Sauter, Molly. "Conclusion: The future of DDoS." *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet*. New York: Bloomsbury Academic, 2014. 159–162. *Bloomsbury Collections*. Web. 26 Apr. 2023. <<http://dx.doi.org/10.5040/9781628926705.0014>>.

Downloaded from Bloomsbury Collections, www.bloomsburycollections.com, 26 April 2023, 15:29 UTC.

Copyright © Molly Sauter 2014. You may share this work for non-commercial purposes only, provided you give attribution to the copyright holder and the publisher, and provide a link to the Creative Commons licence.

Conclusion: The future of DDoS

Over the course of this book, I've attempted to arrive at a thorough description of the history and current practice of activist DDoS actions. The question now is, will the practice of activist DDoS actions continue, or are practical, theoretical, and ethical challenges faced too great to allow for the tactic to be effective?

As I described earlier, downtime is notoriously hard to achieve for an all-volunteer activist DDoS action, especially against a large corporate target. An “arms race” dynamic has ensued, which encourages the use of nonvolunteer botnets and exploits to augment volunteer efforts and which also diminishes the ethical validity of activist DDoS actions. The defensive capabilities of for-hire firms such as Akamai, Prolexic, and Arbor Networks, responding mainly to the advancements in criminal DDoS actions, continue to outstrip the capabilities of nearly all activist campaigns.

As downtime continues to become more and more difficult to ethically achieve, media exhaustion also becomes a concern. In 2013, criminal DDoS actions received more coverage than activist DDoS actions, and coverage often does not make clear the distinctions between the two types of actions. Could activist DDoS actions simply become invisible in the sea of criminal actions? Or could the media landscape go the other way, with DDoS actions of all stripes becoming so commonplace that they warrant no coverage at all? Either outcome would be

devastating for the publicity and messaging goals of activist DDoS actions.

The use of DDoS as a tactic of extortion, criminality, and nation-state initiated censorship is damaging to its perceived legitimacy as an activist tactic. This association hampers the perception of activist DDoS actions as legitimate and worthwhile acts of political activism, and also prevents the further diffusion of the tactic. The flamboyant, antisocial pantomime performed by Anonymous and other similar groups further restricts *open* use of the tactic to an online fringe.

Because of its enduring associations with criminality and extreme online subcultures, in addition to its current legal status and particular technical challenges, I think it is unlikely at this time that DDoS actions will ever become a part of the popularly accepted activist repertoire of contention in the near future, unlike similar physical-world tactics like sit-ins or occupations. However, I predict that DDoS actions will remain popular among internet-based fringe groups and subcultures, particularly those that adhere to a Barlowian view of the independent, self-contained nature of the internet. As high-profile hacker and computer crime cases come to trial these will serve as radicalizing events, “group grievances,” for the transgressive, technologically mediated subcultures that are currently serving as cultural laboratories for disruptive online activism.

This radicalization, which occurs most strongly in the aftermath of convictions (such as those of Andrew Aurenheimer, also known as weev; or Jeremy Hammond) or tragedies (such as the suicide of Aaron Swartz), further underlines the perceived disjuncture between behavioral norms in these subcultures (or, in some cases, in more mainstream, technologically sophisticated populations) and the legal response delivered by the state. The popular association of activist DDoS actions with criminality is often not of interest to these radicalized groups, and may even be a point of attraction. The disapproval of the state can serve to underscore its cluelessness with regard to the internet and technologically mediated transgressive subcultures, a cluelessness

that these subcultures in turn often see as something to mock and exaggerate.

Is the use of DDoS by these groups abridging their ability to develop other innovating forms of online activism? The answer to this is an unequivocal “no.” Though not examined in this book, the resurgence of tactics like doxing, “human flesh search,” information exfiltration, leaking, defacement, software development, the remote organization of backup internet connectivity in the event of nation-level shutdowns, alternative infrastructure and service construction, and large-scale data analysis, either automated or human-distributed, are all indicators of innovative developments in tactical and strategic activism. However, many of these are advanced activities, requiring significant skill, organization, support, and planning to pull off. They are not entry-level activities. As such, the pool of potential participants is much smaller, and would not necessarily benefit from a massive influx of inexperienced but nonetheless eager participants. Moreover, many of the tactics listed earlier and others are not attention-oriented in the same way that many activist DDoS actions are: massive amounts of media attention are not their goal, and may be detrimental. The attention-oriented nature of activist DDoS actions lends itself to encouraging media coverage at a level that other tactics might not.

As a “street-less” space, that the internet runs counter to many assumed practices of speech and public politics appears to belie Nathan Jurgenson’s “digital dualism” fallacy.¹ The “speechy” nature of the online space had led to this seeming contradiction, wherein existing speech online is so highly valued that we drastically devalue other types of disruptive, activist speech which are tolerated, even specifically valued, in the off-line world. If we acknowledge that civil disobedience and disruptive activism are valuable tools of activist speech and political discourse in the physical world, then it must also be acknowledged that they should be equally valuable and desirable in the online space. In the online space, dissenting speech should have a platform and a voice, ones that we are

occasionally obligated to encounter, just as we encounter them in the physical world. As an avenue for speech, the internet should also be open to dissenting, potentially disruptive speech. Without forced encounters with dissent, our democratic society will stagnate.

Activist DDoS actions started as an exploration into the activist potential of the internet by activists experienced in street activism. In its modern incarnation, activist DDoS is practiced mainly by fringe actors, who consider the online space a primary zone of interaction, socialization, and political action. Though in many ways an extremely accessible stepping stone to more involved methods of online activism, DDoS actions remain privileged in many ways, including their basic technological nature, the specific populations involved, and the specific legal and cultural challenges inherent in modern nonmainstream computer use. Though DDoS itself may become increasingly marginalized as an activist practice, high-profile campaigns such as Operation Payback and the ensuing legal battles have opened the debate on the validity, desirability, and potential of disruptive activism and civil disobedience in the online space. This book is presented as a step toward the robust analysis of these repertoires of contention in the online space that has become such an integral part of our modern culture.

Note

- 1 Nathan Jurgenson, "Digital Dualism versus Augmented Reality," *Cyborology*, February 24, 2011. Last accessed March 3, 2014, <http://thesocietypages.org/cyborgology/2011/02/24/digital-dualism-versus-augmented-reality/>.