Roger Williams University Law Review

Volume 28
Issue 1 *Vol. 28 No. 1 Winter 2023*

Article 5

Winter 2023

Cyber Sit-Ins: Bringing Protest Online by Modernizing the Computer Fraud and Abuse Act

Blair V. Robinson
Juris Doctorate candidate, Roger Williams University School of Law

Cyber Sit-Ins: Bringing Protest Online by Modernizing the Computer Fraud and Abuse Act

Blair V. Robinson*

"Hello, leaders of Scientology. We are Anonymous. . . . We do not forgive. We do not forget. Expect us."[1]

INTRODUCTION

These self-consciously cryptic words marked the beginning of Project Chanology, the first mass political action by the infamous hacktivist organization, Anonymous.[2] Project Chanology responded to what members of Anonymous saw as intolerable censorship by Scientology.[3] For example, the Church had conducted aggressive litigation against media outlets that shared a leaked video of Tom Cruise praising the Church and appearing manic.[4] The protest spanned several days in January of 2008 and vast distances as members of Anonymous demonstrated outside of Scientology

* Blair Victoria Robinson, J.D Candidate, Roger Williams University School of Law, 2023 & M.A. in Cybersecurity Candidate, Roger Williams School of Justice Studies, 2023.

1. @Church0fScientology, *Message to Scientology,* YOUTUBE (Jan. 21, 2008), https://www.youtube.com/watch?v=JCbKv9yiLiQ.

2. The Bryant Park Project, *'Anonymous' Takes on Scientology*, NPR, at 1:20, (Feb. 11, 2008), https://www.npr.org/templates/story/story.php?storyId=18873367 [https://perma.cc/EBT9-LPLN].

3. *Id.* at 1:58.

4. Marcus Baram, *Scientology's Anonymous Critics: Who Are They?*, ABC NEWS (Mar. 25, 2008), https://abcnews.go.com/US/story?id=4513883&page=1 [https://perma.cc/GA2F-TMQD].

buildings nationwide.[5] These demonstrations also saw the group's first use of Guy Fawkes masks, which quickly became their trademark.[6] Most importantly, this protest brought a crucial innovation to the organized civil disobedience mainstream: Anonymous took their march digital.[7]

Hundreds of activists used a technique called Distributed Denial of Service (DDoS) to overwhelm Scientology's websites as their fellow protestors swarmed the Church's buildings.[8] DDoS is a hacking technique that works by flooding a web server with web traffic, just as a traditional protest works by flooding the street with foot traffic.

This Comment argues that DDoS[9] actions are, at times, a legitimate protest tool. Unfortunately, the Computer Fraud and Abuse Act (CFAA) currently criminalizes all DDoS activities, regardless of free speech considerations.[10] Therefore, Congress should amend the CFAA to recognize an affirmative defense based on finding minimal automation, minimal damage, and a published political purpose. This change would acknowledge the long tradition of American protest and Constitutional penumbra that protects political speech in American law to bring that tradition online.

In Part I, this Comment explains foundational terms and reviews the history of online protest. Part II examines the requirements of a prosecution under the CFAA. Part III argues that a "free-speech" affirmative defense should be available in these cases.

I. RELEVANT BACKGROUND

A. *What is Hacking?*

The original hackers used the term "hacking" to describe their hobbyist, do-it-yourself approach to exploring emerging

5. *Id.*
6. *Id.*
7. *See id.*
8. *Id.*
9. As well as DDoS's closely related cousin, the Denial of Service (DoS) action. Unlike DDoS, which relies on several machines powering the attack, DoS uses a single machine to overwhelm the target.
10. *See, e.g.*, United States v. Golightley, 840 F. App'x 319 (10th Cir. 2020); United States v. Gottesfeld, 18 F.4th 1 (1st Cir. 2021).

technologies.[11] The original hackers were not hardened criminals; instead, they were curious geeks who used their knowledge to push the boundaries of early computer science. Unfortunately, their ability to compromise these arcane systems led to trouble with law enforcement. Early hacker[12] Kevin Mitnick, for example, was infamously held in solitary confinement due to fears that he could cause a nuclear strike by whistling into a telephone.[13]

Today, people use "hacking" as a general catch-all word to describe anything related to compromising a computer system's security. Hacking, as people use it today, could apply to specific techniques, as in, "they used a SQL-injection hack."[14] Hacking could also refer to what is known as "advanced persistent threat" operations, which is what experts mean when they say things like "Russia is hacking Ukraine."[15] To add to the confusion, hacking does not even need to target a computer. Humans are generally the weakest link in a secure system, and many of the most successful hacks rely on "social engineering" techniques such as

11. Noah C.N Hampson, *Hacktivism: A New Breed of Protest In A Networked World*, 35 B.C. INT'L & COMP. L REV. 511, 515–16 (2012) ("But the term hacking has not always been used to describe the conduct of a cybercriminal. It originally described an innovative use of technology to solve a problem.").

12. And phone "phreaker." "Phreaking" refers to the art of manipulating analog phone switching. Lhoyd Ragay, *The Fascinating History of Phreaking: An Old School Hack for Making Free Phone Calls*, A LITTLE BIT HUMAN (Apr. 4, 2022), https://www.alittlebithuman.com/history-of-phreaking-001/ [https://perma.cc/7ZFJ-6G7G].

13. Chris Snyder, *World famous hacker explains what it was like being locked up in solitary confinement*, BUS. INSIDER, (May 15, 2017, 10:08 AM), https://www.businessinsider.com/heres-what-its-like-being-locked-up-in-solitary-confinement-kevin-mitnick-jail-prison-hacker-hacking-2017-5 [https://perma.cc/F7W9-RKRX]. Mitnick could not, in fact, whistle a nuclear strike—his range topped out around the free-long-distance-phone-call octave.

14. This is a technique that compromises databases by tricking the server into running malicious commands that the attacker enters in place of legitimate user input. Jesse L. Noa, *They Did It for the Lulz: Future Policy Considerations in the Wake of Lulz Security and Other Hacker Groups' Attacks on Stored Private Customer Data*, 1 J.L. & CYBER WARFARE 155, 168–69 (2012) ("A SQL injection is a simple intrusion method that tricks a website and database into running codes that are not intended by the owner of the website/database.").

15. *See, e.g.*, Aaron Schaffer, *Ukraine Suffered Two Cyberattacks in the Lead Up to Russia's Invasion*, WASH. POST (March 30, 2022, 8:02 AM), https://www.washingtonpost.com/politics/2022/03/30/ukraine-suffered-two-cyberattacks-lead-up-russia-invasion/ [https://perma.cc/3XEX-BS8C].

impersonating I.T. personnel to solicit passwords.[16] Moreover, real-life hacking is nothing like the keyboard mashing duels on television. A real-life operation could spend several months conducting physical and network reconnaissance and slowly escalating privileges, making it difficult to parse the difference between hacking and conspiracy, or even how many distinct hacks occurred.[17]

This Comment focuses on one specific hacking technique to avoid ambiguity: the Distributed Denial of Service attack, more commonly known as DDoS.

B. *Distributed Denial of Service (DDoS)*

DDoS works because computers cannot perform multiple operations at once.[18] Computers generally operate so quickly that humans perceive everything on the screen as happening simultaneously, but every computer has limited resources.[19] DDoS works by making many "nonetheless legitimate demands upon the target's computational resources."[20]

Imagine a web server as the host at a diner. Her job is to seat each person who walks through the door, and she can only sit one customer at a time. Usually, that is not an issue. However, one group of customers leaves and re-enters the restaurant, forcing the host to seat them again. The group keeps doing this fast enough that the host focuses all her attention on ushering them, excluding any other guests. Because this group is draining the host's resources, a line forms outside as more and more people must wait. Some paying customers may eventually be seated, but the average wait time skyrockets, and many potential guests decide to leave.[21]

---

16. *Cf.* Paul A. Walker, *Rethinking Computer Network "Attack": Implications for Law and U.S. Doctrine*, 1 NAT'L SEC. L. BRIEF 33, 49 (2011).

17. @Centrify, *Anatomy of a Hack: Perception vs. Reality,* YOUTUBE (Sept. 30, 2020), https://www.youtube.com/watch?v=fqJXREeKTcA.

18. Some emerging technologies, such as parallel processing and quantum computing, may change this in the future.

19. *See* Lillian Edwards, *Dawn of the Death of Distributed Denial of Service: How to Kill Zombies*, 24 CARDOZO ARTS & ENT. L. J. 23, 23–24 (2006).

20. *Id.* at 24. ("The interesting point about a typical DoS attack is that it is accomplished by making a very large number of nonetheless legitimate demands upon the target's computational resources.").

21. Many DDoS attacks use botnets, or networks of automated computers, to augment the amount of traffic they generate. More on this later. *See* discussion *infra* Section IV.A.4 on page 115.

This is essentially how a DDoS works.[22] The attacking computers (the customers) make continued attempts to "talk to" the webserver in a way that keeps it engaged and unable to devote resources to other computers in the queue. The webmaster or "manager" can block individual computers, but the volume of requests, number of different attackers, and technical workarounds make it hard to keep up.[23] When enough people enter the diner at the same time, a banned customer can effectively put on a hat and sunglasses to slip back in with the crowd.[24] And, because the manager doesn't want to kick out a paying guest accidentally, they are forced to let some suspicious characters fall through the cracks. This mechanism makes DDoS challenging to combat and an effective protest tool: the "attack" is just more legitimate (albeit unwanted) traffic than the server can handle.

II. PROTEST IN AMERICAN JURISPRUDENCE

A. *The Right to Protest*

The First Amendment protects Americans' right to "peacefully assemble."[25] While laws restricting speech based on content are presumed unconstitutional, the government has more freedom to regulate the time, place, and manner of speech if such restrictions are applied to all speech regardless of viewpoint.[26] Content-neutral

22. *See* Cybersecurity & Infrastructure Security Agency, *Security Tip (ST04-015): Understanding Denial-of-Service Attacks*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/uscert/ncas/tips/ST04-015 [https://perma.cc/P4QA-M6PZ] (last visited Feb. 17, 2022) (CISA posting offering a more technical breakdown of DDoS).

23. Edwards, *supra* note 19, at 24–25 ("It is impossible for law enforcement authorities to distinguish between web page requests made by legitimate users and those made for the illicit purpose of bringing down the system. The act in both cases is identical; only the intent behind it is different.").

24. This technique, called "IP Spoofing," makes traffic from one computer look like it is coming from a different computer. *See* Ben Lutkevich, *IP Spoofing*, TECHTARGET, https://www.techtarget.com/searchsecurity/definition/IP-spoofing#:~:text=Internet%20Protocol%20(IP)%20spoofing%20is,the%20sender's%20identity%20or%20both [https://perma.cc/B4AG-RPPC] (last updated Oct. 2021).

25. U.S. CONST. amend. I.

26. *See, e.g.*, Virginia v. Black, 538 U.S. 343, 358 (2003) ("The protections afforded by the First Amendment, however, are not absolute, and we have long recognized that the government may regulate certain categories of expression consistent with the Constitution." (citation omitted)).

laws that do not unduly suppress speech or target a particular perspective generally survive judicial review, as do those that target unprotected categories of speech.[27]

In practice, the government can restrict when and where a protest can occur as long as they allow it to happen in some form. Protestors generally cannot physically prevent others from acting. For example, protestors outside of an abortion clinic cannot physically prevent a patient from entering. Additionally, protestors are banned from using personal threats. In the example of the abortion clinic protestors, they cannot threaten individual patients.[28]

Furthermore, the government may not apply content-based speech restrictions in places that it has made available as a public forum, and the government must provide enough public forums to allow for public discourse.[29] For example, New York City could not ban all public marches in the city, nor could it specifically prevent a neo-Nazi group from picketing city hall.

Critically, the right to protest only applies to public or government-owned spaces. Unlike New York City, with its public sidewalks and green spaces, the Internet has no public forums. Private entities own nearly every part of the Internet's infrastructure,[30] and technological interdependencies make it impossible to say whose "property" the protestors trespassed. For instance, if protestors target a political candidate's website, but the site domain is

27. *Id.* at 358–60.

28. *See, e.g.*, Buttny v. Smiley, 281 F. Supp. 280, 287 (D. Colo. 1968) ("Similarly plaintiffs in the present case had a right to be where they were at the time in question, but they did not have the right to exclude others from free movement in the area.").

29. *See, e.g.*, Schad v. Mount Ephraim, 452 U.S. 61 (1981) (holding that town's ban of all live entertainment was unconstitutionally broad).

30. Some municipalities, such as the city of Chattanooga, operate publicly-funded internet providers, but these arrangements are a tiny minority. *See* Sarah Wray, *Chattanooga's municipal broadband pays off with $2.69 billion in benefits*, CITIES TODAY (Feb. 26, 2021), https://cities-today.com/chattanoogas-municipal-broadband-pays-off-with-2-69-billion-in-benefits/ [https://perma.cc/GL2V-FRPP].

hosted on Google Domain[31] and managed by Squarespace,[32] whose "grass" did they trample?

The privatized nature of the Internet makes traditional First Amendment analysis moot. Private entities are allowed to restrict free speech on their platforms—thus, for example, Twitter could ban former President Donald Trump.[33] In addition, a court would likely interpret laws against DDoS actions as permissible time, place, and manner restrictions. Therefore, the current CFAA is not unconstitutional on a First Amendment basis. However, pro-democratic policy favors loosening the current limits to affirm individuals' rights to protest online.

There is currently no other space for this kind of disruptive protest online. While activists have used social media effectively to drive change in the past,[34] it is not a suitable replacement for the type of disruptive protest that drove—and still drives—nearly every modern civil rights movement. Social media platforms that enable this activist method also curtail its effectiveness. Platforms like Facebook and Twitter use algorithms to tailor content that users see, creating a "filter bubble."[35] It makes sense from a business perspective: users who get angry with the content on a platform are less likely to use it. In practice, activists who attempt to leverage

---

31. Domain Name Service (DNS) are the piece of Internet infrastructure responsible for translating URLs that humans can read to IP addresses that computers can read. *See Domain Name System*, UNIV. OF R.I., https://its.uri.edu/services/94530c3ed6b267ca2f277f48a691602d1ebc0dd2c6/ [https://perma.cc/88RV-C84V] (last visited Oct. 8, 2022). For example, the IPv6 address "2001:4860:4860::8844" resolves to "google.com."

32. Squarespace is a website building service that advertises this exact arrangement. *See Connecting a Google Domain to Your Squarespace Site*, SQUARESPACE, https://support.squarespace.com/hc/en-us/articles/206255268 [https://perma.cc/6VXD-D2JP] (last updated Oct. 3, 2022).

33. Twitter, *Permanent suspension of @realDonaldTrump*, TWITTER (Jan. 8, 2021), https://blog.twitter.com/en_us/topics/company/2020/suspension [https://perma.cc/GHK9-M6U5].

34. These "Hashtag Activism" movements, such as Occupy Wall Street, Black Lives Matter, and #MeToo, have generally succeeded by using social media to organize and raise awareness for their traditional marches and media strategy. *See generally* Ann Nenoff, *#MeToo: A Look at the Influence and Limits of "Hashtag Activism" to Effectuate Legal Change*, 2020 U. ILL. L. REV. 1327 (analyzing the #MeToo movement's successful use of social media).

35. *See generally* ELI PARISER, THE FILTER BUBBLE: WHAT THE INTERNET IS HIDING FROM YOU (2011).

social media often preach to the choir while their message fails to reach those whose minds might change.

On the other hand, DDoS has the advantage of being inherently disruptive. It needs to be disruptive to be effective, just like any conventional protest. Protestors historically expect to risk arrest, so much so that the "jailhouse letter" has become a rite of passage for activists.[36] However, these protestors generally risk minor fines and misdemeanor charges such as trespass or violating the peace.[37] In contrast, the CFAA imposes felony penalties of up to five years for first-time offenders and up to twenty years per count for subsequent offenses.[38] This gross overcharging is a relic from an era fueled by cyber-panic and a widespread public misunderstanding of the Internet rooted in the idea that a plucky teenager could probably hack the Pentagon.[39] It is inappropriate to chill disruptive civil disobedience in a country where one in three adults are online "almost constantly."[40]

This argument is nothing new, however. Hacker activists, or "hacktivists," have used the Internet to stage protests since the Web first came online.

B. *What is "Hacktivism"?*

Proponents have coined *hacktivism* to describe the unique coming together of traditional activist rhetoric and modern computer hacking techniques. For example, an early hacktivist organization, The Cult of the Dead Cow described it as "a policy of hacking, phreaking or creating technology to achieve a political or social

---

36. *See, e.g.*, *Prison Letters,* THE MARSHALL PROJECT, https://www.themarshallproject.org/records/2382-prison-letters [https://perma.cc/F32B-289F] (last updated Apr. 12, 2022).

37. *See* John Alan Cohan, *Civil Disobedience and the Necessity Defense*, 6 PIERCE L. REV. 111, 116 (Sept. 2007) (There were over "3000 prosecutions for criminal trespass and similar violations" from sit-ins leading up to the Civil Rights Act of 1964.).

38. 18 U.S.C. § 1030(c)(B)–(C).

39. *See* Joseph M. Olivenbaum, *Ctrl-Alt-Delete: Rethinking Federal Computer Crime Legislation*, 27 SETON HALL L. REV. 574, 596–97 (1997). In 1983, the movie "War Games" provided a point of cultural reference regarding the dangers of computers and their users. *Id.*

40. Andrew Perrin & Sara Atske, *About Three-in-Ten U.S. Adults Say They are 'Almost Constantly' Online*, PEW RSCH. CTR. (Mar. 26, 2021), https://www.pewresearch.org/fact-tank/2021/03/26/about-three-in-ten-u-s-adults-say-they-are-almost-constantly-online/ [https://perma.cc/R3JY-BF2T].

goal"[41] and "hacking in defense of human rights."[42] Electronic Disturbance Theater, another notable early hacktivist collective, further emphasized hacktivism's activist roots: "[t]he same principles of traditional civil disobedience, like trespass and blockage, will still be applied, but more and more of these acts will take place in electronic or digital form."[43]

Proponents of DDoS have likened it to "virtual sit-ins."[44] The analogy seems apt—both involve the use of abnormal traffic to disrupt regular transit and productivity. And, like sit-ins, DDoS actions can be effective catalysts for social and policy change. One early example of this centered around efforts to pressure a hosting service to drop the Basque separatist publication *Euskal Herria Journal* after a terrorist group associated with the publication committed a high-profile political assassination.[45] After several days of continuous DDoS action, the hosting service capitulated and removed *Euskal Herria Journal* from its servers.[46] This DDoS was an early instance of popular mass online demonstration affecting real-world change. Moreover, it was popular; a mainstream Spanish print newspaper went so far as to print editorials publicly supporting the attack.[47]

Euskal Herria Journal's de-platforming was a victory for supporters of DDoS activism's "virtual sit-in" conception. However, the hosting service decried the event as an attempt to censor one of its clients.[48] Other groups concurred, with one organization likening the DDoS to "burning a bookstore to protest a book."[49] Additionally, one prominent member of the Cult of the Dead Cow

41. Julie L.C. Thomas, *Ethics of Hacktivism*, SANS INST. (Jan. 12, 2001), http://www.dvara.net/hk/Julie_Thomas_GSEC.pdf [https://perma.cc/ 33VT-B2L2].

42. JOSEPH MENN, CULT OF THE DEAD COW: HOW THE ORIGINAL HACKING SUPERGROUP MIGHT JUST SAVE THE WORLD 2–3 (2019).

43. Thomas, *supra* note 41.

44. *See, e.g.*, Xiang Li, *Hacktivism and the First Amendment: Drawing the Line Between Cyber Protests and Crime*, 27 HARV. J.L. & TECH. 301, 309 (2013); Mathias Klang, *Civil Disobedience Online*, 2 J. INFO. COMMC'N & ETHICS SOCIETY 75, 81 (2004).

45. MOLLY SAUTER, THE COMING SWARM: DDOS ACTIONS, HACKTIVISM, AND CIVIL DISOBEDIENCE ON THE INTERNET 14 (2014).

46. *Id.*

47. *Id.* at 52.

48. *Id*. at 14.

49. Thomas, *supra* note 41.

hacker group has gone on record comparing DDoS to "shouting down one's opponent."[50] Though, these criticisms are meritless. While disruptive, a DDoS is not destructive in the same sense as book burning.[51] And while "shouting down" may be rude, it is not generally illegal[52]— it is the entire goal of counter-protesting.

III. THE COMPUTER FRAUD AND ABUSE ACT

Federal law treats all DDoS actions equally under the Computer Fraud and Abuse Act without recognizing the tactic's potential for legitimate political speech.[53] DDoS participants are likewise subject to civil charges from the sites they target and their internet service providers.[54] This Comment, however, focuses only on the CFAA's criminal sanctions. The CFAA criminalizes several facets of cybercrime and cyberterrorism[55], but 18 U.S.C. § 1030(a)(5) is the most expansive provision used to prosecute hacktivist actors. Specifically, 18 U.S.C. § 1030(a)(5) makes it a crime to:

> "[K]nowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer; intentionally access a protected computer without authorization, and as a result of such conduct, recklessly cause damage; or intentionally access a protected computer without authorization, and as a result of such conduct, cause damage and loss."[56]

Accordingly, courts generally apply four elements for a § 1030(a)(5) claim:[57] (1) that the defendant knowingly caused the transmission of a program, information, code, or command; (2) the computer was

50. SAUTER, *supra* note 45, at 47.

51. DDoS "clogs up the system" for a while, but the information is still accessible afterward.

52. Counter-protestors must comply with the same relevant time, place, and manner restrictions.

53. *See generally* 18 U.S.C. § 1030.

54. 18 U.S.C. § 1030(g) ("Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.").

55. *See generally* 18 U.S.C. § 1030(a)(1)–(4).

56. 18 U.S.C. § 1030(a)(5).

57. *See* United States v. Golightley, 840 F. App'x 319, 326 (10th Cir. 2020).

protected; (3) the defendant did not have authorization; and (4) the defendant caused damage.

A. *Elements of a CFAA § 1030(a)(5) Claim*

1. Knowingly Causing the Transmission of a Program, Information, Code, or Command

The first element of a § 1030(a)(5) charge is straightforward—it is hard to hack a computer accidentally, and criminal law generally only punishes where there is intent. One wrinkle to note is opt-in botnets;[58] is an individual who volunteers their machine for a botnet "knowing" of the botnet's ultimate use? This argument has not been tested to date, as most CFAA cases plead out.[59]

2. Against A Protected Computer

The second element of a CFAA claim—that the computer was protected—is straightforward to apply as well. When determining whether a computer system was protected, courts broadly consider protections such as physical controls, digital controls, and procedural controls.[60] Factfinders generally construe this point liberally, and whether a computer is "protected" is usually not at issue in CFAA cases.[61] As in other technical areas of evidence, judges tend to defer to expert testimony on this point, and most defendants build their case around the authorization prong.[62]

3. Transmission Is Without Authorization

Authorization is the most heavily argued element of a CFAA case.[63] The Computer Fraud and Abuse Act, codified in 18 U.S.C. § 1030, defines "exceeds authorized access" as accessing "a

58. "A botnet is a network of computers, usually programmed for some repetitive task, under a single control mechanism." T. Luis de Guzman, *Unleashing A Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges*, 59 CATH. U. L. REV. 527, 528 (2010).

59. *See, e.g.*, United States v. Collins, No. 11-CR-00471-DLJ (PSG), 2013 U.S. Dist. LEXIS 36361 (N.D. Cal. Mar. 15, 2013).

60. *E.g.*, a door lock, a password, or a company policy respectively.

61. *See, e.g.*, United States v. Gottesfeld, 18 F.4th 1 (1st Cir. 2021); United States v. Nosal, 676 F.3d 854 (9th Cir. 2012); United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

62. *See id.*

63. *See id.*

computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter."[64]

The Supreme Court of the United States most recently ruled on the CFAA in *Van Buren v. United States*, where it overruled the appellate court in holding that a police officer had not "exceeded authorized use" within the meaning of the CFAA when he ran an unauthorized query on a law enforcement database because he was generally allowed to access it.[65] In this case, Sergeant Van Buren used his police credentials to access a law enforcement database and gathered license plate information to sell to an FBI informant.[66] The government argued that, by violating departmental policy for database use, Van Buren violated the CFAA. The Court disagreed, noting that Congress passed the CFAA in response to several high-profile cyberattacks and that Van Buren's use of his proper police credentials for a nefarious purpose was not like the cyberattacks Congress intended to criminalize.[67] In doing so, the Court reigned in the CFAA's ambiguous language by rooting it in common law trespass theory rather than more liberal contract law.[68]

This ruling is consistent with several lower court decisions from recent years.[69] Therefore, based on current case law, using a computer system for an unauthorized purpose by a person otherwise allowed to access the system is not a cause of action under the CFAA, and violating a terms of service agreement, acceptable use policy, or end user license agreement is not *prima facie* unauthorized use.

However, it is possible to distinguish the defendants in these cases from DDoS activists. Unlike the sergeant in *Van Buren,*

64. 18 U.S.C. § 1030(e)(6).

65. Van Buren v. United States, 141 S. Ct. 1648, 1652 (2021).

66. *Id.* at 1653.

67. *See id.* at 1652, 1662.

68. *See* Orin Kerr, *The Supreme Court Reins in the CFAA in Van Buren*, LAWFARE (Jun. 9, 2021, 9:04 PM), https://www.lawfareblog.com/supreme-court-reins-cfaa-van-buren [https://perma.cc/7SZC-N5M8].

69. *See, e.g.*, United States v. Drew, 259 F.R.D. 449, 466–67 (C.D. Cal. 2009) (holding that violating a website's terms of use is not a *prima facie* CFAA violation); United States v. Nosal, 676 F.3d 854, 863–64 (9th Cir. 2012) (holding that accessing information in violation of company policy is not a *prima facie* CFAA violation).

DDoS involves people with no prior authorization. DDoS commonly utilizes specialized software,[70] whereas Van Buren interacted with the database by logging on with his proper credentials.

4. Transmission Causes Damage

The CFAA defines damage as "any impairment to the integrity or availability of data, a program, a system, or information."[71] However, in practice, many courts gloss over this element or group it with the authorization element because obtaining unauthorized information from a protected computer is damage *per se*.[72]

Apart from the "unauthorized" element,[73] most DDoS cases are cut-and-dry. DDoS hacktivists are typically knowing, generally unwelcome, and usually impair the availability of a system. Therefore, rather than rewrite § 1030, the most effective solution is to add a carve-out in DDoS cases for good-faith political actors.

IV. PROPOSED AFFIRMATIVE DEFENSE

Congress must amend the Computer Fraud and Abuse Act to recognize an affirmative "political speech" defense based on three possible mitigating factors: (1) the defendant's minimal use of technology to augment their attack; (2) the care and proportionality in their target selection; and (3) the publication of a good-faith political message explaining the protest's purpose. The defendant would stipulate the underlying facts supporting the prosecution while arguing these factors like any affirmative defense. Alternatively, courts may apply this test when handing down sentences in DDoS hacktivist cases.

---

70. This comment will discuss two types of this software, FloodNet and the Low Orbit Ion Cannon, below. *Infra* Section IV.A.ii–iii.

71. 18 U.S.C. § 1030(e)(8).

72. *See generally* United States v. Golightley, 840 F. App'x 319 (10th Cir. 2020); United States v. Gottesfeld, 18 F.4th 1 (1st Cir. 2021).

73. There's a case to be made that, if a website is generally public-facing and violating website terms of service isn't *prima facie* unauthorized use, DDoS is not technically "unauthorized." On a technical level, all a DDoS does is request publicly available web pages over and over again. The website terms of service might prohibit this but, again, that's not a winning argument on its own.

A. *Minimal Automation*

The comparison between DDoS and a traditional sit-in or march breaks down somewhat when protestors use technology to automate their attacks. One could argue that any level of automation negates the assumption that behind each computer is a dedicated activist lending their voice to the cause. However, some level of automation is likely needed for a DDoS to affect any reasonably maintained website.[74] Therefore, courts should consider whether the defendant used the minimum necessary amount of automation to make their DDoS effective. This concept can be illustrated by looking at the following three models of automation.

1. The "Hug of Death" or "Forum Raid" Model

Nearly every college student has experienced class registration systems that slow down and crash when registration opens. The "Hug of Death" model of DDoS causes this effect unintentionally or intentionally—for instance, when a popular blog posts a link to a website with significantly less server capacity for the purpose of drawing attention to the smaller website.[75] This is a pure analog for physical protest because each person going to the website is a unique person adding their "voice" to the rally. However, this technique generally only works on small-scale targets without the resources to absorb the traffic,[76] so it is rarely used for political speech.

2. The FloodNet Model

FloodNet was a program developed by an early hacktivist group called the Electronic Disturbance Theater.[77] It essentially

74. *See* Chad Kime, *How to Stop DDoS Attacks*, ESECURITY PLANET (Sept. 2, 2022), https://www.esecurityplanet.com/networks/how-to-stop-ddos-attacks-tips-for-fighting-ddos-attacks/ [https://perma.cc/YS37-DVX9] (explaining several methods of DDoS remediation).

75. SAUTER, *supra* note 45, at 13; *Hug of Death*, TECHOPEDIA, https://www.techopedia.com/definition/31329/hug-of-death [https://perma.cc/4GQL-YGA8] (last updated Sept. 1, 2016).

76. SAUTER, *supra* note 45, at 13–14.

77. Hacker groups tend to really enjoy branding. *See* Klang, *supra* note 44, at 78.

automated going to a website and refreshing the page repeatedly.[78] These protests maintained the one person, one voice aspect of Forum Raiding, but users were free to set their computers up at home before joining physical demonstrations in the streets.[79]

3. The Low Orbit Ion Cannon Model

The Low Orbit Ion Cannon (LOIC) was the tool that made DDoS famous. Anonymous developed it circa 2008 to 2012 and used the tool to fuel its notoriety.[80] This tool would let users volunteer to join a botnet.[81] Anonymous leadership would select the target, and the owners of the individual machines would not directly participate from that point on. However, they would still generally follow Anonymous's public postings and could opt out of the botnet. Federal prosecutors brought CFAA charges against several California teenagers for using this tool, and the defendants accepted a plea deal.[82]

4. The Booter or DDoS as a Service Model

Up to this point, this Comment has explored DDoS actions with explicitly political goals, powered by politically active (or at least willing) volunteers. However, many DDoS actions are powered by "booters," or botnets of hacked machines.

A massive DDoS action against Microsoft's Xbox network and Sony's PlayStation network spoiled the 2014 Christmas season for many newly minted gamers.[83] However, unlike DDoS activities

78. *See* Molly Sauter, *"LOIC Will Tear Us Apart": The Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks*, 57 AM. BEHAV. SCIENTIST 983, 997 (2013) ("Although the tool automated the process of sending packets, a user still had to target and engage the tool manually.").

79. *Id.* ("[A]n original goal of the FloodNet project might have been to 'leave one's computer protesting at home and then hit the streets to do the same'" (citation omitted)).

80. Due to the decentralized nature of open-source and collaborative software development, several different versions of LOIC existed. This section focuses on versions with "Hive Mind" mode, which enabled users to join the LOIC botnet. *See id.* at 997–98.

81. *Id*. at 997.

82. *Thirteen Plead Guilty to Anonymous Hack of Paypal Site*, BBC (Dec. 12, 2013), https://www.bbc.com/news/business-25327175.

83. Dave Smith, *Why Hacker Gang "Lizard Squad" Took Down Xbox Live and PlayStation Network*, BUS. INSIDER (Dec. 26, 2014, 8:49 AM),

undertaken by groups such as the Electronic Disturbance Theater[84] or Anonymous,[85] the perpetrators were not making a political statement. Instead, it was a marketing campaign.[86] Lizard Squad, the group responsible, publicly took credit for the DDoS action and offered to lease their "Lizard Stresser" botnet for a price.[87] Since then, several booter services have entered the market. Many operate slick websites and tout features such as usability and customer service.[88]

Many booter services bill themselves as "stress-testing tools."[89] They claim their intent is not to attack a network, but to see how a network weathers DDoS or heavy traffic.[90] However, many stress-testing tools are booters sold with a wink and a nod, like head shops marketing pipes "for use with tobacco only."[91] These services do not verify that their client owns the targeted network and style themselves to appeal directly to members of the hacker subculture.[92]

Digital activist ethos embraces the democratizing power of information technology, and booters give minority voices a path to relevance by removing the need for a critical mass of protesters.

---

https://www.businessinsider.com/why-hacker-gang-lizard-squad-took-down-xbox-live-and-playstation-network-2014-12 [https://perma.cc/2GYD-G6PJ].

84. Sauter, *supra* note 78, at 992 ("The EDT held several pro-Zapatista actions in 1998 using FloodNet, targeting websites ranging from those of the Clinton White House and the Pentagon to those of Mexican president Ernesto Zedillo and the Frankfurt Stock Exchange . . . .").

85. *Id.* at 990 ("Beginning in 2008 with Operation Chanology, the actions of Anonymous began to take on a more overtly political tone. . . . The operation involved DDOS attacks and other digital tactics as well as physical-world street protests.").

86. Andrew Griffin, *Lizard Squad Sells Chance to Use the Tool That Took Down Xbox Live and PSN at Christmas*, INDEPENDENT, (Dec. 31, 2014, 10:07 AM), https://www.independent.co.uk/games/xbox-live-and-psn-hacks-were-marketing-for-lizard-squad-s-new-cyberattack-service-9951186.html [https://perma.cc/HQU6-KLYE].

87. *Id.*

88. *See generally* Brian Krebs, *Tag Archives: Booter Service*, KREBS ON SECURITY, https://krebsonsecurity.com/tag/booter-service/ [https://perma.cc/KS8P-EYZE] (last visited Oct. 10, 2022). Brian Krebs has done extensive reporting on booter services. *Id.*

89. SAUTER, *supra* note 45, at 13.

90. *Id.*

91. *Id.* at n.iv.

92. *See generally id.*; Krebs, *supra* note 88.

However, booter owners form their botnets using illegal and unethical means. To revisit the restaurant analogy one more time, use of a booter is like using a mind-control ray or zombie virus to get people to help slow down the restaurant. Members of booter botnets are usually themselves victims of cybercrime.[93]

Cybercriminals often use booters for extortion or vandalism. For example, users of a booter called Mirai first targeted the blog "Krebs on Security," and then a piece of Internet infrastructure called DynDNS.[94] The creators of Mirai exploited vulnerabilities in Internet-enabled baby monitors and other "Internet of Things" devices to build an exceptionally powerful botnet.[95] The culprits convinced Krebs on Security's hosting service to drop the site.[96] Its use against DynDNS effectively shut down the Internet in multiple regions for several hours.[97]

B. *Minimal Damage*

Generally, protestors cannot legally cause property damage, so DDoS activists in this scheme must also avoid undue harm. This prong of the defense would ensure that hacktivists use DDoS to deny access to information temporarily without destroying or altering it. In addition, this element of the affirmative defense would incentivize hacktivists to avoid selecting "critical infrastructure" targets such as supervisory control of data acquisition (SCADA)

93. Janine S. Hiller, *Civil Cyberconflict: Microsoft, Cybercrime, and Botnets*, 31 SANTA CLARA HIGH TECH. L.J. 163, 165 (2014).

94. DynDNS provides the same service as Google Domain as discussed above. Nicky Woolf, *DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say*, GUARDIAN (Oct. 26, 2016, 4:42 PM), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet [https://perma.cc/DX2N-5N3S].

95. Editorial Board, *The Day of the Zombie Baby Monitors: When Hackers Weaponized the Internet of Things*, WASH. POST (Oct. 25, 2016), https://www.washingtonpost.com/opinions/the-day-of-the-zombie-baby-monitors-when-hackers-weaponized-the-internet-of-things/2016/10/25/167fdf42-9a1b-11e6-b3c9-f662adaa0048_story.html [https://perma.cc/S7FP-CBEB].

96. Brian Krebs, *The Democratization of Censorship*, KREBS ON SECURITY (Sept. 25, 2016), https://krebsonsecurity.com/2016/09/the-democratization-of-censorship/ [https://perma.cc/KL7D-9LVV].

97. Nick Statt, *How an Army of Vulnerable Gadgets Took Down the Web Today*, VERGE (Oct. 21, 2016, 4:55 PM), https://www.theverge.com/2016/10/21/13362354/dyn-dns-ddos-attack-cause-outage-status-explained [https://perma.cc/AYB2-8ZPK].

systems[98] or hospital record systems.[99] Property owners would also still have civil recourse against DDoS protestors if Congress only amended the criminal portion of the CFAA.

The lack of public infrastructure online is the hardest part of translating traditional protest methods to cyberspace because there will likely be some unavoidable spillover that affects other related systems. Online spaces do not have public parks or sidewalks for protesters to practice their First Amendment rights—instead, somebody owns every website, server, and connection that makes up the Internet, so there is no "public park" online analog.[100]

However, those affected by spillover would still have civil recourse under the CFAA. Spillover effects are usually *de minimis,* and DDoS protestors can tailor their targets to minimize collateral effects. Additionally, violations of terms of service agreements or end-user licensing agreements are not *prima facie* CFAA violations, so third parties affected by spillover would need to allege actual system effects to recover damages.

C. *Published Political Purpose*

Given the inevitability of spillover effects, ensuring that the protestors act in good faith rather than with a general desire for chaos is crucial. Good faith and purpose separate protests from riots.[101] This prong requires the defendant to publish a political message on publicly available media contemporaneously with the DDoS action to take credit for the DDoS and explain the political motivation.

While melodramatic, the complete statement that Anonymous released for Project Chanology articulated a clear political purpose

---

98. *See* Reese Nguyen, *Navigating* Jus Ad Bellum *in the Age of Cyber Warfare*, 101 CAL. L. REV. 1079, 1107 (2013) (explaining that SCADA systems are generally used to manage critical infrastructure, such as electrical power grids and water treatment facilities).

99. I am borrowing the concept of "targeting" from the law of armed conflict. *See* David A. Wallace & Shane R. Reeves, *Protecting Critical Infrastructure in Cyber Warfare: Is It Time for States to Reassert Themselves?*, 53 U.C. DAVIS L. REV. 1607, 1617 (2020) ("The law of armed conflict regulates the targeting of both persons and objects, regardless of the means or methods used by the parties, in both international and non-international armed conflicts.").

100. *See* SAUTER, *supra* note 45, at 94.

101 *See* Klang, *supra* note 44, at 80 ("The classic justification of civil disobedience lies in a conflict of law with moral principle.").

logically tied to their target selection.[102] They were upset at Scientology for using litigation to quash criticism; therefore, they chose to DDoS Scientology websites and wanted the world to know.[103] By contrast, the creators of Mirai did not publish anything to justify targeting Brian Krebs, let alone targeting one of the foundational services of the Internet.[104]

Furthermore, there must be a good-faith element to the justification, and the actor must not be using the DDoS for pecuniary gain. This defense is not a fig leaf for the Lizard Squads and extortioners of the world. While courts may be hesitant to weigh in on what sort of speech is "legitimate," applying a pecuniary gain test would provide a bright-line rule.

Other commentators have proposed adding stricter scienter or *mens rea* requirements to the CFAA, such as "includ[ing] a specific intent provision requiring a prosecutor to prove that the defendant had a specific intent to cause *significant or irreparable damage* to the target beyond a mere inconvenience."[105] While attractive from a rulemaking standpoint, this test would disproportionately burden prosecutors. This scheme would require the prosecutor to establish the defendant's intent rather than putting the burden on the defendant to make an affirmative defense. Most DDoS actions are not a protest, and the government has a legitimate interest in mitigating spillover effects, so putting the burden of proof on the defense in these cases is the better policy. Placing the burden on the defense may also guide how DDoS protestors structure their cyber-protests because they would plan on relying on a "political speech" defense from the first keystroke. Finally, CFAA cases are incredibly technical and challenging to present to a jury, so requiring the prosecution to educate the jury on more elements would ultimately be imbalanced.

CONCLUSION

Token punishments affirm the rule of law; more stringent punitive measures aim to make an example of the accused and deter

102. *See* CHURCH0FSCIENTOLOGY, *supra* note 1.

103. *See id.*

104. Woolf, *supra* note 94.

105. *See,* Andrew T. Illig, Comment, *Computer Age Protesting: Why Hacktivism is a Viable Option for Modern Social Activists*, 119 PENN. ST. L. REV. 1033, 1055–56 (2015) (emphasis added).

dissent. Civil disobedience has a long and valuable history in America and abroad. It must be allowed to survive in the digital frontier. Specifically, Congress must rework the CFAA to consider the political legitimacy of digital activism. These proposed amendments would effectively protect political speech while mitigating damage by recognizing an affirmative defense based on minimal automation, minimal damage, and a published political purpose to acknowledge the place for disruptive discourse in online American civic life. It is patently unjust for a college student to be sentenced to years in prison for participating in a DDoS of the city government's website while her roommate gets a slap on the wrist for participating in a sit-in at city hall. This disparity is inconsistent with the American tradition of peaceful protest.