Röhle, T., 2021. "DDoS: From Activist Event to Perpetual Crisis."
communication +1, vol 8, iss 1,
DOI: 10.7275/40mc-td21

DDoS: From Activist Event to Perpetual Crisis

Theo Röhle, University of Gothenburg, theo.rohle@jmg.gu.se

This paper focuses on recent changes in the way Distributed Denial of Service (DDoS) attacks are technically administered in order to reassess their role as an activist tactic. By contextualising current forms of attacks within the history of hacktivism, it is possible to discern a shift from DDoS as short-lived event to an enduring phenomenon. The paper discusses the implications of this temporal shift, in terms of a growing reliance on DDoS protection providers and increasingly opaque traffic flows that are managed by these new intermediaries. This discussion then extends towards infrastructure studies in order to question established notions about the relationship between breakdown and visibility. The paper concludes by calling for a stronger engagement with different temporal aspects of recurring communication crises in general and DDoS attacks in particular.

Keywords: hacktivism, Distributed Denial of Service attack, infrastructure, breakdown, maintenance

Introduction

From March to October 2016 recurring attempts were made at blocking access to the official website of the organisation Black Lives Matter.[1] An Anonymous-affiliated team calling itself 'Ghost Squad' took responsibility for some of them, causing confusion on the part of commentators.[2] For many, it was unclear how to reconcile the thrust of these attacks with the political orientation of earlier actions of Anonymous such as campaigns against Scientology and in support of Julian Assange. Ghost Squad, specifically, had earlier targeted the website of the Ku Klux Klan. Yet in a video posted on May 2 on a YouTube channel called @anonymous_exposes_racism, the group explained that they had "seen people in your movement on the streets and social media chanting and posting slogans such as 'Kill Whitey,' 'Death to the slave masters' and other objectionable statements," and had, therefore, decided to take action: "We will not tolerate racist behaviour and hate speech from your movement or any other organization any more than we do from the KKK."[3] Earlier, an account called, "_s1iege" had tweeted screenshots of an ongoing Distributed Denial of Service (DDoS) attack along with the hashtag #OPAllLivesMatter.[4]

These events in 2016 raise many complex questions relating to the nature of online activism and to the specific circumstances of the fight for racial justice in the US.[5] While the full scope of these questions cannot be covered here, the attacks against Black Lives Matter provide an exemplary point of entry for thinking about changes in DDoS attacks as a political tactic. Blocking access to websites of political opponents

---

[1] Corin Faife, "The DDoS Vigilantes Trying to Silence Black Lives Matter", *Ars Technica*, December 14, 2016, https://arstechnica.com/information-technology/2016/12/hack_attacks_on_black_lives_matter/.

[2] Catalin Cimpanu, "Anonymous Ghost Squad Hackers Take Down Black Lives Matter Website", *Softpedia*, May 1, 2016, https://news.softpedia.com/news/anonymous-ghost-squad-hackers-take-down-black-lives-matter-website-503579.shtml.

[3] anonymous exposes racism, "Anonymous Calls out #BlackLivesMatter for Anti-White Racism," YouTube Video, 3:01. May 3, 2016, https://www.youtube.com/watch?v=dDXsInz9jz8.

[4] Anonymous (@_s1ege), "#OpAllLivesMatter #GhostSquadHackers blacklivesmatter.com #Defaced and #Ddos'd ~s1ege" *Twitter*, April 30, 2016, https://twitter.com/_s1ege/status/726206708473847809.

[5] For investigations of these aspects, see Amber M. Hamilton, 'A Genealogy of Critical Race and Digital Studies: Past, Present, and Future', *Sociology of Race and Ethnicity* 6, no. 3 (2020): 292-301; Sarah J. Jackson, Moya Bailey, and Brooke Foucault Welles, *#HashtagActivism: Networks of Race and Gender Justice* (Cambridge, MA: MIT Press, 2020); Marcia Mundt, Karen Ross, and Charla M Burnett, 'Scaling Social Movements Through Social Media: The Case of Black Lives Matter', *Social Media + Society* 4, no. 4 (2018), doi.org/10.1177/2056305118807911.

by means of DDoS attacks has long been considered a key tactic of online activism.[6] It represents a specific kind of induced crisis of communication that causes disruption in the flow of communication, thereby providing an opportunity to focus attention on certain issues.[7] However, as the example of Ghost Squad demonstrates, it is also a polyvalent tactic in the sense that the political (or commercial, criminal or plain malevolent) purposes affiliated with it can diverge widely and are prone to sudden shifts of political orientation.

One development that is especially apparent when considering the events in 2016 is that DDoS attacks have become a more enduring phenomenon. From early campaigns, which in many ways resembled traditional forms of political activism, involving a multitude of engaged people causing temporary disruptions that lasted for some hours or days, DDoS has turned into sustained cascades of highly automated attacks that can last for several months.

The aim of this paper is to spell out the consequences of this shift from DDoS as short-lived events to enduring phenomenon. The core argument is that this shift of temporality has repercussions on the distributional layers of internet infrastructure that have escaped the attention of existing scholarship on DDoS as an activist tactic. This point will be developed through three steps. First, the paper provides a technical overview of developments in the DDoS landscape. Secondly, this overview is related to established positions and periodisations in DDoS research. Thirdly, the discussion extends towards infrastructure studies in order to focus on the relationship between breakdown and visibility. The paper concludes by calling for a stronger engagement with the temporal aspects of recurring communication crises in general and DDoS attacks in particular.

DDoS – Technical Developments

A DDoS attack seeks to exhaust the capacity of a web server by overwhelming it with requests, thus rendering content inaccessible. Under normal working conditions, a request to a server, initiated by a user, prompts that server to send the requested data. During a successful DDoS attack, a server is unable to distinguish between legitimate requests by regular users and requests that are sent with the purpose of bringing the server down. In trying to fulfil all requests, the server and/or the network eventually meet capacity limits, which means that legitimate requests receive error responses.

---

[6] Molly Sauter, *The Coming Swarm. DDoS Actions, Hacktivism, and Civil Disobedience on the Internet* (New York; London: Bloomsbury Academic, 2014).

[7] Tim Jordan and Paul Taylor, *Hacktivism and Cyberwars: Rebels with a Cause?* (London; New York: Routledge, 2004), 75-82.

Usually, DDoS attacks do not affect the data that is stored on a server, but rather make it temporarily inaccessible. Yet, depending on the scale of the attack, it can take a considerable amount of time and resources to restore the functionality of the system.

Denial of Service has a long legacy as a technique for disturbing online communication and a wide range of different strategies have been developed and implemented.[8] Many of these approaches are well known in the field of computer science and there is an equally active development of counter-strategies for defending servers and networks against them.[9] A key factor in these strategies is the ability to identify patterns in DDoS attack traffic, since such patterns can be used as the basis for developing filtering and blocking rules, as well as more flexible traffic management mechanisms based on Machine Learning.[10] At the same time, there is a constant search for vulnerabilities in online systems that can be exploited for expanding DDoS capabilities. The proliferation of connected devices commonly referred to as the Internet of Things is especially prone to such exploitation, since these devices often lack adequate security features.[11]

The simplest versions of DDoS that rely on sending large numbers of identical requests, so-called volumetric attacks, often produce easily identifiable traffic patterns, which is why most websites today are effectively defended against them. More advanced versions of DDoS rely on application layer attacks. These are based on a strategy where requests are sent in ways that mimic the behaviour of regular users, making it difficult to identify and filter out attack traffic. Two popular kinds of application layer attacks are HTTP flood and reflection attacks. An HTTP flood can be initiated by different kinds of software, from simple scripts to more elaborate and established techniques, where requests for large amounts of data are sent at longer intervals. Some of these techniques are comparatively easy to defend against, since they involve identifiable combinations of IP addresses and user agents that can be blocked. Also, many systems serve cached versions of frequently requested files, which reduces the load on servers and, thus, protects them against simple HTTP floods –

---

[8] Laura DeNardis, "A History of Internet Security", in *The History of Information Security: A Comprehensive Handbook*, ed. Karl de Leeuw and Jan Bergstra (Amsterdam, London: Elsevier, 2007), 681-704.

[9] Sajal Bhatia, Sunny Behal, and Irfan Ahmed, "Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions", in *Versatile Cybersecurity*, ed. Mauro Conti, Gaurav Somani, and Radha Poovendran (Cham: Springer Nature Switzerland, 2018), 55-97.

[10] Kian Son Hoon et al., "Critical Review of Machine Learning Approaches to Apply Big Data Analytics in DDoS Forensics", in *2018 International Conference on Computer Communication and Informatics* (ICCCI), 2018, 1-5. https://doi.org/10.1109/ICCCI.2018.8441286.

[11] Constantinos Kolias et al., "DDoS in the IoT: Mirai and Other Botnets", *Computer* 50, no. 7 (2017): 80-84.

which again has triggered the development of counterstrategies on the part of attackers.

Reflection attacks rely on exploiting specific vulnerabilities of systems in order to prompt them to send requests to a target server. Even more advantageous for an attacker are systems that not only reflect, but also amplify traffic, i.e. that send (sometimes considerably) larger amounts of traffic to the target than the attacker sent to the system, thus amplifying bandwidth resources.[12] Beyond the exploitation of such functionalities and vulnerabilities, the spread of malware allows attackers to take complete control over a system, and then instruct them to send requests to a target server or a reflection server. Compromised devices can be gathered into botnets, which receive their instructions from command and control servers. The challenge for the bot herder is then to distribute malware as efficiently as possible, to establish reliant and secure communication to the command and control server, to secure the botnet against being taken over by others and to make it difficult to track down the command and control server that issues instructions.[13]

The example of the DDoS attack against Black Lives Matter illustrates how these developments play out in practice. As a detailed technical investigation shows,[14] botnet commands in this case could be traced back to servers that were rented temporarily from Digital Ocean, a company offering Virtual Private Services and hosted by DMZHOST, a hosting company that keeps the identity of its clients secret. Yet, even if it were possible to identify the clients of these companies, it is not unlikely that they would turn out to be a commercial entity offering DDoS as a service. These services are marketed openly on the web, thinly disguised as "booters" or "stressers" that website owners can use to test the resilience of their systems.[15]

---

[12] Kulvinder Singh and Ajit Singh, "Memcached DDoS Exploits: Operations, Vulnerabilities, Preventions and Mitigations", in *2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*, 2018, 171-79, https://ieeexplore.ieee.org/document/8586810.

[13] Pascal Geenens, "IoT Botnets. The Journey So Far and the Road Ahead", in *Botnets: Architectures, Countermeasures, and Challenges*, ed. Georgios Kambourakis et al. (New York: CRC Press, 2020), 33-100.

[14] Seamus Tuohy, "Botnet Attack Analysis of Deflect Protected Website Blacklivesmatter.com", *eQualitie*, December 14, 2016, https://equalit.ie/en/deflect-labs-report-3-3d/.

[15] Santanna, José Jair, "DDoS-as-a-Service: Investigating Booter Websites" (PhD diss., University of Twente, 2017), https://research.utwente.nl/en/publications/ddos-as-a-service-investigating-booter-websites.

From this – very rough – sketch of developments in the DDoS landscape, three aspects can be singled out as especially pertinent when it comes to DDoS as a political tactic:

1. Complexity of motives

The use of reflection tactics, botnets, command and control servers, virtual private services, etc., increases the distance between the attacker and the target, rendering the attribution of attacks ever more difficult, if not impossible. Therefore, performing a DDoS attack involves very little risk of being exposed. However, the different layers of the attack infrastructure are also characterised by a functional differentiation which can be tied to different motives of the involved actors. Some parts, such as commercial booter services or virtual private services, can be primarily driven by financial gain, whereas other parts, such as malware development, can be primarily fuelled by reputation in hacker circles; others still can be based on political motives, both grass-root activist or state-sponsored.[16] The current DDoS landscape is thus characterised by a growing complexity of interlinked motives on different levels of the attack infrastructure.

2. Automation and consolidation

The use of botnets represents one aspects of a tendency to automate and consolidate DDoS attack capabilities. Both the identification of vulnerable devices and their recruitment into botnets are processes that are increasingly automated, minimising the manual effort involved in being a bot herder. Increasing automation implies that the administration of these services is becoming less laborious and that there is increased competition between different providers, driving prices down. The resulting availability of pre-packaged attack capabilities as a service means that it requires neither technical expertise nor established contacts nor substantial funds to launch attacks against political opponents. In the words of the technical report on the attacks against Black Lives Matter: "Silencing online voices is becoming ever easier and cheaper on the Internet."[17]

---

[16] Some authors seek to identify causal historical trajectories from hacktivism to other forms of DDoS, e.g., Tracey Caldwell, "Hacktivism Goes Hardcore", *Network Security* 2015, no. 5 (1 May 2015): 12-17. The argument here does not follow this line of reasoning, but rather focuses on the intermingling of different motives on different functional layers.

[17] Tuohy, "Botnet Attack Analysis of Deflect Protected Website Blacklivesmatter.com".

3. Reliance on professional protection

With the web becoming an increasingly hostile environment, there is a constant risk that attempts will be made at blocking access to the online presence of activist organisations whenever content or actions are perceived as controversial by others.[18] Without professional protection, even simpler attacks have the potential of blocking access to content. This means that activist organisations have to take the possibility of attacks into account and prepare accordingly by soliciting protection from professional providers of IT security. However, relying on these services also means being at the mercy of a provider's internal policies and business objectives.[19]

Taken together, these three developments suggest an ongoing qualitative shift of DDoS from exceptional disruptions that can work in favour of activists' political purposes to a situation where DDoS becomes part of the infrastructural conditions of online activism. This shift raises crucial questions about power relations in the digital realm: Under what circumstances can DDoS be perceived as a tactic for activists to unbalance prevailing asymmetries of power and under which circumstances does it instead serve to stabilise such asymmetries or contribute to the establishment of new ones?

Phases of Hacktivism

Political DDoS attacks (or DDoS actions as Sauter prefers to call them[20]), especially those performed by Anonymous, are usually considered as part of a broader history of hacktivism. In a recent overview over hacktivism research, Romagna offers a precise

---

[18] For an early empirical investigation from this perspective, see Ethan Zuckerman et al., "Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites" (The Berkman Center for Internet & Society at Harvard University, December 2010), https://cyber.harvard.edu/sites/cyber.harvard.edu/files/2010_DDoS_Attacks_Human_Rights_and_Media.pdf, 10.

[19] A case that has been the subject of substantial debate, both in technical and legal circles, was Cloudflare's decision to terminate its services for the neo-nazi site, "The Daily Stormer," in 2017, see Steven Johnson, "Inside Cloudflare's Decision to Let an Extremist Stronghold Burn", *Wired*, 16 January, 2018, https://www.wired.com/story/free-speech-issue-cloudflare/; Kate Klonick, "The Terrifying Power of Internet Censors", *The New York Times*, 13 September, 2017, https://www.nytimes.com/2017/09/13/opinion/cloudflare-daily-stormer-charlottesville.html.

[20] Sauter, *The Coming Swarm*.

definition of the term as well as a synthesis of periodisations suggested in various historical accounts. Incorporating previous definitions,[21] he defines hacktivism as,

> the sum of ideologies, individual and collective actions typical of traditional activism, applied in cyberspace using hacking techniques, while addressing or exploiting network infrastructure's technical and ontological features, with the final goal of reaching a sociopolitical change in society.[22]

According to Romagna, hacktivism can be placed in between cyberattacks that have permanently destructive consequences and less invasive forms of cyberactivism that primarily rely on disseminating information. Hacktivism involves actual hacking practices, yet with a merely temporary disruptive impact.

Romagna suggests a distinction between three different phases of hacktivism based on changes in normative, organisational and technological aspects. The first phase (from late 1980s to early 2000s) is characterised by the expansion of hacking practices from the specific concerns of the hacking community itself to wider political issues. A prominent example indicating this development is Floodnet: a DDoS software developed by the Electronic Disturbance Theater in 1998 in order to raise attention for the cause of the Zapatistas in Mexico. As Sauter points out in a more detailed analysis of these developments, the extension of hacking practices into more broad-ranging politics did not come without frictions; for example, when silencing political opponents clashed with ideals of a "free flow of information" that was considered central to hacker culture.[23] Karatzogianni highlights the central role of hacktivism in different "ethnoreligious struggles" with patriotic or nationalist agendas during this phase.[24]

The second phase, from 2003 onwards, is characterised by the rise of Anonymous. While Anonymous remains an amorphous organisational formation that

---

[21] Stefania Milan, "Hacktivism as a Radical Media Practice", in *The Routledge Companion to Alternative and Community Media*, ed. Chris Atton (New York: Routledge, 2015), 550-60; Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David F. Ronfeldt (Santa Monica, CA: Rand, 2001), 239-88.

[22] Marco Romagna, "Evolution of Hacktivism: From Origins to Now", in *From Sit-Ins to #revolutions: Media and the Changing Nature of Protests*, ed. Olivia Guntarik and Victoria Grieve-Williams (New York: Bloomsbury Academic, 2020), 65-76, 65.

[23] Sauter, *The Coming Swarm*, 47.

[24] Athina Karatzogianni, *Firebrand Waves of Digital Activism 1994-2014* (London: Palgrave Macmillan, 2015).

is difficult to categorise[25], Romagna sees its growing importance during this phase as a sign of consolidation. The organisational form of hacktivism shifts from smaller, clandestine hacker groups to a larger collective that resembles social movements and with successful strategies for gaining media attention.[26] However, the "patriotic" strand of hacktivism also remains relevant in this phase, with the targeting of Estonian websites in 2007 as a prominent example. The planned transfer of a Russian monument triggered a surge of DDoS attacks against Estonian publications, banks and government websites.[27] The case highlighted the vulnerability of internet infrastructure, eventually leading to the establishment of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn.[28] It is also an example of DDoS attacks where it becomes increasingly difficult to distinguish between "grass-roots" hacktivism and state-sponsored attacks.

The third phase is characterised by diversification. What sets this phase apart from the second, according to Romagna, is that it becomes less of a priority to involve average internet users. Whereas hacktivism software during the second phase was often designed to lower the threshold for participation, the third phase is characterised by small expert teams, some of them with loose affiliation to Anonymous, cooperating in varying constellations. In terms of values, there is a tendency towards particular forms of "vigilante justice"[29] against particular targets, rather than concerted efforts to align with broader sociopolitical agendas.[30] Again, the patriotic strand of hacktivism prevails in this phase, often in reaction to specific geopolitical tensions or conflicts.

Phases of DDoS: Technological developments

While shifts in values and organisational forms are key factors in describing the historical development of hacktivism more broadly, Desiriis suggests that

---

[25] E. Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (London, New York: Verso, 2014); Carolin Wiedemann, "Between Swarm, Network, and Multitude: Anonymous and the Infrastructures of the Common", *Distinktion: Journal of Social Theory* 15, no. 3 (2 September 2014): 309-26.

[26] Romagna, "Evolution of Hacktivism: From Origins to Now", 72.

[27] Finn Brunton, *Spam: A Shadow History of the Internet*, Infrastructures (Cambridge, Massachusetts: The MIT Press, 2013), 188-190.

[28] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School", *International Studies Quarterly* 53, no. 4 (2009): 1155-75.

[29] Romagna, "Evolution of Hacktivism: From Origins to Now", 75.

[30] In this sense, the DDoS attack against Black Lives Matter mentioned in the beginning fits this description well.

technological developments are central to identifying different phases in the development of DDoS specifically.[31]

Some of the first political DDoS attacks, such as the "netstrike" against Strano in 1995[32] and the "Deportation Class" action against Lufthansa in 2001,[33] relied on users who manually and repeatedly sent requests to the targeted server by reloading a website. As Sauter shows, this first phase was quickly superseded by methods where the sending of requests was automatically performed by software such as the Floodnet software used in the Zapatista campaigns.[34] Many DDoS actions performed by Anonymous involved a software called the Low Orbit Ion Cannon (LOIC) that, once installed on a user's computer, could be instructed to send large amounts of requests to a target server.[35]

The third phase in Desiriis' periodisation of the technological development of DDoS is characterised by the increasing involvement of botnets. The most prominent example for this phase is a malware called Mirai, which succeeded in infecting huge numbers of low-end Internet of Things devices, such as security cameras, video recorders and routers, in 2016.[36] This botnet resulted in some of the largest DDoS attacks to date, including an attack on DynDNS that caused major websites including Twitter, *The New York Times*, Reddit and Netflix to become inaccessible for several hours at a time. Within the course of a few months, similar attacks based on Mirai botnets were launched against telecommunication companies and media organisations, as well as blogs of individual journalists.[37]

Functionally, there are similarities between sending requests in an automated way via software like the LOIC and a botnet like the one assembled by Mirai. In each case, a network of computing devices is made to adhere to instructions that are issued from a specific location (a command and control server in the case of botnets, an IRC chat channel controlled by Anonymous in the case of LOIC), which makes it possible

---

[31] Marco Deseriis, "Hacktivism: On the Use of Botnets in Cyberattacks", *Theory, Culture & Society* 34, no. 4 (July 2017): 131-52.

[32] Sauter, *The Coming Swarm*, 50.

[33] Sauter, *The Coming Swarm*, 53-54; Ricardo Dominguez, "Electronic Civil Disobedience Post-9/11", *Third Text* 22, no. 5 (2008): 661-70, 662-667.

[34] Sauter, *The Coming Swarm*, 109-113.

[35] Coleman, *Hacker, Hoaxer, Whistleblower, Spy*, 133-140; Sauter, *The Coming Swarm*, 113-133.

[36] Garrett M. Graff, "How a Dorm Room Minecraft Scam Brought Down the Internet", *Wired*, December 13, 2017, https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/.

[37] Robinson Meyer and Adrienne LaFrance, "When the Entire Internet Seems to Break at Once", *The Atlantic*, October 21, 2016, https://www.theatlantic.com/technology/archive/2016/10/when-the-entire-internet-seems-to-break-at-once/504956/.

to synchronise these devices' resources in order to target a server and overwhelm its capacities. However, while the LOIC, to varying degrees, relied on the *voluntary* contribution of bandwidth and computing power of those using the software, botnets consist of devices that are used for these purposes *without* the consent of their owners.

Effectivity and Legitimacy of DDoS

There is no doubt that the growing use of non-voluntary botnets does make a significant difference in terms of the effectivity of DDoS attacks. Due to improvements in web security, it is questionable whether highly publicised events such as Anonymous' Operation Payback in 2010 would have had any noticeable effect without their involvement.[38] However, there is an ongoing debate whether it also makes a difference in terms of legitimacy whether users have clearly signalled their consent to the use of their equipment (as in the case of the LOIC) or whether it is used in a non-voluntary way, after being infected by malware. Sauter points out that the question of whether to automate server requests was already prevalent during the first phase of DDoS actions and that some technical possibilities were actively disregarded in order to "maintain a one-to-one participant to signal ratio."[39]

For many scholars involved in hacktivism research, the legitimacy of DDoS hinges on the question of whether it should be considered a form of civil disobedience. Delmas is sceptical about including any form of hacktivism in this category since it would lower the level of commitment that she considers central to civil disobedience.[40] Sauter, on the other hand, makes an elaborate case for including DDoS under the category of civil disobedience by comparing it to offline forms of activism and developing a set of criteria for assessing the legitimacy of specific actions. One of these criteria concerns the use of non-voluntary botnets, which they regard as "a grossly unethical action"[41] that impacts negatively on legitimate forms of activism. Celikates and de Zeeuw make the opposite case, arguing that non-voluntary botnets should be considered as legitimate forms of civil disobedience, since they reflect a

---

[38] Candice Delmas, "Is Hacktivism the New Civil Disobedience?", *Raisons Politiques*, no. 1 (2018): 63-81, 70; Deseriis, "Hacktivism", 144; Parmy Olson, *We Are Anonymous: Inside the Hacker World of Lulzsec, Anonymous, and the Global Cyber Insurgency* (New York: Little, Brown and Co, 2012), 117.

[39] Sauter, *The Coming Swarm*, 44.

[40] Delmas, "Is Hacktivism the New Civil Disobedience?", 69.

[41] Sauter, *The Coming Swarm*, 132.

transformation of activist strategies towards "algorithmic resistance."[42] Fordyce makes a similar case involving a historical-critical reading of the concept of the automaton.[43]

Desiriis discusses the use of non-voluntary botnets from an ethical perspective, highlighting both the absence of user consent and the problem of intransparency when decisions about targets are delegated to a small "techno-elite."[44] However, rather than engaging in the debate about legitimacy and civil disobedience, he primarily treats botnets as a case in order to explore how the hybridity of contemporary socio-technical assemblages impacts upon anthropocentric notions of political agency. Drawing on Deleuze and Guattari's distinction between signifying and a-signifying components, as well as Simondon's notions of transindividuation, he seeks to "grasp the evolution of the hacktivist DDoS from a collective human action that uses specialized software tools to achieve specific political ends to a process of transindividuation that is activated by unspecialized network resources."[45] From this perspective, it appears that the use of non-voluntary botnets for hacktivist purposes has "reversed the relationship between collective subjectivation and technological efficiency."[46] Rather than establishing a functional relationship between existing political struggles and technical means to promote this struggle, technicity itself becomes the site of politics.

Breakdown and visibility

Following Desiriis' argument, DDoS attacks can, thus, be interpreted as a struggle about technicity:

> In this respect, Anonymous may well be the name of an emerging *koiné*, a new lingua franca whereby the machines' openness to the

---

[42] Robin Celikates and Daniel de Zeeuw, "Botnet Politics, Algorithmic Resistance and Hacking Society", in *Hacking Habitat: Art of Control*, ed. Ine Gevers (Utrecht: Niet Normaal Foundation, 2016), 209-17, 217.

[43] Robbie Fordyce, "DDoS Attacks as Political Assemblages", *Platform* 5, no. 1 (2013): 6-20. Other versions of these arguments are brought forward by Evgeny Morozov, "Pro-WikiLeaks Denial of Service Attacks: Just Another Form of Civil Disobedience.", *Slate Magazine*, December 13, 2010, https://slate.com/technology/2010/12/pro-wikileaks-denial-of-service-attacks-just-another-form-of-civil-disobedience.html; Cory Doctorow, "We Need a Serious Critique of Net Activism", *The Guardian*, January 25, 2011, sec. Technology, https://www.theguardian.com/technology/2011/jan/25/net-activism-delusion.

[44] Deseriis, "Hacktivism", 145.

[45] Deseriis, "Hacktivism", 136.

[46] Deseriis, "Hacktivism", 146.

> surrounding milieu meets the human belief that defending such openness works in the service of a freer society.[47]

This perspective shares many concerns with debates in infrastructure studies that focus on the "enabling environments"[48] that are taken for granted during times of 'normal' operation. As John Durham Peters states, infrastructure is usually "full of inertia," but at the same time remains "open to sabotage."[49] Moments of crisis or breakdown are considered to be privileged vantage points for those studying infrastructure, because of their potential to reveal aspects that usually escape attention.

Many contributions in the field refer to the seminal list of characteristics of infrastructure developed by Star and Ruhleder, including the assertion that infrastructure "becomes visible upon breakdown."[50] If infrastructure has a tendency to fade into the background, a key question is what kind of strategies can help in rendering it visible – what Bowker and Star have conceptualised as "infrastructural inversion."[51] What is special about breakdown in this sense is that it not only allows researchers to observe socio-technical constellations in a state of uncertainty and negotiability, but also confronts ordinary users, i.e. those relying on the infrastructure in question, with the fragility of their enabling environments – "the server is down, the bridge washes out, there is a power blackout."[52] While such moments of disruption might be experienced as irritating, they are also illuminating. As Jackson puts it, "Breakdown disturbs and sets in motion worlds of possibility that disappear under the stable or accomplished form of the artifact."[53]

However, the strong association between breakdown and visibility that runs through infrastructure research[54] has also been subject to qualifications. In a recent

---

[47] Deseriis, "Hacktivism", 146.

[48] John Durham Peters, *The Marvelous Clouds: Toward a Philosophy of Elemental Media* (Chicago, London: University of Chicago Press, 2015), 3.

[49] Peters, *The Marvelous Clouds*, 31.

[50] Susan Leigh Star and Karen Ruhleder, "Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces", *Information Systems Research* 7, no. 1 (1996): 111-34, 113.

[51] Geoffrey C. Bowker and Susan Leigh Star, *Sorting Things out. Classification and Its Consequences* (Cambridge, Mass.: MIT Press, 2000), 34.

[52] Star and Ruhleder, "Steps Toward an Ecology of Infrastructure", 113.

[53] Steven J. Jackson, "Rethinking Repair", in *Media Technologies. Essays on Communication, Materiality, and Society*, ed. Tarleton Gillespie, Pablo J. Boczkowski, and Kirsten A. Foot, Inside Technology (Cambridge, Mass.: MIT Press, 2014), 221-39, 230.

[54] See also Lisa Parks and Nicole Starosielski, "Introduction", in *Signal Traffic: Critical Studies of Media Infrastructures*, ed. Lisa Parks and Nicole Starosielski (Urbana: University of Illinois Press, 2015), 1-27, 6.

contribution to the debate, Seberger and Bowker question the premise that failure is an observable quality of an object, because this perspective disregards the role of human subjectivity in experiencing the visibility of infrastructure.[55] They highlight the fact that instances of "hyper-functionality" can be equally disturbing and are, thus, revealing from a subjective point of view. By broadening the range of human experiences that potentially contribute to the awareness of infrastructure, they seek to arrive at an understanding of breakdown that is not tied to "objectival visibility."[56]

A different critique is developed in a seminal paper by Graham and Thrift.[57] Questioning the premise that breakdown appears in the form of extraordinary events, they seek to shift focus towards small and everyday instances of failures that they consider inherent to infrastructures. By assuming brokenness and decay, rather than smooth functionality, as the status quo, they seek to highlight the role of maintenance and repair that usually receives little attention. By focusing on the human labour that is necessary to keep infrastructures functional, this perspective also helps to grasp the profoundly sociotechnical nature of infrastructure, rather than seeing it as primarily technical arrangements. Jackson points out how this shift of focus, "draws our attention around the sociality of objects forward, into the ongoing forms of labor, power, and interest – neither dead nor congealed – that underpin the ongoing survival of things as objects in the world."[58]

Both kinds of qualifications – the integration of subjective experience and the integration of maintenance and repair – thus seek to broaden the horizon of what can be considered as breakdown. They also tie in with a stronger orientation of the field towards process and practices reflected in the shift of terminology from infrastructures to "infrastructuring."[59] However, scholarly contributions that more

---

[55] John S. Seberger and Geoffrey C. Bowker, "Humanistic Infrastructure Studies: Hyper-Functionality and the Experience of the Absurd", *Information, Communication & Society*, 21 February, 2020, 1-16.

[56] Seberger and Bowker, "Humanistic Infrastructure Studies", 3.

[57] Stephen Graham and Nigel Thrift, "Out of Order: Understanding Repair and Maintenance", *Theory, Culture & Society* 24, no. 3 (2007): 1-25.

[58] Jackson, "Rethinking Repair", 230.

[59] Helena Karasti and Anna-Liisa Syrjänen, "Artful Infrastructuring in Two Cases of Community PD", in *Proceedings of the Eighth Conference on Participatory Design: Artful Integration: Interweaving Media, Materials and Practices - Volume 1*, PDC 04 (New York, NY, USA: Association for Computing Machinery, 2004), 20-30; Volkmar Pipek and Volker Wulf, "Infrastructuring: Toward an Integrated Perspective on the Design and Use of Information Technology", *Journal of the Association for Information Systems* 10, no. 5 (2009); Christopher A Le Dantec and Carl DiSalvo, "Infrastructuring and the Formation of Publics in Participatory Design", *Social Studies of Science* 43, no. 2 (2013): 241-64.

explicitly focus on the role of temporality in infrastructure have hitherto mostly been confined to the field of anthropology and urban geography.[60]

DDoS as breakdown

There is, thus, an emerging debate about the relationship between breakdown and visibility within the broader field of infrastructure studies. As a specific kind of breakdown of communication infrastructure, DDoS attacks are a relevant phenomenon to consider in this regard. Accordingly, similar questions have been raised in this field of research, for example by Sauter:

> A direct action DDoS seeks to strip away the attractive, humanized facade to reveal a corporate target's reality as black boxed and monolithic, fundamentally unresponsive (metaphorically and actually) to human concerns.[61]

In this sense, the temporary crisis of communication is ascribed a potential to reveal, to open up for scrutiny and to open up for new possibilities. Beck strikes a similar chord when discussing the deterritorialising effect of DDoS attacks and pointing out how these "changed belief structures, produced new knowledge, spawned physical protests, and made local oppressive actions visible globally."[62] Breakdown plays a similar role in Desiriis' argument, which, with a more sociotechnical focus, revolves around the "margin of indetermination of machines and living beings."[63] In his argument, botnets and Anonymous itself are seen as sociotechnical amalgamations that raise the question of indetermination. However, it is the breakdown of communication induced by DDoS attacks that represents the inflection point where this negotiation of openness becomes visible.

When confronting these perspectives with the critique developed by Graham and Thrift,[64] it appears that DDoS research, too, is preoccupied with major failures at the expense of mundane acts of maintenance. This is hardly surprising given the

---

[60] Nikhil Anand, Akhil Gupta, and Hannah Appel, eds., *The Promise of Infrastructure* (Durham, NC: Duke University Press, 2020); Mary Lawhon et al., "Thinking through Heterogeneous Infrastructure Configurations", *Urban Studies* 55, no. 4 (2018): 720-32; Kavita Ramakrishnan, Kathleen O'Reilly, and Jessica Budds, "The Temporal Fragility of Infrastructure: Theorizing Decay, Maintenance, and Repair", *Environment and Planning E: Nature and Space*, 2020, doi.org/10.1177/2514848620979712.

[61] Sauter, *The Coming Swarm*, 45.

[62] Christian Beck, "Web of Resistance: Deleuzian Digital Space and Hacktivism", *Journal for Cultural Research* 20, no. 4 (1 October 2016): 334-49, 346.

[63] Deseriis, "Hacktivism", 148.

[64] Graham and Thrift, "Out of Order".

canonical cases that are discussed in the literature. Historically, the political use of DDoS follows the logic of political campaigning by actively creating temporarily disruptive events that trigger public and media attention – as reflected in the name "Electronic *Disturbance* Theater." As an intentionally created communication crisis with a political agenda, it seems that the very essence of DDoS is its exceptionality. However, when looking at the recent technological development of DDoS beyond the canonical examples, the question of exceptionality becomes more complicated. In the following section, the sketch of technical developments provided above will be used as a basis for a more elaborate discussion of the relationship between exceptionality and visibility.

DDoS becomes ordinary

As discussed, central aspects that are characteristic for the development of the DDoS landscape are the growing complexity of motives and the automation and consolidation of DDoS capabilities. These developments have contributed to DDoS attacks becoming a persistent, rather than an exceptional phenomenon,[65] and have resulted in an increasing reliance of activist organisations on professional protection services. Whereas the existing scholarship has primarily focused on DDoS as a tactic employed by activist organisations, the shift towards DDoS as a persistent phenomenon necessitates a stronger focus on how they are subjected to such attacks. From being a tool in the hacktivist arsenal – as the periodisations discussed above portray it – DDoS has turned into an aspect of the material infrastructural conditions of online activism. This calls for a stronger engagement with the systemic consequences of DDoS protection requirements and a critical investigation of the actors providing such services.

A productive theoretical approach to guide such an investigation is developed by Burkart and McCourt, who focus on the productive or systemic consequences of hacking rather than on its exceptional or disruptive qualities.[66] A key argument in their analysis, based on a political economy perspective, is that hacking creates particular kinds of economic risks. Systemically speaking, "the market processes these risks by commodifying them."[67] The authors point towards the global increase in

---

[65] Mattijs Jonker et al., "Millions of Targets under Attack: A Macroscopic Characterization of the DoS Ecosystem", in *Proceedings of the 2017 Internet Measurement Conference*, IMC '17 (New York, NY, USA: Association for Computing Machinery, 2017), 100-113.

[66] Patrick Burkart and Tom McCourt, "The International Political Economy of the Hack: A Closer Look at Markets for Cybersecurity Software", *Popular Communication* 15, no. 1 (2017): 37-54.

[67] Burkart and McCourt, "The International Political Economy of the Hack", 41.

cybersecurity spending, which indicates a growing market for both cybersecurity tools and services and insurance against hacking losses as well as increasing venture capital that flows into cybersecurity companies.

While their analysis focuses on hacking in general, the core argument holds for DDoS attacks as well. For companies, the inaccessibility of content due to a DDoS attack, even if it is temporary, poses a direct financial risk. For activist or journalistic websites, DDoS attacks represent a risk that relevant information is withheld from public debate. In both cases, DDoS attacks can also negatively impact on organisations' reputation, economy and public support. Providers of commercial DDoS protection seize upon this opportunity, marketing their services towards larger corporations that are prepared to invest substantially in IT security. Actors that are considered to be leading in this particular field are Akamai, Cloudflare, Imperva and Radware.[68] The increase of Cloudflare's market capitalisation from 5 billion dollars in 2019 to 23 billion dollars in 2020 gives an indication of the growing relevance of this form of "risk processing." According to a 2019 forecast, the global market for DDoS protection and mitigation is expected to almost double from 2.4 billion in 2019 to 4.7 billion in 2024.[69]

DDoS protection services rely on a combination of different techniques for identifying and filtering out malicious traffic. This is increasingly done as a service and on the network level, which implies that the owner of a website agrees to route all incoming traffic through the servers of the protection provider. There, the traffic is analysed in order to identify patterns that can be linked to known attacks, sometimes also involving assessments of individual IP addresses' reputation. Scale is a significant aspect in this regard, since the performance of filtering mechanisms can be improved by analysing large amounts of attack data, especially when these mechanisms are based on Machine Learning. But scale is also an advantage when it comes to the size of the provider's network. For example, the Content Delivery Networks of Akamai and Cloudflare play an increasingly central role for the distribution of large files across the web, e.g., for streaming services, by means of

---

[68] David Holmes, "The Forrester Wave™: DDoS Mitigation Solutions, Q1 2021", 2021, https://www.a10networks.com/wp-content/uploads/The-Forrester-Wave-DDoS-Mitigation-Solutions-Q1-2021.pdf.

[69] MarketsandMarkets, "DDoS Protection and Mitigation Market by Solutions & Services – 2024", July 2019, https://www.marketsandmarkets.com/Market-Reports/ddos-protection-mitigation-market-111952874.html.

redundant local storing and dedicated private networks.[70] However, their bandwidth capacities, along with high flexibility when it comes to traffic management, also provides effective measures against DDoS attacks.[71]

The commercial offerings of these protection providers are out of reach for under-resourced NGOs. They therefore rely on free versions of protection services, sometimes involving limits on the volume of attack traffic that is processed. Cloudflare has gained a dominant position in this field by offering free basic DDoS protection services without volume limitations. There are also more comprehensive free protection programmes specifically geared towards human rights organisations and journalistic outlets, such as Google's "Project Shield"[72] and Cloudflare's "Project Galileo."[73] Similar advanced protection programmes for independent media organisations and NGOs are offered by non-commercial providers such as eQualitie[74] and Qurium.[75]

Even if NGOs, thus, have a number of options to choose from, they have, structurally speaking, become dependent on the free DDoS protection services provided by the above companies and organisations. The fact that the market for DDoS protection is dominated by few actors and that scale favours the largest ones, raises concerns about growing market concentration in this area.

The politics of infrastructuring

The discussion above points towards a different relationship between breakdown and visibility than is usually envisaged in infrastructure studies. Rather than holding a potential for increased visibility, DDoS attacks have – by shifting from exceptional events to perpetual crisis – contributed to the establishment of new intermediaries in the form of DDoS protection providers. As an ever-larger part of internet traffic is being routed through the networks of these intermediaries, it is affected by centrally implemented decision mechanisms that remain opaque to the average user.

---

[70] Christian Sandvig, "The Internet as the Anti-Television: Distribution Infrastructure as Culture and Power", in *Signal Traffic: Critical Studies of Media Infrastructures*, ed. Lisa Parks and Nicole Starosielski (Urbana: University of Illinois Press, 2015), 225-45.

[71] Ramesh K. Sitaraman et al., "Overlay Networks: An Akamai Perspective", in *Advanced Content Delivery, Streaming, and Cloud Services*, ed. Mukaddim Pathan, Ramesh Kumar Sitaraman, and Dom Robinson (Hoboken, New Jersey: Wiley, 2014), 307-28.

[72] https://www.projectshield.withgoogle.com/

[73] https://www.cloudflare.com/galileo/

[74] https://equalit.ie/portfolio/deflect/

[75] https://www.qurium.org/secure-hosting/

This development clearly diverges from earlier incarnations of internet infrastructure that spawned hopes of self-organisation[76] and "fringe intelligence."[77] These hopes were especially tied to the end-to-end principle, where routing and control functions are performed by adaptive decision mechanisms at the edges of the network, whereas the core merely transmits according to basic rules.[78] Even if historical investigations point toward the need to nuance this picture,[79] there is an observable shift in how traffic is being processed and analysed. Rather than the "nonsynchronous optimization" of the earlier internet that "prefers to leave the optimal unsettled,"[80] the current situation is, according to McKelvey, characterised by "polychronous optimization"[81] that is technically administered by "intermediary daemons." Ever more fine-grained information about what kinds of traffic are being transported supplies these intermediaries with criteria for "micro-decisions"[82] about the routing of data: "The unsettled metastability of the internet is replaced by a regulated system of service guarantees and data limits. The diagram shifts from the edges to the core, with infrastructures progressively taking on greater management capacities."[83]

The growing reliance on DDoS protection services is, thus, part of a general development towards traffic management mechanisms that remain opaque to users – and, as such, a new kind of infrastructural invisibility. Taking the long-term consequences of DDoS attacks into consideration, therefore, provides a more comprehensive picture of the power relations emerging from the use of such attacks. This suggests that, when discussing the legitimacy and effectivity of DDoS, it does not

---

[76] Tarleton Gillespie, "Engineering a Principle: 'End-to-End' in the Design of the Internet", *Social Studies of Science* 36, no. 3 (2006): 427-57.

[77] Tiziana Terranova, *Network Culture. Politics for the Information Age* (London, Ann Arbor, MI: Pluto Press, 2004), 66.

[78] Jerome H. Saltzer, David P. Reed, and David D. Clark, "End-to-End Arguments in System Design", *ACM Transactions on Computer Systems* 2, no. 4 (1984): 277-88.

[79] Bradley Fidler, " The Evolution of Internet Routing: Technical Roots of the Network Society", *Internet Histories* 3, no. 3-4 (2 October 2019): 364-87.

[80] Fenwick McKelvey, *Internet Daemons: Digital Communications Possessed*, Electronic Mediations 56 (Minneapolis, London: University of Minnesota Press, 2018), 113.

[81] McKelvey, *Internet Daemons*, 115.

[82] Florian Sprenger, *The Politics of Micro-Decisions: Edward Snowden, Net Neutrality, and the Architectures of the Internet* (Lüneburg: Meson Press, 2015).

[83] McKelvey, *Internet Daemons*, 115. On the question whether this development should be seen as a practical necessity, see Christopher S. Yoo, *The Dynamic Internet: How Technology, Users, and Businesses Are Transforming the Network* (Washington, D.C: AEI Press, 2012), 91 and from a more theoretical perspective Paul Dourish, "Protocols, Packets, and Proximity", in *Signal Traffic. Critical Studies of Media Infrastructures*, ed. Lisa Parks and Nicole Starosielski (University of Illinois Press, 2015).

suffice to focus on particular political constellations; rather, there is a need to also reflect upon their impact on an infrastructural level.

What this change of perspective implies is to pay closer attention to the different kinds of temporality involved in DDoS attacks, including a reassessment of established notions of breakdown and visibility. The maintenance approach in infrastructure studies can be seen as one step in this direction. Contrasting an emphasis on the eventfulness of large-scale ruptures with a more process-oriented focus on decay and repair helps to recognise different modes of temporality involved in communication breakdown. Yet, the protection provided by services such as Cloudflare hardly fit the description of small-scale and ad-hoc maintenance. The traffic management performed by these providers is rather systematic, centralised and globally coordinated. Therefore, following Holt, such intermediaries cannot merely be considered "connecting agents or messy middlemen – they are in many cases key infrastructures and primary agents of power."[84]

DDoS protection represents an emerging kind of infrastructure that does not become visible upon breakdown, but rather thrives on it. A promising approach to explore this relationship could be to abandon visuality as a guiding metaphor. As Carmi convincingly argues, sound and listening metaphors are a more apt choice when seeking to theorise persistent forms of communication crises, especially those re-appearing in certain patterns or rhythms. According to her, reoccurring patterns of "media distortions" engender forms of "processed listening" that seek to measure, categorise and filter "deviant" behaviour:

> when specific bodies, behaviors and rhythms interfere with media companies' business model(s), they illegitimize them and filter, remove, delete, and reduce them. They become noise, disturbance, deviant, and spam.[85]

While Carmi does mention DDoS attacks in passing, an elaborated account of DDoS protection as a form of "processed listening" remains a desiderate. Thinking of these intermediaries as forms of listening would help to refocus attention to forms of temporality other than the event – the progressive weaving of measurement capabilities into the infrastructure of the internet, the continuous adaptation of

---

[84] Jennifer Holt, "Data Troubles: Digital Distribution in the Platform Economy", *On_Culture*, no. 8 (2019), http://geb.uni- giessen.de/geb/volltexte/2020/15092/, 3.

[85] Elinor Carmi, *Media Distortions: Understanding the Power behind Spam, Noise, and Other Deviant Media* (New York: Peter Lang, 2019), 40.

filtering rules to recurring patterns identified in traffic analysis and the gradual persuasion of website owners to become accustomed to their reliance on protection.

Conclusions

This paper has focused on crises of communication caused by current forms of DDoS attacks and has highlighted the need to reflect upon the different temporal dimensions of such attacks. In a more immediate sense, a successful DDoS attack disrupts the exchange of data between clients and servers, thus rendering content inaccessible. Depending on the political constellations involved, this can have a revealing impetus, in the sense that it focuses attention on specific political questions. It can also create a sense of technicity, i.e. bringing the openness and negotiability of technical constellations to the fore. However, when these kinds of breakdown become ordinary, they rather appear as detrimental to visibility, elevating protection providers into an intermediary position where they decide about the accessibility of content, thus introducing opaque mechanisms of traffic management.

Acknowledging these long-term effects of DDoS attacks allows for a more comprehensive understanding of their role, both in terms of hacktivist tactics and in terms of infrastructural developments. Hacktivism research that focuses on DDoS as a political tactic seems preoccupied with the immediate political impact of specific attacks. This comes at the expense of their more systemic infrastructural consequences. Integrating further temporal perspectives could help to better understand the interrelationship between specific, situated attacks and the broader economic and technological structures that they bring about. Broadening the horizon in this way seems especially important when discussing the legitimacy of DDoS attacks. To put it bluntly: How relevant is the immediately perceivable effect of current DDoS attacks compared to the behind-the-scenes infrastructural adjustments that they trigger? Depending on the (empirical) answer to this question, many arguments that have been brought forward in favour of DDoS as a political tactic might have to be re-evaluated.

On a more abstract level, the paper has highlighted the need to reflect upon different forms of temporality when theorising the relationship between breakdown and infrastructure. As a kind of communication crisis, DDoS points to the fact that certain kinds of persistent breakdown render infrastructure opaque, rather than allowing revealing insights. Focusing on the way that repetitive patterns of interference contribute to long-term infrastructural transformations holds the potential of broadening analyses of power relations in current media environments. Programmatically speaking, it is also a call to explore a greater variety of temporal

relationships between crises of communication and infrastructures of communication.

Bibliography

Anand, Nikhil, Akhil Gupta, and Hannah Appel, eds. *The Promise of Infrastructure*. Durham, NC: Duke University Press, 2020.

Anonymous (@_s1ege), "#OpAllLivesMatter #GhostSquadHackers blacklivesmatter.com #Defaced and #Ddos'd -s1ege" *Twitter*, April 30, 2016, https://twitter.com/_s1ege/status/726206708473847809.

anonymous exposes racism. "Anonymous Calls out #BlackLivesMatter for Anti-White Racism," *YouTube Video*, 3:01. May 3, 2016. https://www.youtube.com/watch?v=dDXsInz9jz8.

Beck, Christian. "Web of Resistance: Deleuzian Digital Space and Hacktivism". *Journal for Cultural Research* 20, no. 4 (2016): 334-49.

Bhatia, Sajal, Sunny Behal, and Irfan Ahmed. "Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions". In *Versatile Cybersecurity*, edited by Mauro Conti, Gaurav Somani, and Radha Poovendran, 55-97. Cham: Springer Nature Switzerland, 2018.

Bowker, Geoffrey C., and Susan Leigh Star. *Sorting Things out. Classification and Its Consequences*. Cambridge, Mass.: MIT Press, 2000.

Brunton, Finn. *Spam: A Shadow History of the Internet*. Infrastructures. Cambridge, Massachusetts: The MIT Press, 2013.

Burkart, Patrick, and Tom McCourt. "The International Political Economy of the Hack: A Closer Look at Markets for Cybersecurity Software". *Popular Communication* 15, no. 1 (2017): 37-54.

Caldwell, Tracey. 'Hacktivism Goes Hardcore'. *Network Security* 2015, no. 5 (1 May 2015): 12-17.

Carmi, Elinor. *Media Distortions: Understanding the Power behind Spam, Noise, and Other Deviant Media*. New York: Peter Lang, 2019.

Celikates, Robin, and Daniel de Zeeuw. "Botnet Politics, Algorithmic Resistance and Hacking Society". In *Hacking Habitat: Art of Control*, edited by Ine Gevers, 209-17. Utrecht: Niet Normaal Foundation, 2016.

Cimpanu, Catalin. "Anonymous Ghost Squad Hackers Take Down Black Lives Matter Website". *Softpedia*, May 1, 2016. https://news.softpedia.com/news/anonymous-ghost-squad-hackers-take-down-black-lives-matter-website-503579.shtml.

Coleman, E. Gabriella. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London, New York: Verso, 2014.

Delmas, Candice. "Is Hacktivism the New Civil Disobedience?" *Raisons Politiques*, no. 1 (2018): 63-81.

DeNardis, Laura. "A History of Internet Security". In *The History of Information Security: A Comprehensive Handbook*, edited by Karl de Leeuw and Jan Bergstra, 681-704. Amsterdam, London: Elsevier, 2007.

Denning, Dorothy E. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy". In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, edited by John Arquilla and David F. Ronfeldt, 239-88. Santa Monica, CA: Rand, 2001.

Deseriis, Marco. "Hacktivism: On the Use of Botnets in Cyberattacks". *Theory, Culture & Society* 34, no. 4 (2017): 131-52.

Doctorow, Cory. "We Need a Serious Critique of Net Activism". *The Guardian*, 25 January 2011, sec. Technology. https://www.theguardian.com/technology/2011/jan/25/net-activism-delusion.

Dominguez, Ricardo. "Electronic Civil Disobedience Post-9/11". *Third Text* 22, no. 5 (2008): 661-70.

Dourish, Paul. "Protocols, Packets, and Proximity". In *Signal Traffic. Critical Studies of Media Infrastructures*, edited by Lisa Parks and Nicole Starosielski. University of Illinois Press, 2015.

Faife, Corin. "The DDoS Vigilantes Trying to Silence Black Lives Matter". Ars Technica, 14 December 2016. https://arstechnica.com/information-technology/2016/12/hack_attacks_on_black_lives_matter/.

Fidler, Bradley. 'The Evolution of Internet Routing: Technical Roots of the Network Society'. *Internet Histories* 3, no. 3-4 (2019): 364-87.

Fordyce, Robbie. "DDoS Attacks as Political Assemblages". *Platform* 5, no. 1 (2013): 6-20.

Geenens, Pascal. "IoT Botnets. The Journey So Far and the Road Ahead". In *Botnets: Architectures, Countermeasures, and Challenges*, edited by Georgios Kambourakis, Marios Anagnostopoulos, Weizhi Meng, and Peng Zhou, 33-100. New York: CRC Press, 2020.

Gillespie, Tarleton. "Engineering a Principle: 'End-to-End' in the Design of the Internet". *Social Studies of Science* 36, no. 3 (2006): 427-57.

Graff, Garrett M. "How a Dorm Room Minecraft Scam Brought Down the Internet". *Wired*, December 13, 2017. https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/.

Graham, Stephen, and Nigel Thrift. "Out of Order: Understanding Repair and Maintenance". *Theory, Culture & Society* 24, no. 3 (2007): 1-25.

Hamilton, Amber M. 'A Genealogy of Critical Race and Digital Studies: Past, Present, and Future'. *Sociology of Race and Ethnicity* 6, no. 3 (2020): 292-301.

Hansen, Lene, and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School". *International Studies Quarterly* 53, no. 4 (2009): 1155-75.

Holmes, David. "The Forrester Wave™: DDoS Mitigation Solutions, Q1 2021", 2021. https://www.a10networks.com/wp-content/uploads/The-Forrester-Wave-DDoS-Mitigation-Solutions-Q1-2021.pdf.

Holt, Jennifer. "Data Troubles: Digital Distribution in the Platform Economy". *On_Culture*, no. 8 (2019). http://geb.uni-giessen.de/geb/volltexte/2020/15092/

Hoon, Kian Son, Kheng Cher Yeo, Sami Azam, Bharanidharan Shunmugam, and Friso De Boer. 'Critical Review of Machine Learning Approaches to Apply Big Data Analytics in DDoS Forensics'. In 2018 International Conference on Computer Communication and Informatics (ICCCI), 1-5, 2018. https://doi.org/10.1109/ICCCI.2018.8441286.

Jackson, Sarah J., Moya Bailey, and Brooke Foucault Welles. *#HashtagActivism: Networks of Race and Gender Justice*. Cambridge, MA: MIT Press, 2020.

Jackson, Steven J. "Rethinking Repair". In *Media Technologies. Essays on Communication, Materiality, and Society*, edited by Tarleton Gillespie, Pablo J. Boczkowski, and Kirsten A. Foot, 221-39. Inside Technology. Cambridge, Mass.: MIT Press, 2014.

Johnson, Steven. 'Inside Cloudflare's Decision to Let an Extremist Stronghold Burn'. *Wired*, 16 January 2018. https://www.wired.com/story/free-speech-issue-cloudflare/.

Jonker, Mattijs, Alistair King, Johannes Krupp, Christian Rossow, Anna Sperotto, and Alberto Dainotti. "Millions of Targets under Attack: A Macroscopic Characterization of the DoS Ecosystem". In *Proceedings of the 2017 Internet Measurement Conference*, 100-113. IMC '17. New York, NY, USA: Association for Computing Machinery, 2017.

Jordan, Tim, and Paul Taylor. *Hacktivism and Cyberwars: Rebels with a Cause?* London, New York: Routledge, 2004.

Karasti, Helena, and Anna-Liisa Syrjänen. "Artful Infrastructuring in Two Cases of Community PD". In *Proceedings of the Eighth Conference on Participatory Design: Artful Integration: Interweaving Media, Materials and Practices - Volume 1*, 20-30. PDC 04. New York, NY, USA: Association for Computing Machinery, 2004.

Karatzogianni, Athina. *Firebrand Waves of Digital Activism 1994-2014*. London: Palgrave Macmillan, 2015.

Klonick, Kate. 'The Terrifying Power of Internet Censors'. *The New York Times*, 13 September 2017. https://www.nytimes.com/2017/09/13/opinion/cloudflare-daily-stormer-charlottesville.html.

Kolias, Constantinos, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. "DDoS in the IoT: Mirai and Other Botnets". *Computer* 50, no. 7 (2017): 80-84.

Lawhon, Mary, David Nilsson, Jonathan Silver, Henrik Ernstson, and Shuaib Lwasa. 'Thinking through Heterogeneous Infrastructure Configurations'. *Urban Studies* 55, no. 4 (2018): 720-32.

Le Dantec, Christopher A, and Carl DiSalvo. 'Infrastructuring and the Formation of Publics in Participatory Design'. *Social Studies of Science* 43, no. 2 (2013): 241-64.

MarketsandMarkets. "DDoS Protection and Mitigation Market by Solutions & Services - 2024", July 2019. https://www.marketsandmarkets.com/Market-Reports/ddos-protection-mitigation-market-111952874.html.

McKelvey, Fenwick. *Internet Daemons: Digital Communications Possessed*. Electronic Mediations 56. Minneapolis, London: University of Minnesota Press, 2018.

Meyer, Robinson and LaFrance, Adrienne. "When the Entire Internet Seems to Break at Once". *The Atlantic*, October 21, 2016. https://www.theatlantic.com/technology/archive/2016/10/when-the-entire-internet-seems-to-break-at-once/504956/.

Milan, Stefania. "Hacktivism as a Radical Media Practice". In *The Routledge Companion to Alternative and Community Media*, edited by Chris Atton, 550-60. New York: Routledge, 2015.

Morozov, Evgeny. "Pro-WikiLeaks Denial of Service Attacks: Just Another Form of Civil Disobedience." Slate Magazine, December 13, 2010. https://slate.com/technology/2010/12/pro-wikileaks-denial-of-service-attacks-just-another-form-of-civil-disobedience.html.

Mundt, Marcia, Karen Ross, and Charla M Burnett. 'Scaling Social Movements Through Social Media: The Case of Black Lives Matter'. *Social Media + Society* 4, no. 4 (2018), https://doi.org/10.1177/2056305118807911.

Olson, Parmy. *We Are Anonymous: Inside the Hacker World of Lulzsec, Anonymous, and the Global Cyber Insurgency*. New York: Little, Brown and Co, 2012.

Parks, Lisa, and Nicole Starosielski. "Introduction". In *Signal Traffic: Critical Studies of Media Infrastructures*, edited by Lisa Parks and Nicole Starosielski, 1-27. Urbana: University of Illinois Press, 2015.

Peters, John Durham. *The Marvelous Clouds: Toward a Philosophy of Elemental Media*. Chicago, London: University of Chicago Press, 2015.

Pipek, Volkmar, and Volker Wulf. "Infrastructuring: Toward an Integrated Perspective on the Design and Use of Information Technology". *Journal of the Association for Information Systems* 10, no. 5 (2009).

Ramakrishnan, Kavita, Kathleen O'Reilly, and Jessica Budds. 'The Temporal Fragility of Infrastructure: Theorizing Decay, Maintenance, and Repair'. *Environment and Planning E: Nature and Space*, 2020. https://doi.org/10.1177/2514848620979712.

Romagna, Marco. "Evolution of Hacktivism: From Origins to Now". In *From Sit-Ins to #revolutions: Media and the Changing Nature of Protests*, edited by Olivia Guntarik and Victoria Grieve-Williams, 65-76. New York: Bloomsbury Academic, 2020.

Saltzer, Jerome H., David P. Reed, and David D. Clark. "End-to-End Arguments in System Design". *ACM Transactions on Computer Systems* 2, no. 4 (1984): 277-88.

Sandvig, Christian. "The Internet as the Anti-Television: Distribution Infrastructure as Culture and Power". In *Signal Traffic: Critical Studies of Media Infrastructures*, edited by Lisa Parks and Nicole Starosielski, 225-45. Urbana: University of Illinois Press, 2015.

Santanna, José Jair. "DDoS-as-a-Service: Investigating Booter Websites" (PhD diss., University of Twente, 2017). https://research.utwente.nl/en/publications/ddos-as-a-service-investigating-booter-websites.

Sauter, Molly. *The Coming Swarm. DDoS Actions, Hacktivism, and Civil Disobedience on the Internet*. New York; London: Bloomsbury Academic, 2014.

Seberger, John S., and Geoffrey C. Bowker. "Humanistic Infrastructure Studies: Hyper-Functionality and the Experience of the Absurd". *Information, Communication & Society*, 2020, https://doi/10.1080/1369118X.2020.1726985

Singh, Kulvinder, and Ajit Singh. "Memcached DDoS Exploits: Operations, Vulnerabilities, Preventions and Mitigations". In *2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*, 171-79, 2018.

Sitaraman, Ramesh K., Mangesh Kasbekar, Woody Lichtenstein, and Manish Jain. "Overlay Networks: An Akamai Perspective". In *Advanced Content Delivery, Streaming, and Cloud Services*, edited by Mukaddim Pathan, Ramesh Kumar Sitaraman, and Dom Robinson, 307-28. Hoboken, New Jersey: Wiley, 2014.

Sprenger, Florian. *The Politics of Micro-Decisions: Edward Snowden, Net Neutrality, and the Architectures of the Internet*. Lüneburg: Meson Press, 2015.

Star, Susan Leigh, and Karen Ruhleder. "Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces". *Information Systems Research* 7, no. 1 (1996): 111-34.

Terranova, Tiziana. *Network Culture. Politics for the Information Age*. London ; Ann Arbor, MI: Pluto Press, 2004.

Tuohy, Seamus. "Botnet Attack Analysis of Deflect Protected Website Blacklivesmatter.com". *eQualitie*, December 14, 2016. https://equalit.ie/en/deflect-labs-report-3-3d/.

Wiedemann, Carolin. "Between Swarm, Network, and Multitude: Anonymous and the Infrastructures of the Common". *Distinktion: Journal of Social Theory* 15, no. 3 (2014): 309-26.

Yoo, Christopher S. *The Dynamic Internet: How Technology, Users, and Businesses Are Transforming the Network*. Washington, D.C: AEI Press, 2012.

Zuckerman, Ethan, Hal Roberts, Ryan McGrady, Jillian York, and John Palfrey. "Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites". The Berkman Center for Internet & Society at Harvard University, December 2010. https://cyber.harvard.edu/sites/cyber.harvard.edu/files/2010_DDoS_Attacks_Human_Rights_and_Media.pdf.