far more to do with the symbolic content of the protests. The president of CBS News at the time of the sit-ins recounted many years later that "for the first time, segregation came out of the closet. The

152. *See* Brenner, *supra* note 73, ¶¶ 81, 84.

153. Owen Edwards, *Courage in Greensboro*, Smithsonian, Feb. 2010, at 28, 28.

154. Howell Raines, My Soul Is Rested: Movement Days in the Deep South Remembered (1977) (quoting Franklin McCain), *as reprinted in* The Eyes on the Prize Civil Rights Reader 114, 115 (Clayborne Carson et al. eds., 1991) (internal quotation marks omitted).

155. *Id.*

156. Edwards, *supra* note 153, at 28-29.

157. *See id.*; Rebekah J. Kowal, *Staging the Greensboro Sit-Ins*, Drama Rev., Winter 2004, at 135, 136.

158. Kowal, *supra* note 157, at 136.

159. *See* Diedre B. Flowers, *The Launching of the Student Sit-In Movement: The Role of Black Women at Bennett College*, J. Afr. Am. Hist. 55 (2005).

conscience of the whole nation was touched."[160] Brave students who studied Gandhi's techniques and sent internal memoranda swearing off violence simply occupied space, prepared to be arrested.[161] Ultimately, it was the arrest of forty-five of them that motivated the black community to boycott Greensboro's department stores and to push the city toward change.[162]

After the EDT launched its FloodNet attack against government and financial targets in Mexico, Frankfurt, and the United States, a member of the group explained the logic behind the group's attacks: "FloodNet is a symbolic gesture. . . . Let's kick up the dust, that's what hacktivists are trying to do. And if we can kick up enough dust then we'll be able to get the media to look at us."[163] Some legal commentators and professionals have no problem using the term "civil disobedience" to describe the actions of groups like the EDT. One of the first articles to offer an overview of different types of cybercrime uses rhetoric like "perpetrators" and "crimes,"[164] but it also describes the EDT's activities against the Mexican government as "civil disobedience" in its primary text—not as a quotation from any attacker's description of the same.[165] One student commentator claims that the only difference between the civil rights protests of the 1960s and DoS attacks around the turn of the twenty-first century is the difference in setting: cyberspace instead of physical space.[166] The lawyer representing the man indicted for attacking the City of Santa Cruz recently agreed: "It is no different from occupying the Woolworth's lunch counter in the civil rights era."[167] While the word "hacktivism" at least signals to an audience that society must still sort out a measure of moral tension inherent in online ac-

160. Kowal, *supra* note 157, at 149.

161. Raines, *supra* note 154, at 116; Kowal, *supra* note 157, at 138, 147.

162. Kowal, *supra* note 157, at 136.

163. Warren, *supra* note 139.

164. Sinrod & Reilly, *supra* note 40, at 203.

165. *Id.* at 184; *see also* Giselle Fahimian, *How the IP Guerrillas Won: ®™ark, Adbusters, Negativland, and the "Bullying Back" of Creative Freedom and Social Commentary*, 2004 Stan. Tech. L. Rev. 1, ¶ 22 ("One popular form of electronic civil disobedience is accomplished through denial-of-service ('DoS') attacks, also referred to as virtual or electronic sit-ins.").

166. Andrew P. Lycans, Book Note, *Cyberdemons: Regulating a Truly World-Wide Web*, 101 Mich. L. Rev. 1925, 1934 (2003) (reviewing Stuart Biegel, Beyond Our Control?: Confronting the Limits of Our Legal System in the Age of Cyberspace (2001)). Much less egregious but still unsettling is the conclusion of a professor at NYU that groups like Anonymous provide "discrete micro-protest possibilities that aren't otherwise present," as if to suggest that its hacker members do not have other means of being "part of something greater." Gabriella Coleman, *Anonymous: From the Lulz to Collective Action*, OWNI.eu (May 10, 2011), http://www.owni.eu/2011/05/10/anonymous-from-the-lulz-to-collective-action.

167. Reilly, *supra* note 127.

tivity deemed illegal, using the phrase "civil disobedience" or going as far as invoking the Greensboro sit-ins seems to submit that the self-described activists are somehow already in the right and just waiting for their critics to catch up.[168]

2. The Moral Legacy of American Civil Disobedience

The difference in word choice is no small matter. A strong current in political philosophy views civil disobedience not just as having a place in democracy but as a problem that strikes at the heart of a democracy's moral legitimacy.[169] The struggle among scholars over the definition of civil disobedience is itself a testament to this fact.[170] To some, a simpler definition of the concept has its advantages. Framing civil disobedience as being composed only of two elements—illegality and the moral nature of arguments justifying the act—is logically coherent and, in one view, lacks any self-serving additions or qualifications that a group might use to justify its actions but exclude others.[171]

For Henry David Thoreau, a simple definition like this one might vindicate his calculation not to obey certain laws.[172] In his famous essay on civil disobedience, he elaborates on this concern with stories about his indignant refusal to pay taxes, culminating in a bold assertion about the relationship between government and the individual: "There will never be a really free and enlightened State, until the State comes to recognize the individual as a higher and independent power, from which all its own power and authority are derived, and treats him accordingly."[173] Of course, this principle does little to distinguish between

168. The reason for this presumption is that there is no real unified scholarly definition of the concept, *see infra* text accompanying note 170, and thus attempts to construct a modern concept of civil disobedience really seem to have value only to the extent that they describe those historical instances of illegal protest that we choose to revere now.

169. *See* Rawls, *supra* note 125, at 363 ("[The question of when the duty to oppose injustice trumps the duty to follow the law] involves the nature and limits of majority rule. For this reason the problem of civil disobedience is a crucial test case for any theory of the moral basis of democracy."); *see also* Elliot M. Zashin, Civil Disobedience and Democracy 67-69 (1972) (showing how the problem of civil disobedience raises the question of what constitutes the "consent" of the governed, which both Hobbes and Locke see as connected to a "quasi-moral obligation to obey the law in a political society").

170. There is no universally accepted definition of "civil disobedience" in the literature. Robert T. Hall, The Morality of Civil Disobedience 13 (1971).

171. For an example of an argument for this minimalist definition, see *id.* at 14-17.

172. *See* Henry David Thoreau, The Variorum: Civil Disobedience 45 (Walter Harding ed., 1967) ("It costs me less in every sense to incur the penalty of disobedience to the State than it would to obey. I should feel as if I were worth less in that case.").

173. *Id.* at 55.

rebellion and civil disobedience,[174] and Thoreau's readers are left to wonder if his rhetoric would be helpful at all to anyone resisting an audit by the Internal Revenue Service, much less working toward the desegregation of public accommodations.

A more persuasive construction of civil disobedience arises not out of indignant rants about taxes but from the writings of moral leaders who personally struggled for and achieved justice in volatile times, when pressure to abandon principled direct action came from many different directions.[175] John Rawls uses the following description of civil disobedience in his influential work *A Theory of Justice*: "a public, nonviolent, conscientious yet political act contrary to law usually done with the aim of bringing about a change in the law or policies of the government."[176] In his famous letter from a Birmingham jail, Dr. Martin Luther King, Jr., describes his philosophy of direct action in terms that support the principles that Rawls outlines.

First, the public character of acts of civil disobedience serves to illustrate the conviction behind the message that participants want to send.[177] Rawls writes that civil disobedience out in the open becomes "a form of address, an expression of profound and conscientious political conviction, [which] takes place in the public forum."[178] Similarly, Dr. King describes the desire for public demonstration as a desire to "create such a crisis and foster such a tension that a community which has constantly refused to negotiate is forced to confront the issue."[179] Crucially, this tension is personal. It arises from the presentation of protestors' physical bodies themselves "as a means of laying [their] case before the conscience of the local and the national community."[180]

---

174. *See* HALL, *supra* note 170, at 21.

175. Dr. Martin Luther King, Jr., used the term "direct action" to refer to organized physical activism that created constructive tension in a community without resorting to violence. *See* Letter from Martin Luther King, Jr., to Alabama Clergymen (Apr. 16, 1963) [hereinafter King Letter], *available at* http://www.africa.upenn.edu/Articles_Gen/Letter_Birmingham.html ("I have tried to stand between these two forces, saying that we need emulate neither the 'do nothingism' of the complacent nor the hatred and despair of the black nationalist.").

176. RAWLS, *supra* note 125, at 364 (paraphrasing H.A. Bedau, *On Civil Disobedience*, 58 J. PHIL. 653, 661 (1961)).

177. In Hall's articulation of a minimalist definition, he wrongly asserts that a definition requiring acts to be public would deny "any possible moral justifiability" to nonpublic criminal acts. *See* HALL, *supra* note 170, at 16. While it is true that such acts would not be considered civil disobedience under the Rawlsian definition, Rawls leaves open the possibility that they could be justified on other grounds.

178. RAWLS, *supra* note 125, at 366.

179. King Letter, *supra* note 175.

180. *Id.* Valorizing the willingness to accept punishment makes sense only in the context of a democracy in which public deliberation is possible in the first place, however. One scholar points out that those who sheltered Jews in Nazi Germany

Second, the requirement of nonviolence in Rawls's definition is especially important.[181] This requirement is not based on moral qualms with harming others but rather with protecting the overall persuasiveness of protest. Violence quickly crowds out a deliberative resolution of conflict by both deemphasizing the protestor's logic and foreclosing an audience's willingness to adhere to an argument.[182] Nonviolent acceptance of punishment, in contrast, leaves space for the argumentative strength of protest to operate and reaffirms that the protestors identify as part of the same community as the opposition whom they seek to persuade.[183] Justice Fortas, commenting on his dissent to an opinion upholding an injunction against Dr. King's march in Birmingham, described Dr. King's acceptance of criminal liability for ignoring the injunction, without complaint, as "action in the great tradition of social protest in a democratic society where all citizens, including protesters, are subject to the rule of law."[184]

Respect for the rule of law is the key element that an oversimplified definition of civil disobedience lacks. As Justice Fortas suggests, this respect is embodied in the restraint shown by those who physically occupy public space yet project only the force of their arguments. The health of a democracy depends fundamentally on the public's faith that structures of governance prevent the need for extrajudicial violence in resolving conflict.[185] Unfortunately, deciding

---

would certainly not have been required to publicize their actions for their disobedience to have been considered morally justified. *See* Kent Greenawalt, *A Contextual Approach to Disobedience*, 70 COLUM. L. REV. 48, 70 (1970).

181. *See* RAWLS, *supra* note 125, at 366.

182. *Id.* ("[Civil disobedience] tries to avoid the use of violence, especially against persons . . . because it is a final expression of one's case."). A leading theory of audience adherence to argumentation in speech communication literature confirms this direct tradeoff: "The use of argumentation implies that one has renounced resorting to force alone, that value is attached to gaining the adherence of one's interlocutor by means of reasoned persuasion. . . . Recourse to argumentation assumes the establishment of a community of minds . . . ." CH. PERELMAN & L. OLBRECHS-TYTECA, THE NEW RHETORIC: A TREATISE ON ARGUMENTATION 55 (John Wilkinson & Purcell Weaver trans., Univ. of Notre Dame Press 1969) (1958).

183. French philosopher E. Dupréel describes each logical justification used in an argument as "a moderating act, a step toward greater communion of heart and mind." PERELMAN & OLBRECHS-TYTECA, *supra* note 182, at 55.

184. ABE FORTAS, CONCERNING DISSENT AND CIVIL DISOBEDIENCE 35 (1968). The opinion upholding the injunction that Dr. King ignored was issued in *Walker v. Birmingham*, 388 U.S. 307 (1967).

185. Public faith that political institutions are able to accommodate social change is a necessary condition for any regime's stability, democratic or otherwise. *See* SAMUEL P. HUNTINGTON, POLITICAL ORDER IN CHANGING SOCIETIES 1-5 (1968). In a consolidated democracy, civil society and political society earn the right to mediate this popular sentiment by embedding opposition to the state in a spirit of

whether the actions of the State or an individual dissenter are truer to the rule of law is difficult. Such a decision is dependent upon speculation about what *will* be good for democracy once some yet-unmoved obstacle has vanished, revealing uncharted political space. Protestors' open willingness to accept the penalty for violating the law invites onlookers to decide for themselves how best to respect the rule of law moving forward: whether to accept the application of criminal law as a final resolution of the protest or to join in a bold new vision for the community.[186]

3. The True Nature of DoS Attacks

DoS attacks have no role to play in this sacred tradition of civil disobedience. Hidden behind individual computer screens, even well-meaning dissidents who voluntarily pit their computing resources against the most notorious targets are at best participating in a shallow gesture. The relative or actual anonymity that participants enjoy in large-scale DoS attacks[187] depersonalizes their message, requires much less commitment,[188] and thus evidences much less con-

---

constitutionalism and respect for the rule of law. *See* JUAN J. LINZ & ALFRED STEPAN, PROBLEMS OF DEMOCRATIC TRANSITION AND CONSOLIDATION 7-10 (1996).

186. *See* King Letter, *supra* note 175 ("[A]n individual who breaks a law that conscience tells him is unjust, and who willingly accepts the penalty of imprisonment in order to arouse the conscience of the community over its injustice, is in reality expressing the highest respect for law."). Since in its purest form this act requires no legal justification to be morally proper—and in fact may have less moral force if a protester attempts to justify the act on legal grounds—this Note will not address civil disobedience as an affirmative defense to crimes or the distinction between "direct" and "indirect" civil disobedience. For that discussion, see, for example, William P. Quigley, *The Necessity Defense in Civil Disobedience Cases: Bring in the Jury*, 38 NEW ENG. L. REV. 3 (2003).

187. *See supra* text accompanying note 34. It is noteworthy that federal law enforcement officials were able to track several suspected participants in Anonymous's 2010 DoS attack on PayPal who either did not know how to mask their online identities or deliberately chose not to do so. *See* Sengupta, *supra* note 148, at B1. In response to the arrests of these individuals, Anonymous boldly proclaimed in an open letter to law enforcement, "Your threats to arrest us are meaningless to us as you cannot arrest an idea." *Id.* Presumably, however, the pages of instructions that Anonymous provided to new members on how to mask their online identities made this proclamation more confident. *See id.* In September 2011, Anonymous announced that it was developing a new DDoS tool to replace LOIC and cited the volume of arrests of members using LOIC as a reason for the switch. *See* Damon Poeter, *Anonymous To Retire Low Orbit Ion Cannon?*, PC MAG. (Aug. 2, 2011), http://www.pcmag.com/article2/0,2817,2390341,00.asp#fbid=ngA4eBICbTm.

188. *See infra* note 211. The fact that a person can only be in one physical space at a time implies that a choice to appear somewhere in protest represents a commitment unshared by someone who can simultaneously and anonymously participate in a number of DoS attacks from the comfort of home.

viction than a public act of disobedience in which an individual must take responsibility for her actions and face possible criminal punishment.[189] Individuals protesting from home may feel just as strongly as public protestors, but the community receiving their message will generally have no way of measuring that conviction other than reading scattered essays and comments online and measuring server downtime or bandwidth used by traffic.

The damage that DoS attacks cause, while not rising to the level of physical violence, necessarily threatens the economic and social liberties of others and thus disqualifies such attacks from being considered civil disobedience.[190] These threats break down the deliberative process generated by civil disobedience, in which protestors rely only on the strength of their arguments and identify as part of the same community as their audience. First, the harm caused by a DoS attack drowns out the logical persuasiveness of hacktivists' arguments. Victims of the collateral damage associated with attacks would likely attest to the absence of any meaningful purpose behind their losses.[191] Second, DoS attacks negate the potential for a more robust political dialogue about the issues motivating the hacktivists who perpetrate these attacks. By presuming the opposition's unwillingness to negotiate, the DoS attacker presents no community-affirming option for resolving conflict that allows the target or the legal apparatus to respond to the presence of the protestor by standing down.[192] It is

189. *See* Greenawalt, *supra* note 180, at 70 (arguing that willingness to accept punishment ensures that protest is more convincing at three junctures: (1) Such willingness satisfies those who are incidentally harmed by protest that the protestors face worse harm; (2) it forces individual protestors to act only on strong convictions; and (3) it suggests to the audience that the magnitude of the injustice under scrutiny is great).

190. *See* RAWLS, *supra* note 125, at 366 ("Indeed, any interference with the civil liberties of others tends to obscure the civilly disobedient quality of one's act."). In contrast, the sit-ins in Greensboro led to economic losses for businesses not as an inevitable consequence of direct action but as a result of the intervening sentiments of community members of different races who responded to the tension of the protest in different ways. *See supra* text accompanying note 158.

191. *See supra* text accompanying note 44.

192. The only true test for a protestor's respect for the rule of law is when his mode of protest actually runs afoul of the law. Anonymous's involvement in the Fall 2011 "Occupy" protests demonstrates this point. At first, the group's focus was to enable a new movement of nonviolent physical protest in spaces that would accommodate it. The group conducted a successful social media campaign in September 2011 to focus national attention on the original Occupy Wall Street campaign in New York City's Zuccotti Park. Saki Knafo, *Occupy Wall Street and Anonymous: Turning a Fledgling Movement into a Meme*, HUFFINGTON POST (Oct. 20, 2011), http://www.huffingtonpost.com/2011/10/20/occupy-wall-street-anonymous-connection_n_1021665.html. Months later, when the Mayor of Toronto called for the city to evict "occupiers" who lacked a permit to remain in a public park, Anonymous threatened to deny service to the city's website instead of drawing on its social media prowess to organize a grassroots response. *See* Alyshah Hasham,

no defense that, historically, higher-profile electronic "sit-ins" against the Frankfurt Stock Exchange, the WTO, the IMF, and the World Bank have only slowed down servers at most and not seriously denied access.[193] The visibility of these attacks depends on the level of disruption they cause, and to the extent that the success of these attacks depends on their visibility, so too does their success.

Once the mechanics and effects of DoS attacks are in full relief, the moral status of such attacks is clear. In a paper that EDT founder Stefan Wray presented to the 1998 Socialist Scholars Conference, he quoted Thoreau's assertion that the best kind of government "governs not at all" and implied that Thoreau's tradition of civil disobedience is the one that became "woven into the fabric of dissent in this country."[194] Given the paltry respect that DoS attacks demonstrate for established order, it is apparent that an advocate like Wray *must* rely on a strategy of protest no more nuanced than Thoreau's in justifying the means that his group employs to protest its opponents' policies. The "civil disobedience" that Thoreau exercised when refusing to pay taxes as a war protest presents an image that, if accepted as a legitimate form of political protest, would appear to give a group with any disagreement with the powers-that-be a justification for the stubborn, unlawful resistance of its choice. The reason is that Thoreau's approach to citizenship, embodied in any coherent justification for DoS attacks, is only concerned with the rule of law so long as democratic institutions accommodate the citizen's private moral agenda.[195]

IV. The Limits of the Generative Internet

The Internet is a social force not naturally concerned with the rule of law—it is a "generative" construct that empowers individuals to create and manipulate information in a way that defies previously understood limits.[196] To the

'*Anonymous*' *Threat Doesn't Faze Mayor Ford*, Toronto Star (Nov. 13, 2011), http://www.thestar.com/news/article/1086197--hacker-group-anonymous-threatens-cyber-attack-if-city-evicts-occupy-toronto?bn=1 ("You have said that by next week the occupiers shall be removed. And we say by next week if you do not change your mind, you shall be removed from the Internet.").

193. *See* Kreimer, *supra* note 124, at 159-60.

194. Wray, *supra* note 151.

195. Thoreau is crystal clear about this distinction: "It is not desirable to cultivate a respect for the law, so much as for the right. The only obligation which I have a right to assume is to do at any time what I think right." Thoreau, *supra* note 172, at 33.

196. *See* Jonathan L. Zittrain, *The Generative Internet*, 119 Harv. L. Rev. 1974, 1981 (2006) ("Generativity is a function of a technology's capacity for leverage across a range of tasks, adaptability to a range of different tasks, ease of mastery, and accessibility.").

extent that this construct changes the shape of our social order,[197] the legal and moral issues raised by DoS attacks inform a larger debate about the meaning of cyberspace. Cyberspace is obviously not the same as physical place, but scholars disagree over the relevant differences.[198] Courts are unable to predict all of the ways in which the Internet could be used, and thus they lack the capacity to sort out all of the possible differences between cyberspace and physical space prior to applying the law in new ways. New technological phenomena like DoS attacks help to reveal these differences by demonstrating the unique kinds of actions that are possible in cyberspace.[199]

This Part proposes that the DoS phenomenon provides a useful standpoint from which to understand the unique challenges that cyberspace poses for legal practitioners. First, the fact that prosecutors must stretch statutory definitions of cybercrime to their limits to prosecute DoS attacks suggests that legislatures should be more focused on the specific harms that evolving technology could bring rather than the ways in which new uses of technology fit into preexisting categories of conduct. Second, existing justifications for DoS attacks attempt to infuse cyberspace with some of the most sacred notions of community formation available in physical space, thereby raising the question of whether cyberspace is an equally adequate staging ground for democratic community. Together, these two issues suggest that analysis of the differences between physical space and cyberspace is most valuable when it clarifies the essential democratic values that are inherent in laws governing physical space before making judgments about how actions in cyberspace protect or threaten those values.

A. Knowing What To Punish

Legislators cannot successfully outlaw computer crimes by attempting to draw property lines where they cannot be drawn. As long as the definitions of federal and state cybercrimes continue to rely primarily on the concept of "authorization," prosecutors and courts will have too much discretion to identify offenses. Moreover, the prosecution of offenses under these statutes will not send a convincing signal that the conduct involved is actually wrong. The criminal law plays an important expressive role in defining acceptable conduct for American society.[200] By making it clear that DoS attacks are not fundamentally of the same nature as lawful computer use, an ideal statute prevents the offend-

197. *See* YOCHAI BENKLER, THE WEALTH OF NETWORKS 30 (2006).

198. *See* Julie E. Cohen, *Cyberspace as/and Space*, 107 COLUM. L. REV. 210 (2007) (surveying various theories of the interaction between cyberspace and the concept of "place" and the complex web of functionalist, postmodern, and other perspectives underlying those theories).

199. Cyberlaw appears to be mired in a perpetual state of "catching up." *See supra* text accompanying note 89.

200. *See supra* note 119 and accompanying text.

er from arguing that her use would be understood as prosocial but for the predictable refusal of authorization from her morally blameworthy target.

Those states that have proscribed actions accompanied by a specific intent to deny Internet service are at the head of the curve because such prohibitions do not force prosecutors and judges to rely primarily on a broadly defined actus reus as the core element of the crime. New categories of criminal conduct on the Internet have the potential to sprout up anywhere that technology can be used in a novel way to do harm.[201] When new harms arise from the use of otherwise benign tools, it stands to reason that a malicious intent will be the only element of an electronic act that distinguishes it as unlawful.[202] A specific intent element cuts through the legal and moral ambiguity of offenses predicated solely upon a lack of authorization and gives prosecutors and courts the means to punish the creation of harm without the discretion to overreach.[203]

While prohibitions of harm done on the Internet should be specific, adapting to new circumstances requires our notions of what may qualify as harm to be broad. Although the CFAA's prohibition of actions that intentionally cause damage is useful for prosecuting felonies that cause high-dollar losses, the networked nature of the Internet means that even large tangible losses can be distributed across a wide variety of targets who may each individually experience only very small losses.[204] Congress should also be mindful of the serious threats to intangible values—such as the promotion of free speech—that cyberattacks may pose to targeted entities even if those entities cannot tally up enough of a dollar loss to get the Department of Justice's attention.[205]

---

201. *See supra* text accompanying note 68; *see also supra* note 135.

202. The intent to undertake a harmful act may not be what makes the act harmful, but the mens rea element may be necessary to distinguish logically between harmful and harmless actions when no other concept is available to distinguish them.

203. To dispose of residual vagueness problems with the word "authorization" entirely, a jurisdiction could implement a statute proscribing all actions accompanied by an intent to deny service but allow express authorization by server owners to serve as an affirmative defense. Pennsylvania's DoS-specific statute omits discussion of "authorization," but it fails to provide an affirmative defense that could shield computer security practitioners from criminal liability. *See* 18 Pa. Cons. Stat. § 7612 (2011). While express authorization is completely unworkable as an interpretation of "authorization" in broader cybercrime statutes, *see supra* text accompanying note 81, it seems practical to require computer security practitioners to secure express authorization before using DoS attacks to test networks.

204. *See* Katyal, *supra* note 68, at 1090-91.

205. It is conceivable that, given limited resources, the Department of Justice would only seek to prosecute felony violations of 18 U.S.C. § 1030(a)(5)(A). Damage of $5000 or more to a target is the basic trigger for felony liability. *See supra* note 101.

B. *Making Cyberspace Safe for Democracy in a Physical World*

The difference between physical place and cyberspace is also significant when it comes to our intuitions about democratic traditions like political protest. Jonathan Zittrain of the Berkman Center explains why:

> In front of a building, you get to play your First Amendment card all the way to the door before you are dragged away . . . . In cyberspace, you don't have clear public byways intersecting private spaces, so there is no place to camp out and play your First Amendment card. If you try to deny service to someone else, by whatever means you use, you could be in pretty big trouble.[206]

As Zittrain suggests, fast and loose comparisons between the Internet and the physical world are at best a source of legal confusion. At worst, they are also dangerous inasmuch as they threaten awareness of the true constituent elements of community and democracy. Some courts have been cautious about transplanting concepts directly from physical place to cyberspace, which is encouraging.[207] Many courts, though, have found cyberspace metaphors to be expedient, seemingly principled grounds for decisions.[208] A presumption of caution in transplanting legal concepts from physical place to cyberspace does not seem to have taken hold yet in the Supreme Court's protection of free speech on the Internet.[209] Current First Amendment doctrine is itself well prepared to deem unprotected even expressive actions that cause identifiable harm,[210] but the normative view of the Internet as a space primarily serving free expression threatens to obscure this principle.[211]

---

206. Patti Hartigan, *They Call It Hacktivism*, Bos. Globe, Jan. 24, 1999, at F5 (quoting Jonathan Zittrain, Faculty Co-Dir., Harvard Univ. Berkman Ctr. for Internet & Soc'y).

207. *See, e.g.*, Intel Corp. v. Hamidi, 71 P.3d 296, 309 (Cal. 2003).

208. Mark A. Lemley, *Place and Cyberspace*, 91 Calif. L. Rev. 521, 527-29 (2003) (observing that courts are often willing to apply "inviolability" rules from real property to information online even though such protections have never historically existed).

209. Indeed, a prominent Supreme Court case striking down restrictions on free speech over the Internet relies on the *opposite* presumption. *See* Reno v. ACLU, 521 U.S. 844, 885 (1997) ("The dramatic expansion of this new marketplace of ideas [the Internet] . . . continues to be phenomenal. As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship.").

210. *See supra* Section III.A.

211. Anonymity, for example, may encourage the free flow of information, especially from more hesitant sources such as political dissidents under repressive regimes.

Some concepts used to organize physical space are useful in cyberspace. For example, it is true that a hacker intrudes into a clearly private space when he gains unauthorized access to a system. This fact does not, however, provide a line designating where private cyberspace ends and public cyberspace begins.[212] Not only is there no line, but there is no gray area or middle ground between the two spaces that would be comparable to public accommodations in the physical world, where sit-ins sought to bring attention to the public character of certain spaces that are technically private.[213] The eager online activist looking to bring an argument to a public place where all can take notice need only post her own content to her personal blog.

The absence of distinctly public space on the Internet makes it more difficult for people to use cyberspace as an alternative site for forming strong communities. Carol Rose's *The Comedy of the Commons*[214] demonstrates how even nonpolitical recreational activity in physical spaces is particularly important for the formation of a democratic community—political protest in those spaces would presumably have similar value toward that end.[215] Zittrain's description of the Internet as "generative" might provide some guidance as to how Internet users could form community identity: acting in the aggregate to express prefe-

---

See Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1642 (1995). Demanding unfettered anonymity in the interest of free expression, however, ignores serious threats to civility and accountability for the verifiability of information. *See id.* at 1645.

212. Ignoring the difficulties that Kerr's definition of "authorization" poses for statutes seeking to criminalize actions like DoS attacks that do not require passing security barriers, *see supra* text accompanying note 81; Kerr, *supra* note 67, at 1600, this definition would appear to clear up the public/private cyberspace problem on a technical basis. *But see* Lemley, *supra* note 208, at 537-39 (explaining that even a clear private right in cyberspace could be heavily qualified in ways similar to those in which a fee simple interest is qualified in physical space).

213. The absence of a concept of physical proximity on the Internet means that a move toward privatizing cyberspace has disproportionately negative effects on the public character of cyberspace. *See* Lemley, *supra* note 208, at 536-37. *But see* Kreimer, *supra* note 124, at 152 (observing that search engine result pages and similar domain names function as "informational neighborhood[s]" in which activists can position their web pages "near" the object of their protest).

214. Carol Rose, *The Comedy of the Commons: Custom, Commerce, and Inherently Public Property*, 53 U. CHI. L. REV. 711 (1986) (contesting the notion that public property always creates a "tragedy" of the commons and describing a "comedy" of the commons defined by community interactions that produce value with potentially increasing returns to scale).

215. *See id.* at 778 (1986) (identifying recent hints that "property used for political speech has come to be viewed as inherently public").

rences for some content and not for other content.[216] Nevertheless, the generative quality of the Internet is distinctly different than Rose's comedy in that a generative space prioritizes individual freedom over community formation. Zittrain describes generativity as "a function of a technology's capacity for leverage across a range of tasks, adaptability to a range of different tasks, ease of mastery, and accessibility."[217] While each of these attributes is potentially conducive to the formation of communities, none of them is inherently about shared experiences.

Conversely, in the analysis of British customary doctrine upon which Rose builds her comedy, she describes how customary public activities are valuable not just for their interactive quality but also for their capacity to anchor community identity in particular public places.[218] Cerebrally, it makes sense to describe the aggregate excitement of individuals participating in a maypole dance as a product of "increasing returns to scale," but, viscerally, this scene is more about the fact that there was one source of excitement and that it was shared by a defined community.[219] The Internet is unique in that an untold number of individual interactions can seemingly merge to form a cloud of community activity. For the individual person, however, the experience is inherently isolated. The rapid pinging of information back and forth between individuals across a distance is revolutionary, but it cannot provide an alternative to the emotional basis for relationship formation that occurs when individuals sharing public spaces engage in immediate mutual recognition.[220] Such mutual

216. *See* Zittrain, *supra* note 196, at 1994 (noting how quickly the "generative grid" can channel public preferences, vaulting certain applications and services to a high level of success and popularity very soon after implementation).

217. *Id.* at 1981.

218. *See* Rose, *supra* note 214, at 759 ("[T]he location of customary public activities may matter a great deal, not because it would be impossible to conduct these activities elsewhere, but because to relocate would rupture the continuity of the community's experience and diminish the significance of the activity itself. The community's custom signals its emotional investment in a place. Moreover, the custom communicates this information to everyone—including the property's owner who, under British customary law, acquiesced in that investment.").

219. *See id.* at 767-68 ("Activities of this sort may have value precisely because they reinforce the solidarity and fellow-feeling of the whole community; thus the more members of the community who participate, even if only as observers, the better for all.").

220. *See* Robert D. Putnam, *Bowling Alone: America's Declining Social Capital*, J. Democracy, Jan. 1995, at 65, 75, *available at* http://www.unbc.ca/assets/politicalscience/class_materials/200905/bowling_alone.pdf (suggesting that the "technological transformation of leisure" could disrupt opportunities for social-capital formation by offering the individual fuller satisfaction of her tastes "at the cost of the positive social externalities associated with more primitive forms of entertainment"). One commentator writing on this subject acknowledges that online interaction could enhance community in physical space. Ultimately,

recognition is essential to the deliberative-democratic dialectic[221] that engendered one of this nation's most revered moments of change.

Trying to force-fit a concept of civil disobedience into cyberspace inspires an intuitive response: Physical protest is personal, server downtime is not.[222] In a DoS attack, no one will be challenged by the emotionally charged sight of physical "bodies . . . laying [the protestors'] case before [the community's] conscience."[223] Even so, server downtime can cause real damage to the target's self-expression or economic well-being, especially when the targeted entity relies on the Internet to convey its message or survive financially. DoS attacks are thus the perfect example of why commentators should be careful to deconstruct loaded concepts like "protest" or "free speech" before celebrating the Internet's openness.[224] These attacks exploit that openness[225] through actions that are antithetical to effective political protest like civil disobedience: While shying

however, she agrees with Putnam as to the irreplaceability of physical interaction in building social capital. She presents President Barack Obama's run for office as an example of how the Internet served civic engagement insofar as it enabled latent physical communities to organize for the election. *See* Nicol Turner-Lee, *The Challenge of Increasing Civic Engagement in the Digital Age*, 63 FED. COMM. L.J. 19, 24, 31 (2010).

221. "Dialectic" here refers specifically to the type of personal argumentative exchange that begins when a protestor expresses her message with conviction during effective civil disobedience. *See supra* text accompanying notes 182-183.

222. Putting technology between the attacker and the target reduces the extent to which the attacker must personally invest in the violence. *See supra* note 189. As a result, the attack fails to recreate the human experience accompanying more palpable and directly confrontational forms of violence. *Cf.* Jane Mayer, *The Predator War*, NEW YORKER, Oct. 26, 2009, at 36, 40, *available at* http://archives.newyorker.com/?i=2009-10-26#folio=036 (warning that Predator drone strikes in the War on Terror are "seductive" in part because they hide the human cost of violence (quoting Peter W. Singer) (internal quotation marks omitted)).

223. King Letter, *supra* note 175.

224. Cass Sunstein, for example, can only explain why an "electronic town meeting" fails to live up to the founders' aspirations once he has established why a deliberative-democracy model is superior to a marketplace-of-ideas model in understanding the importance of the First Amendment. *See* Cass R. Sunstein, *The First Amendment in Cyberspace*, 104 YALE L.J. 1757, 1786-87 (1995). *See generally* Cass R. Sunstein, *Beyond the Republican Revival*, 97 YALE L.J. 1539 (1988) (identifying key aspects of a deliberative view of democracy, such as the desire for consensus and the normative focus on evaluating political practices, which are inherent in republicanism and serve to distinguish such a view from a perspective of free speech that employs marketplace metaphors).

225. Zittrain acknowledges that it is the very generativity of the Internet that creates the potential for viruses and other malicious interference with the rights of others. *See* Zittrain, *supra* note 196, at 1995-96.

away from a real public forum, attackers manage to reach through the world's broadband cables to commit violence against targets silently.

When the waitress at the Greensboro Woolworth's lunch counter claimed that blacks were not welcome "here," she invoked the idea of place in a way that was highly dissonant to the students. "Here" was a department store that served blacks at one counter but not another. "Here" was also a city in the New South that some considered to be "free of old prejudices and ideally prepared to lead the region toward new levels of prosperity and enlightenment."[226] The contradictions inherent in the segregation of that lunch counter were apparent only because of the ways that the community had already begun to integrate in physical space. The Civil Rights Movement relied greatly on the television to project images of nonviolent resistance to places far from Greensboro,[227] but those images would not have been compelling if nonviolent tactics had not first been potent in the place where they were carried out. In the words of one student organizer, "[P]robably the most powerful weapon that people have literally no defense for is love, kindness."[228] And while one can speak of such a weapon over a broadband connection, the weapon is most effective when used in person.

Conclusion

This Note has argued that DoS attacks are an underappreciated threat to speech, infrastructure, and the economy and that they serve as an example of the evolving means by which Internet users can employ otherwise benign technologies to do harm. While the categories of conduct proscribed by cybercrime statutes can be stretched to include DoS attacks, the most coherent legal prohibitions on such attacks employ language criminalizing actions taken with the intent to effectuate denial of service. This focus on the harm itself as the anchor of legal regulation is important in a rapidly evolving cyberspace because it forces legislators and courts to identify core values in need of protection and the harms that could threaten them. The DoS phenomenon also demonstrates the danger of subordinating concerns about the quality of speech to the protection of the generative character of the Internet, as it is that character that could threaten a more fundamental, deliberative tradition of expression that enhances democracy in the physical world.

226. Flowers, *supra* note 159, at 53 (quoting William H. Chafe, Civilities and Civil Rights: Greensboro, North Carolina, and the Struggle for Freedom 5 (1980)) (internal quotation marks omitted).

227. *See* Theodore Carter Delaney, *The Sit-In Demonstrations in Historic Perspective*, 87 N.C. Hist. Rev. 431, 437-38 (2010).

228. Raines, *supra* note 154, at 116.