Gabriella Coleman
Gabriella Coleman is an Assistant Professor of Media, Culture, and Communication at New York University.

The ethics of digital direct action
Denial-of-service attacks and similar tactics are becoming more widely used as protest tools.

Last Modified: 01 Sep 2011 22:36

Although some Anonymous participants protest in person, most of their political activity consists of direct action online, such as launching Distributed Denial of Service attacks [GALLO/GETTY]

The political movement known as Anonymous has managed to capture the attention of the media, the hearts of many supporters, and the ire of many spectators after an eight-month spree of political interventions, stretching from Distributed Denial of Service (DDoS) campaigns, to human rights technical assistance in Tunisia, to a more recent spate of hacks under the guise of Operation Antisec.

The state has now fully entered the fray with its own flurry of activity. In the past month, twenty-two alleged participants in the United States and the United Kingdom have been arrested, the bulk of them (14) in connection with a single operation: the spectacular wave of DDoS attacks aimed directly at protesting actions taken by Mastercard and Paypal in December 2010. These were launched after these companies refused to accept donations for Wikileaks front man Julian Assange, soon after the activist organisation released a trove of diplomatic cables. Hackers and activists supporting the DDoS campaign (and certainly not all do support the campaign) regard this act as legitimate protest activity, akin to a blockade or "digital sit-in". Yet, if convicted, the participants of Anonymous could be charged with felonies and land in prison with excessive punishments.

On July 20, 2011, a day after the US-based arrests, FBI officials offered a rare glimpse into its justification for the crackdown, citing a need to nip "chaos" in the bud: "We want to send a message that chaos on the internet is unacceptable," said Steven Chabinsky, deputy assistant FBI director.

Although most of the arrests were for the DDoS campaign, the FBI official never differentiated between hacking and DDoSing. The former is defined by computer break-ins or trespassing, while the latter refers to gumming up a server by bombarding it with too many requests. Curiously, this official also never went so far as to label the alleged participants criminals, terrorists, or vigilantes.

By complaining about Anonymous' (hereafter Anons) tactics in the absence of any stated criminal offense, the FBI appears to acknowledge, if in a somewhat oblique fashion, that the hunt for some Anons is politically motivated. The FBI also appears to acknowledge that, in contrast to terrorists and criminals, whom the state is justified in prosecuting since they have violated the contract that ostensibly undergirds social norms in modern civil society, Anons are in fact exercising their rights as citizens to demonstrate on behalf of "causes" they believe in: "[Even if] hackers can be believed to have social causes, it's entirely unacceptable to break into websites and commit unlawful acts. There has not been a large-scale trend toward using hacking to actually destroy websites, [but] that could be appealing to both criminals or terrorists. That's where the 'hacktivism,' even if currently viewed by some as a nuisance, shows the potential to be destabilising," insisted Chabinsky, in language that mirrors critiques of 1960s-era social movements.

Of course these brief statements should not be taken as the state's sole, much less its final, words on Anonymous. They are interesting insofar as they gesture toward a social fact concerning Anonymous' increasingly prominent role in social protest movements: Many of their actions are politically motivated and conscientious, and the December 2010 DDoS campaign, Operation Avenge Assange, was no exception.

DDoS campaigns can be legitimate tactics

Whether or not one agrees with all of Anonymous' many tactics - some of them being illegal and disruptive, others falling in the province of peaceful and legal human rights assistance, and still others in a gray moral and legal zone - under certain circumstances, the DDoS can be considered as non-violent protest in line with well-recognised protocols for public assembly, the difference being the medium. Of course, as with any form of public assembly, some Anons are merely along for the ride. Others might in fact exhibit reckless behaviour.

But this is an inevitable feature of Anonymous' platform, open to seasoned activists and newcomers alike: Some novice participants cut their teeth on politics for the first time with their Anonymous brethren, forming, no doubt, an individual political consciousness, which has fed into a more robust sense of democracy in action, especially after Anons held campaigns in support of the uprisings in the Middle East and Africa that have helped to displace authoritarian regimes that had managed to exploit their constituencies for decades on end.

Even if the FBI is ambivalent about explicitly denouncing Anonymous as a criminal threat, its tactics of arrest and intimidation and their criminalisation of all tactics used by Anons, such as DDoS, constitute an approach to security and surveillance that deserves critical attention, especially if any of these arrests move to trials.

There are many ways to think of the DDoS campaign against PayPal and Mastercard, but one way we might think of it is as digital direct action. Emerging organically, this movement did not wait for a judge, politician, nor a journalist to declare a legal or moral judgment. Citizens took matters into their own hands. In less than 24 hours, a large assembly of citizens took not to the streets where protest activity traditionally unfolds, but to the digital agora to act on their own accord, to loudly assert their opinion on a matter, and to act directly against

those actors they felt were acting unjustly. If they happened to break laws, these laws were viewed, with good reason, to be unjust.

Like all traditions, direct action is diverse in its make-up, tactics, history, and purpose. At times, activists seek to block access in order to protect a resource, as with tree sit-ins in the Pacific Northwest or blocking Japanese whaling ships in the Southern Ocean as carried out by Sea Shepherd. In the long tradition of Plowshares actions, the intent is to get arrested in order to publicise an issue. Anonymous rendered Mastercard and Paypal's webpages defunct for a number of days by flooding their servers with too many requests and did so to garner media attention, to make their platform visible, and to demand that Assange be given due process. In this sense, they were successful, no matter what the outcome of the case made against them.

What made the events of December 2010 unusual - and extraordinary - as a moment of direct action poses a challenge for prevailing theories of civil disobedience. Many of the most notable acts of civil disobedience, even virtual sit-ins, have been organised by small affinity groups in which participants are public and typically well aware of the legal consequences of their actions.Some participants in these actions even have their lawyer's phone number written on their arm in permanent marker.

Anonymous, which prides itself on not having a readily identifiable, corporate form, was powerless to defend itself using these methods. Thus, as the December events unfolded, I was glued to the computer watching how Anons would or even could minimise the risk and chaos that to some degree characterised these interactions. Remarkably, "the hive mind", as they refer to themselves, never spun out of control. They stayed on target and conjoined their disruptions with manifestos and videos explaining their rationales.

But at the time, one thing was clear and has been repeated by sympathetic and unsympathetic observers alike: Many participants were likely unaware of the legal risk they were taking, and did not have lawyers to contact in the face of a future arrest. The spectacular events of December, combined with the recent arrests, have of course changed all of this; many of us have now been educated as to the risks at hand. The legal risks and the philosophical subtleties of DDoS as a disruptive direct action tactic no longer reside within the sole province of a smaller circle of activists who have practiced and theorised this tradition for over a decade. A much larger swath of citizens have subsequently entered the fray.

In light of these arrests, whether or not DDoS campaigns are always an effective political sword to wield (and they are strong arguments to be made on both sides) is not the primary question that should concern us. The key issue is the evidence used to decide who is involved and to determine what they ought to be charged with doing. If a DDoS action is deemed as always and under every circumstance unacceptable - always a tactic of chaos - this will in the short term result in excessive penalties; in the long term, an excessive clamp down, such as felony charges for those that stand accused, could stifle these tactics altogether on the internet.

This is damaging to the overall political culture of the internet, which must allow for a diversity of tactics, including mass action, direct action, and peaceful of protests, if it is going to be a medium for democratic action and life.

Gabriella Coleman is an Assistant Professor of Media, Culture, and Communication at New York University. Her first book, Coding Freedom: The Aesthetics and the Ethics of Hacking, is forthcoming with Princeton University Press and she is currently working on a new book on Anonymous and digital activism.