Article

Theory Culture & Society

Theory, Culture & Society
2017, Vol. 34(4) 131–152

DOI: 10.1177/0263276416667198
journals.sagepub.com/home/tcs
SAGE

Hacktivism: On the Use of Botnets in Cyberattacks

Marco Deseriis
Northeastern University

Abstract

This article offers a reading of internet-based activism or 'hacktivism' as a phenomenon that cannot be confined to the instrumental use of information technologies. It focuses on a subset of hacktivism – the distributed-denial-of-service (DDoS) attack for political ends – that aims at making an internet host unavailable to its intended users. Since the early 2000s these attacks have been increasingly conducted by means of botnets – networks of infected computers that send bogus requests to a target website without the consent of their users. The capacity of botnets to engender a more-than-human politics is analyzed from two distinct theoretical angles. First, drawing from Deleuze and Guattari, the hacktivist DDoS is discussed as an assemblage of signifying and a-signifying components, voluntary and involuntary actions. Second, Gilbert Simondon's notions of transindividuation and transduction allow for a conceptualization of hacktivism as a sociotechnical assemblage with a high degree of indetermination.

Keywords

anonymous, botnet, DDoS attack, Gilles Deleuze, electronic civil disobedience, Felix Guattari, hacktivism, Gilbert Simondon

Since its introduction in the 1990s, the term hacktivism has been denoting a range of political practices that make creative use of information technologies or, conversely, technical inventions and software hacks that have explicitly political goals. Hacktivist campaigns and interventions span collective actions of electronic civil disobedience (Jordan and Taylor, 2004), illegal hacking of corporate and government databases (Olson, 2012; Coleman, 2014), political coding of free and open source software (Chopra and Dexter, 2008; Kelty, 2008; Coleman, 2013), the development of encryption technologies that bypass government surveillance (Assange et. al., 2012), and the anonymous leaking of classified

Corresponding author: Marco Deseriis. Email: m.deseriis@neu.edu
Extra material: http://theoryculturesociety.org/

information (Greenberg, 2012). In all these cases, hacktivism denotes the capacity to introduce or make an unconventional *use* of information technologies for a variety of political ends.

Taking a non-utilitarian approach, this article advances a reading of hacktivism as a phenomenon that cannot be reduced to the instrumental use of information technologies. It does so by examining the concatenation of hacking and activism from the vantage point of a significant subset of hacktivist practices: the distributed-denial-of-service (DDoS) attack. Because of the low level of technical literacy that it requires of its participants, the hacktivist DDoS attack enables widespread participation in an online protest. In this sense, it is one of those rare instances in which a large-scale collective action meets the hacker's ability to forge tools and find ingenious technical solutions. At the same time, the distributed-denial-of-service attack is criticized by some hackers for its reliance on buggy software, for denying freedom of speech to political opponents, and for the network congestion it may cause.

Whereas the terms of this controversy have been widely discussed (Galloway, 2004; Jordan and Taylor, 2004; Samuel, 2004; Deseriis and Marano, 2008; Sauter, 2014; Coleman, 2014), in this article I do not limit myself to examining the hacktivist DDoS from the standpoint of its legitimacy and effectiveness. Rather, I frame the distributed-denial-of-service attack as a hybrid sociotechnical assemblage of human and nonhuman actors to ask what are the effects of this hybridization on anthropocentric notions of political agency. The question is explored through the different techniques, discourses, and technologies that have been employed to conduct distributed-denial-of-service attacks since the mid-1990s. After dividing the history of the hacktivist DDoS into an early conceptual phase, in which hacktivists manually reloaded a target website, and a second phase characterized by the development of ad hoc software designed to automate the webpage reload, I focus on a third, ongoing, phase defined by the growing use of botnets – networks of infected computers that are remotely controlled to execute a DDoS.

The use of botnets marks a significant discontinuity with early hacktivist practices because it mobilizes networks of infected computers without user consent. Rather than criticizing this shift for its dubious ethics and politics, I argue that it might reveal the irruption of a more-than-human logic into human affairs. As different media theorists point out, the relative autonomy and emergent properties of computer networks are most evident in network accidents and anomalies such as viruses, worms, spam, porn, and botnets (Galloway and Thacker, 2007; Pasquinelli, 2008; Parikka and Sampson, 2009; Sampson, 2012). Indeed, as we will see, the viral assembling of a botnet escapes the control of the human actors who leverage its distributed power to perform a variety of actions – including spam deliveries, stealing user credentials, and network takeovers. From this angle, a botnet-based hacktivist DDoS

is nothing but a political appropriation of networked resources that have been assembled to perform a variety of nonpolitical tasks.

But if digital networks are constitutive to hacktivism and have properties of their own, then their political function is not merely determined *a posteriori* by their mode of use. Rather, taking a cue from Mark Hansen, we should bear in mind 'the crucial capacity of machines to function *beyond* or *outside* of the experiential domain occupied by humans, but nonetheless in a broader coupling with them' (2012: 42). To account for this political capacity of technology to invite new sets of actions and relations, the hacktivist DDoS is examined from two distinct theoretical angles. First, drawing from Deleuze and Guattari's conceptual couple, social subjection and machinic enslavement, I discuss the hacktivist DDoS as a sociotechnical assemblage of signifying and a-signifying components, voluntary and involuntary actions, human imagination and a-subjective flows of desire. In this sense, the centrality of botnets to contemporary cyberwar calls for a thorough examination of the machinization of desire, both from the perspective of internet users' unintended actions and the political economy of these machines.

Second, drawing from Gilbert Simondon's theory of individuation, I examine the hacktivist assemblage as a sociotechnical process of 'transindividuation' whereby a collective comes into being through an invented technical object. According to Simondon, technical invention has the capacity to institute a 'transindividual' relation proceeding directly from individual to individual, without the need for any other intermediary or external validation. On the one hand, technical being 'is inexhaustibly rich in informational terms; it is open to any human gesture that makes use of it and recreates it, inserting itself into an *élan* of universal communication' (1989: 263–4). On the other hand, the technical operation has for Simondon an 'intrinsic normativity' that 'modifies the code of values of a closed society' (p. 265) by introducing new sets of relations among humans and between humans and the natural world.

Drawing from Simondon's insight that technical invention modifies the values of a community, I argue that the normativity intrinsic to the botnet – in short, what a botnet can do – forces a change in the values of early hacktivism. Whereas early distributed-denial-of-service attacks extended to cyberspace tactics of civil disobedience such as the strike and the sit-in, the use of botnets marks an ontological shift in the status of hacktivism. Because botnets are unspecialized machines whose efficiency and resilience is independent of the particular uses humans make of them, they are, in Simondonian terms, machines with a high degree of indetermination This indetermination presupposes a receptivity to the information environment that allows the botnet to couple with other technical individuals so as to evolve in time. It also implicitly invites humans to value their own indetermination, that is, to

develop a sensibility and caring for the openness of machines and living beings alike beyond any utilitarian concern.

To elucidate this point, the final part of the article examines the use of botnets by the hacktivist network Anonymous. My wager is that Anonymous' hacktivism is more concerned with keeping open 'the technical conditions of social becoming' (Barthélémy, 2012: 204) than with putting technology at the service of political aims that are extrinsic to the reticular organization of the technical world.

From Subjection and Enslavement to Subjectivation and Generativity

In *A Thousand Plateaus*, Deleuze and Guattari introduce the concepts of social subjection and machinic enslavement to denote two different kinds of relationship between humans and machines. 'There is enslavement', write Deleuze and Guattari, when human beings are 'constituent pieces of a machine that they compose among themselves and with other things (animals, tools), under the control and direction of a higher unity' (1987: 457). By contrast, social subjection occurs when the higher unity constitutes the human 'as a subject linked to a now exterior object, which can be an animal, tool, or even a machine' (p. 457). Although Deleuze and Guattari point out that subjection and enslavement should be seen as 'two coexistent poles', different forms of social and political organization can lean more towards one or the other. While the great despotic empires of antiquity did not discriminate among humans, animals and tools – enslaving them indifferently as building components of the same 'mega-machine' – the rise of modern capitalism brings about a new regime of social subjection. On the one hand, the modern nation-state subjects the worker to its laws and territorial organization so as to compensate for capital's push towards deterritorialization and abstraction (p. 455). On the other hand, the worker is formally free to use technologies that are exterior to him. The worker, however, ceases to be an exterior user of the machine as soon as cybernetics introduces 'humans-machines systems' wherein 'the relation between humans and machines is based on internal, mutual communication and no longer on usage or action' (p. 458). In fact, as the 'science of feedback' in the human, the animal, and the machine (Wiener, 1948), cybernetics treats its living and technical components indifferently, enslaving them to a machine that is only interested in their information exchanges.

Deleuze and Guattari use the example of network television to explain how subjection and enslavement may coexist within the same informational machine. As a signifying machine, TV subjectifies individuals by assigning them – as either subject of enunciations or spectators – pre-codified roles that reflect the dominant order '(you, dear television viewers, who make TV what it is . . .)' (p. 458). As an a-signifying machine, TV

enslaves spectators by turning them into input/output elements that either block or allow the flow of information. Thus, as Maurizio Lazzarato (2006) points out, 'subjection operates at the molar level of the individual (its social dimension, the roles, functions, representations and affections). Enslavement on the other hand operates at the molecular (or pre-individual or infrasocial) level (affects, sensations, desires, those relationships not yet individuated or assigned to a subject).' This distinction implies two different ways of looking at the relationship between humans and machines: 'Social subjection regards individuals and machines as entirely self-contained entities (the subject and the object) and establishes insurmountable boundaries between them. Machinic enslavement, by contrast, considers individuals and machines as open multiplicities' (2006).

If enslavement and subjection coexist within network TV, they surely coexist within the internet. The internet user is subjectified qua user – i.e. as a subject of will and action – every time he opens a social media profile, subscribes to a weblog or newsletter, chooses one website over another, and so forth. Besides reinforcing the dominant position of content, service and 'identity providers', these signifying operations rely on a clear-cut distinction between the subject and the object, the user and the medium, the human and the machine. Conversely, the user is enslaved *by* the machine every time he performs a-signifying activities such as restarting a computer, upgrading a software, running an antivirus, and so forth. These operations – which are often involuntary and required by the network in order to maintain its functionality – turn the user into an intrinsic component of an assemblage that knows no distinction between the human and the technical. 'In machinic enslavement, there is nothing but transformations and exchanges of information, some of which are mechanical, others human' (Deleuze and Guattari, 1987: 458).

There are, however, a few key differences between TV and the internet that Deleuze and Guattari's distinction between subjection and enslavement does not fully capture. Whereas TV interpellates viewers as spectators, the internet user is not simply targeted as a consumer of information but also as a relay that can share or comment upon existing information, thus becoming himself a source of information. Hence, on a signifying level, the internet user is constantly prodded to become a *subject of enunciation* – a position that TV reserves to a selected few. On an a-signifying level, internet users' input exceeds the level of signification every time programmers, hackers, software engineers and web designers develop protocols or applications that reconfigure both the capacity of machines to communicate with one other and their broader coupling with human beings. In this respect, Jonathan Zittrain's definition of the internet as a 'generative technology' that allows third-party coders to expand it in new and unforeseen directions (Zittrain, 2008) is useful to

think of machines that cannot be despotically overcoded, or directed from above, without losing much of their power.

From this perspective, the coupling of social subjection and machinic enslavement appears inadequate to describe the active subject position of internet users and the generative character of networked information technologies. In particular, socio-technical phenomena such as open source software, wikis, and user-generated content suggest that *subjectivation* and *generativity* are not alternative to one another but, like subjection and enslavement, presuppose and reinforce each other. In this sense, signifying processes such as the cyber-libertarian belief that information should be free, the collaborative ethos of open source software, and the reputation economy often associated with user-generated content can be seen as part of a larger process whose material and a-signifying side includes the production of hardware and software for accessing, storing, and sharing information.

Thinking hacktivism through the lens of this broader coupling allows us 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, which blur the boundaries between the voluntary and the involuntary, the subjective and the a-subjective, human and nonhuman agency. In the next section, I examine the historical evolution of the hacktivist DDoS from an early phase based on the manual reload of a target website to a second phase characterized by the development of software tools designed to automate the webpage reload. After considering how this evolution seems to indicate a tendency toward subjectivation and generativity, I turn to the botnet to reflect upon the forceful return of the involuntary and a-subjective features of machinic enslavement.

The Early Stages of the Hacktivist DDoS

The first documented distributed-denial-of-service attacks for political ends date back to the mid-1990s, when artists and activists based in Italy began exploring the possibility of using the web as a platform for coordinating and *enacting* political protest at a global level.[1] In December 1995, the Italian hacktivist group Strano Network organized the first global netstrike to protest the French government's nuclear experiments at the Moruroa atoll in Polynesia.[2] Broadly publicized through international listservs and activist networks such as ECN and nettime, the netstrike targeted a list of ten websites, including the French Ministry of Foreign Affairs, the Ministry of Economy, and the Paris-based Nuclear Energy Agency. On 21 December 1995, internet activists from all over the world simultaneously connected to the websites for an hour and manually reloaded their pages, slowing their operations down and making some of them unavailable for a few minutes (Di Corinto and

Tozzi, 2002). The experiment was repeated in support of the Zapatista struggle in Chiapas, Mexico, and for a variety of political causes in the following years.

It is worth noting that this kind of distributed-denial-of-service attack is the most basic form of cyberprotest and does not require advanced technical skills. Since the users have to perform the repetitive task of manually reloading a target URL over and over, the emphasis shifts from the DDoS' technical efficiency to the organizational efforts that go into its preparation. As Tommaso Tozzi points out, 'the netstrike event is a symbolic act and whether the [target] website is effectively blocked has practically no value. What matters lies elsewhere: raising awareness among the largest number of people on key issues' (Tozzi, 2001). From this perspective, it is no surprise that the language used to publicize early political DDoSs was borrowed from traditional forms of activism. Indeed, the very term netstrike was initially meant to denote an internet analog to a workers' strike. Likewise, the synonymous 'virtual sit-in' – an expression that was popularized by the Electronic Disturbance Theater in the late 1990s – extended a well-known tactic of civil disobedience like the street blockade to the electronic realm.

If these metaphors may obfuscate the technical dimension of the DDoS, they are effective in translating a disembodied and solitary gesture such as the manual reload of a webpage into a collective act of resistance. Tim Jordan and Paul Taylor use the expression 'mass action hacktivism' to describe this 'combination of politics and inefficient technology' which attempts to defy 'the lack of physicality in online life, in favour of a mass collection of virtual bodies that are yet not present to each other' (2004: 69). In order to fill this gap between online and offline presence, electronic and embodied selves, code and natural language, the hacktivists of the 1990s often recurred to an evocative and performative language. For example, Electronic Disturbance Theater co-founder Ricardo Dominguez describes the virtual sit-ins organized by his group as a new kind of drama whose often unknowing actors include hackers, artists and activists, administrators of target websites, the media, and the cyber-police. This 'invisible theater' was meant to function as the *simulation* of a physical attack that operated between the syntax of computer code and natural language, operational disturbance and the symbolic amplification of such disturbance (Dominguez, 2003).

The Electronic Disturbance Theater (EDT) performed such disturbance by coding and releasing the Zapatista FloodNet, a software that could be pointed to a target URL and easily executed by a web browser. Launched in 1998, the FloodNet inaugurated a new phase in the hacktivist DDoS in that it automated the webpage reload, thereby freeing its users from the need of manually reloading the target website. Indeed, as Dominguez notes, with the FloodNet activists could theoretically leave their computers 'protesting at home and then hit the streets to do the

same' (2009: 1810). In this way, *FloodNet required the users to consent to the action only at the moment of launching the application*. Then they could forget about it and turn to other activities while their machines kept working on their behalf. By contrast, with the manual reload, the hacktivists *had to constantly renew their remote presence* by hitting over and over again the browser's reload button.

Further, FloodNet introduced another important discontinuity with early netstrikes. The EDT's first virtual sit-ins made the software executable through a web server, without the need for users to download it and install it on their machines. While this move made the action more user friendly, it also centralized the originating point of the attack. By connecting to a webpage hosting the FloodNet, the participants in the virtual sit-in entrusted the EDT with special privileges. These included the right to shut down the protest at any time, to redirect it onto other websites, and to keep track of the participants' physical location by having access to their IP numbers. To be sure, the more technically skilled hacktivists could still cloak their IP address. Yet the EDT provided no instructions on how to do it as EDT members openly used their names in conjunction with their actions so as to establish the virtual sit-in as a public and thus legitimate form of dissent.

Another unintended consequence of the centralization of the attack was that the protesters' network had now a point of vulnerability, which exposed it to possible retaliations. Such vulnerability became apparent when the EDT launched Swarm, a virtual sit-in that was meant to jam the websites of the Mexican president, the Pentagon, and the Frankfurt Stock Exchange in support of the Mexican Zapatistas. Announced and coordinated from the Ars Electronica Festival in 1998, Swarm met the unexpected response of the Pentagon, which defended its own servers by installing a 'hostile applet' on many of its webpages. The applet deflected the FloodNet's requests back onto The Thing, a small New York-based ISP that was hosting the FloodNet. As a result, many participants saw their web browsers crash. This technical failure prompted the hacktivists to organize the ensuing virtual sit-ins without relying on a centralized web server. Further, on 31 December 1999, the EDT released the FloodNet's source code, which allowed for the development of derivative versions of the applet by other hacktivist groups.[3]

In sum, the shift from the netstrikes of the mid-1990s to the virtual sit-ins of the late 1990s freed participants from the manual reload, allowing them to engage in a range of activities such as attending online meetings, writing press releases, recruiting other activists, testing the efficacy of attack tools, talking to journalists, and so forth. In this sense, we can say that such automation marked a shift from machinic enslavement to subjectivation. At the same time, enslavement persisted as an a-signifying process in that even though the hacktivists did not have to manually reload a website, their machines' synchronized participation was still

essential to the functioning of the DDoS. Furthermore, enslavement initially coexisted with subjection as the first centralized distributed-denial-of-service attacks turned participants into willing components of a machine whose control was ultimately in the hands of a single group of hacktivists. And yet, the post-Ars Electronica decentralization and the release of the FloodNet source code allowed for a generative proliferation of hacktivist tools, which coexisted with the subjectivation described above. This means that the hacktivist DDoSs of the late 1990s evolved from enslavement and subjection to generativity and subjectivation. On the signifying axis subjection-subjectivation, this development describes a tendency towards a multiplication of independent groups that espouse the ethos and practice of electronic civil disobedience. On the a-signifying axis enslavement-generativity, the collaborative development of software tools also points in the direction of a proliferation of spontaneous initiatives.

At the same time, enslavement was never entirely transcended. This is particularly clear if we consider that the FloodNet was designed to perform a highly specialized task. While the automated reloading freed time for human subjectivation, the generativity of this tool remained necessarily limited. As Simondon points out, 'in order to make a machine automatic, it is necessary to sacrifice many of its functional possibilities and many of its possible uses' (1958: 11). In this respect, the machinic enslavement of a FloodNet-based DDoS implies a coupling between humans and machines in which the latter are denied any autonomy and reduced to the status of tools. While until the late 1990s this instrumental use of software appears to be in the service of a willful human politics, beginning in the early 2000s, the growing centrality of botnets to cyberwar poses the political problem of weapons that operate beyond the human experiential domain and yet in a broader coupling with human desire.

The Botnet as a Desiring-Machine

In early February 2000, the websites of Yahoo, CNN, Amazon, eBay, E*Trade and Dell came to a grinding halt for several hours, spreading panic across the internet. Two months later, the Royal Canadian Mounted Police arrested Michael Calce *aka* Mafiaboy, a 15-year-old boy from the West Island of Montreal. Over the previous months, Mafiaboy had been hacking into the computer networks of several US universities and seizing control of them. Then, using Trinoo – an attack tool that allows an intruder to exploit networks of compromised computers to send bogus requests to an IP address – he had launched a massive distributed-denial-of-service against Yahoo and several other high-profile websites.[4] Galvanized by the fame acquired within the black hat hacking community, Mafiaboy had continued DDoS-ing

other high-profile websites, inflicting an estimated combined loss of $1.2 billion on some of the most powerful internet companies of the time (Calce and Silverman, 2008).

Mafiaboy's exploit was remarkable not because of his mastermind technical abilities, which were average, but because it exposed the vulnerability of the internet. While the massive DDoS attack against Yahoo may have not been powerful enough to overwhelm the internet's main routers, at speeds higher than 1 gigabit per second it was powerful enough to knock down the routers of the largest search engine of the time. In this way, the incident brought to the world's attention the existence of a vast shadowy infrastructure of infected 'zombie' computers that are remotely controlled by 'botmasters' through obfuscated command-and-control servers. Because botnets are usually invisible to the users whose machines have been compromised by malware, they can be employed for a wide range of activities. These may include delivering spam, stealing financial credentials from internet users, extorting money from companies by preventing customers from accessing their websites, and taking offline the websites of governments and NGOs. From this point of view, botnets appear as neutral resources whose economic or political function is ultimately determined by their mode of use.

This instrumental reading, however, tells only one part of the story. Although they are ultimately controlled by humans, botnets display a high degree of autonomy and cooperation between their human and nonhuman components (Van der Wagen and Pieters, 2015). Botnets have in fact a political economy of their own as they are routinely rented out to spammers and DDoS-ers at a price that depends on the botnet's efficiency and capability, that is, on the number of infected computers and their geographical location (Stone-Gross et al., 2011). Furthermore, because bots can be detected and neutralized by antivirus software and anti-spam filters, the botmaster (or botherder) has to frequently replenish her loads supplies (or payloads) as well as ensure that the command-and-control servers are obfuscated and can quickly migrate when detected. Hence, botnets are dynamic assemblages whose composition, performance and value depend on numerous factors – including their fast-evolving topology, their ability to handle diversified tasks, their owners' purchasing power, the demand for DDoS and spam services, the market price of payloads, the techno-legal power accorded to anti-spam firms within a given jurisdiction, and the competition of concurrent botnets.

The more resilient botnets constantly evolve so as to avoid detection, maintain a positive balance between gained and lost bots, and outpace the competition (Wagenaar, 2012). Whereas the first botnets were programmed in a centralized fashion so that the bots were controlled only by the command-and-control server, second-generation botnets like Storm, Sality, ZeroAccess, and Zeus embed a peer-to-peer architecture that

turns every bot into a server that can handle instructions to other bots (Rossow et al., 2013). Thus, on the one hand, peer-to-peer botnets are much more resilient to takedown and can more easily expand their infrastructure against competitors. On the other hand, this flexibility allows the botherders to diversify, segment, and rent out the botnet piece by piece (Brunton, 2013: 182). From this angle, botnets are not merely tools. Rather, if these nonhuman operators have become a staple of the internet it is because they have been able to incorporate the most resilient software of their time in order to reproduce themselves.

This autopoietic nature of the botnet suggests that the herding of zombie computers is less a form of subjective control than the expression of the a-signifying and affective features of machinic enslavement discussed above. For every infected computer there is an internet user who partakes in the information exchange that turns his machine into a productive component of the botnet. While some media theorists have attributed the uncontrolled proliferation of worms, spam and spyware to the exponential growth of a largely illiterate population of internet users (Zittrain, 2008), my wager is that these users often *seek* and *enjoy* free and unregulated forms of exchange that expose their computers to security risks. And even when they do not enjoy such exchanges, the users play an active role in turning over their computers to the botnet as they click on infected email attachments, malicious links, or compromised banner ads. In other words, the botnet does not directly control the user's desire – only the processing power of machines that have been infected *because* of their users' desires. The botnet quietly brings this libido under control and employs it machinically for its own ends.

Thus, keeping in mind that Deleuze and Guattari see *desire as* a *process of production that cuts across the human and the nonhuman*, we can think of the botnet as a 'desiring-machine', that is, as a machine that is both coupled to flows produced by other machines (the internet users' desires as mediated by the network) and a machine that produces its own flows (spam deliveries, DDoS attacks, identity thefts, network takeovers, and so on). The libidinal flows produced by the botnets function in turn as inputs for the monitoring activities of anti-spam and security firms, which record and tell apart legitimate network communications from illegitimate ones. Thus if botnets connect and synchronize libidinal flows, anti-spam filters disjunct and separate botnet-generated flows from the undifferentiated dataflow of internet traffic.

The Transductive Botnet

As we have seen, the conjunctive and the disjunctive logics that are simultaneously at work in this arms race have a counterpart at the level of political economy, where the botnet appears both as a productive and an anti-productive machine. The botnet is productive in that in order to

provide valuable services on the black market, it has to be maintained and profitably rented. But it is also anti-productive in that its operations inflict huge economic losses on companies and end users on a daily basis. For example, it has been estimated that the email spam handled by botnets is a negative externality that costs the net economy 100 times as much as what it generates for the spam industry (Rao and Reiley, 2010).

Thus the botnet is not merely a tool that is developed by a political community to achieve specific objectives – as in the case of FloodNet and its derivative versions – but a machine that has a logic of its own. Following Simondon (1989), we might describe this logic as 'transductive,' that is, as an operation that progressively structures a domain that is filled with potentials, or in a state of 'metastable equilibrium'. The transductive operation, argues Simondon, coincides with a transition phase whereby the dimensions of a domain emerge as correlated and in tension with one another. From this perspective, the botnet's transduction is the common operation of two heterogeneous realities: internet users' desire to access and exchange information and the power of distributed computing and connectivity. These two poles converge in a metastable system that keeps individuating itself as the botnet undergoes different transition phases. Simondon's theory of individuation presupposes in fact 'a primacy of processes of becoming over the states of being through which they pass' (Massumi, 2012: 20).

As Deleuze points out in a short text on Simondon, 'what essentially defines a metastable system is the existence of a 'disparation', the existence of at least two different dimensions, two disparate levels of reality, between which there is not yet any interactive communication' (2004: 87). The botnet establishes this interactive communication (or transduction) between its human and nonhuman components in two steps: first by capturing libidinal flows through the viral propagation of malware and then by putting to work the machinized flows as the bots are delivered instructions by the command-and-control server. As previously noted, the centralized architecture of early botnets has been increasingly integrated with peer-to-peer protocols that allow the bots to handle each other's instructions without having to rely on human input. The machinic intertwining of the human and the automated components of the botnet is also evident from the fact that tracking down a botmaster may not be sufficient to take down a botnet. In fact, law enforcement agencies have to simultaneously neutralize human and technological actors if they want to prevent the botnet from reorganizing itself (Van der Wagen and Pieters, 2015).

The botnet's versatility and capacity to evolve by coupling human and nonhuman actors (Latour, 1994, 2005) make it, in Simondonian terms, a machine with a high degree of technicity. According to Simondon, this kind of machine 'possesses a certain margin of indetermination' that

makes it 'sensitive to external information' (1958: 11). It is worth noting that for Simondon the openness of the machine is not for its own sake. Rather, this indetermination 'assumes the human as permanent organizer, as living interpreter of machines in their relations with one another' (1958: 11). On the one hand, as Muriel Combes notes, 'this concern for the correlation of technical beings in relation to one another is what must lead humans to distance themselves from simple considerations of the utility of technical beings' (2013: 60). On the other hand, the ethical commitment to the reticular mode of being of technical objects does not imply that what Simondon called the 'psychic and collective individuation' is subordinated to their evolution (Combes, 2013: 68). Rather, human beings develop an inventive and nonalienated relationship to technical objects by exploring their margin of indetermination *as they open themselves up to their own indetermination to share their problematic with other beings*.

Perhaps it is no accident that botnets make their appearance in contemporary hacktivism with Anonymous, a form of affiliation whose very name is a hallmark of indetermination. In September 2010, Anonymous – a loose network of internet activists and hackers who defend the right to free speech and unfettered access to information and information technologies – began to make use of botnets to target pro-intellectual property organizations such as the MPAA and the RIAA in solidarity with file sharing sites like The Pirate Bay (Coleman, 2014: 92–9). In December 2010, a large portion of the Anonymous network decided to target PayPal in support of Wikileaks. What makes this hacktivist DDoS particularly significant for the purpose of this article is that in this circumstance a conscious action of civil disobedience overlapped, if only for a few hours, with an automated DDoS executed by botnets.

The DDoS on PayPal

In early December 2010, Anonymous launched one of the largest distributed-denial-of-service attacks in the history of the internet. Coordinating via the IRC network AnonOps, Anonymous decided to target and disable the websites of three major finance companies: Visa, Mastercard and PayPal. The hacktivists held these companies responsible for cutting their finance services to whistleblower website Wikileaks, which had released in late November 2010 a first batch of 220 US State Department diplomatic cables, as part of the world's largest leak of classified material in history. On 6–8 December 2010 thousands of Anonymous affiliates knocked offline for several hours the websites Visa.com and Mastercard.com and put under great pressure the servers of PayPal. The 8 December DDoS on Paypal.com required the mobilization of a large number of human and technical resources. In fact, unlike Visa.com and Mastercard.com, Paypal.com relies on a large

system of distributed servers (CDN) that process millions of financial transactions on a daily basis.

To execute the attacks, the hacktivists relied on an infrastructure made of two primary components: the AnonOps chat network for remote coordination of the actions and DDoS software to overflow the target websites with an excessive number of requests. The DDoS software consisted in turn of two main components: an open source application called the Low Orbit Ion Cannon and two botnets, also operated via IRC, by two botmasters. The Low Orbit Ion Cannon, or LOIC, is a tool that had originally been developed by an open source programmer as a server-stressing tool and then further developed and made available for download through open source sites such as Github and SourceForge. As Molly Sauter points out, the widespread use of these development community websites meant that '[the LOIC projects] were far more social in their development and distribution than FloodNet' (2014: 117).

If LOIC embedded the generative features of open source software, similar to FloodNet its effectiveness was only proportional to the cumulative number of its users. By contrast, as we have seen, the botnet is a network of thousands of zombie computers that is typically managed by a single operator without the knowledge and consent of those whose machines have been infected. In spite of these differences, the LOIC and the botnets presented few striking similarities. In particular, in September 2010, a new 'HiveMind' feature had been added to the Windows version of LOIC so that users could let the operator of an Internet Relay Chat (IRC) channel set their clients on a target and control them remotely at once (Constantin, 2010). Such synchronization made the LOIC resemble a botnet as botnets are also typically operated via IRC channels.[5] In fact, a botnet operator can visualize a list of all the available zombies in an IRC channel exactly in the same way as 'BillOReilly' – the operator of the #loic channel on AnonOps – could visualize a list of the LOIC clients set in the HiveMind mode for the attack on PayPal (Olson, 2012: 115). Such technical convergence was maximized by the fact that at least two botmasters used private IRC channels on AnonOps for controlling their zombie machines. Thus, meeting in a restricted IRC channel named #command, the AnonOps operators and the botmasters determined that for attacking Visa, PayPal and Mastercard they could rely on the combined power of few hundred LOIC clients (synchronized in the HiveMind mode) and roughly 30,000 zombie machines controlled by the botmasters.[6]

Such firepower was barely sufficient to take offline PayPal's content delivery network. It is to be noted that with the exception of a dozen organizers meeting in #command, the LOIC users were completely unaware that the botnets contributed about 95% to the total firepower of the distributed-denial-of-service. Yet, according to investigative reporter

Parmy Olson, this lack of transparency was not considered problematic by the core organizers of the DDoS:

> The upper tier of operators and botnet masters . . . did not see themselves as being manipulative. This is partly because they did not distinguish the hive of real people using LOIC from the hive of infected computers in a botnet. In the end they were all just numbers to them, the source added. If there weren't enough computers overall, the organizers just added more, and it didn't matter if they were zombie computers or real volunteers. (pp. 120–1)

If from the standpoint of the DDoS' technical efficiency the distinction between zombie computers and real volunteers might be inconspicuous, from an ethical and political standpoint it is certainly not – for at least two distinct reasons.

On a first level, the LOIC users participated in a distributed-denial-of-service attack that was coordinated by a handful of hacktivists who recurred to 'secret weapons' without informing the rest of the participants. If the DDoS attack was seen by many Anonymous affiliates (often referred to as 'Anons') as a direct and horizontal way of expressing collective support for Wikileaks, the very existence of an 'upper tier of operators and botnet masters' defeated the notion that all Anons participated in the action on an equal footing. Indeed, the AnonOps administrators and channel operators already owned special privileges that allowed them to monitor the chats, kick and ban selected users, and even shut down the entire chat network. Further, if the botmasters withdrew from the action, this was likely to fail as the LOIC users were unable to form by themselves the critical mass necessary to take PayPal offline. In other words, the needs of cyberwarfare had created a techno-elite whose power sharply contrasted with Anonymous' purportedly horizontal structure and democratic decision-making processes.

On a second level, the employment of botnets meant that the vast majority of the machines used for the distributed-denial-of-service were operated without user consent. In fact, zombie computers lack by definition the kind of consciousness and intentionality that is meant to underpin human politics. This does not mean that these machines do not have political agency. Rather, as we have seen, this agency cannot be understood from the perspective of an anthropocentric politics. For example, on the same days as Anonymous employed botnets in support of Wikileaks, networks of infected machines were used against the AnonOps IRC servers and the Wikileaks website by their opponents.[7] Because, as we have seen, botnets are usually rented out, it is entirely possible that the same infected computers participated in DDoS attacks executed by opposing parties who operated them at different times.

To sum up, on the one hand, the rise of Anonymous and the cooperative development of the LOIC express the combination of subjectivation and generativity that we have already encountered in the post-Ars Electronica hacktivist DDoS. And yet, the emergence of a techno-elite within Anonymous and the use of botnets suggest that subjection and enslavement persist even within a form of hacktivism whose anonymity is meant to express a more egalitarian form of participation. Interestingly, these two poles appear perfectly integrated in the voluntary botnet of LOIC clients as social subjection presupposes a subject of will that is assigned a codified role within an action while machinic enslavement simply describes the concatenation of human and non-human components. Finally, the automated involuntary botnet is a form of *enslavement without subjection* as the machines that partake in the attack are run by robots that do not require user consent in order to function.

Conclusion

The fact that botnets have acquired a central function in hacktivist DDoSs suggests a fundamental shift in the status of hacktivism. If the mass action hacktivism of the mid-to-late-1990s combined grassroots activism with inefficient software so as to highlight the ethical and political dimension of its claims and objectives, the hacktivism of the Web 2.0 seems to have reversed the relationship between collective subjectivation and technological efficiency. As the number of computers that can be actually connected in a swarm is prioritized over semantic and performative tactics, the a-signifying and a-subjective features of machinic enslavement become dominant. Further, because the botnet is a machine rather than a tool, its users limit themselves to learn how to operate it.

In this sense, botnets do not require subjects but only operators in order to function. This means that the contingent uses of a botnet are less significant than a botnet's capacity to elude detection, evolve, and pose threats to critical communication infrastructures. And yet the use of botnets within hacktivist contexts should not be measured only with the yardstick of technical efficiency. Rather, the question is whether the appearance of these autopoietic machines in cyberwar can be reconciled with the ethos and purpose of hacktivism. From a Simondonian point of view, the encounter of a nonspecialized machine such as the botnet with a human collective that is deeply invested in technical culture is a highly significant event. In this respect, Anonymous may well be the name of an emerging *koiné,* a new lingua franca whereby the machines' openness to the surrounding milieu meets the human belief that defending such openness works in the service of a freer society.

To be sure, from an activist perspective such encounter is fraught with risks. To begin with, the machinization of desire expressed by botnets

disrupts the patient organizational work that informs grassroots activism – a work that requires constant mediation and the participants' active effort at leveling existing power relations (including those that derive from different levels of technical knowledge). Further, with the shift from subjectivation to enslavement that we saw at work in the distributed-denial-of-service attack on PayPal, each user was counted only for its available bandwidth. Thus, in this context, two botmasters wielded more technical (and therefore political) power than hundreds of hacktivists combined. In other words, once technical efficiency is prioritized over defining properties of the modern (liberal) subject such as choice and will, the human becomes an unknowing component of an assemblage that follows a logic of its own.

Yet from the perspective of hacking and technical invention the use of botnets is not particularly problematic as botnets exhibit the kind of versatility and longevity that specialized tools like FloodNet and LOIC utterly lack. It is the higher technicity of these machines that makes them attractive to some hackers, who experiment with them with or without the approval of the hacktivist community. Indeed in the *Note complémentaire* to *L'individuation psychique et collective*, Simondon argues that technical invention 'institutes a transindividual relation, proceeding from individual to individual without passing through the communitarian integration that is guaranteed by a collective mythology' (1989: 266). Thus, on the one hand, this transindividual relation allows the individual to access the preindividual and 'inject his excess in the social by the mediation of the technical object' (Toscano, 2007) rather than through a shared political narrative. On the other hand, accessing the metastability of preindividual reality via the reticularity of the technical world implies a shift in the status of the subject from 'a centripetal agent' to 'a distributed subjectivity closely attuned to the sensory affordances of the environment' (Hansen, 2012: 47).

Anonymous integrates these two aspects as technical invention constantly reshapes the internal organization of a sociotechnical assemblage whose participants willingly 'sublimate' their individual identity (Coleman, 2012) so as to keep the assemblage open to the information environment and to many potential couplings. Indeed, as I have argued elsewhere, Anonymous is an 'improper name' that combines heterogeneous processes of subjectivation such as the individualist pseudonymous reputation economy of the hacker world and the collectivism of social movements (Deseriis, 2015). Thus, in shuttling between individualizing technical contributions that keep the technical object open to its becoming and grassroots activism, Anonymous reverses the terms of early hacktivist practices. In other words, it is no longer a matter of identifying a political problem, a power structure, an injustice, and *then* finding an adequate technical solution to organize a resistance. Rather, closed and hierarchical power structures

are likely to collide with a *sociotechnical assemblage that has identified the margin of indetermination of machines and living beings alike as its ontological ground and terrain of struggle*.

In this respect, Simondon's ontogenesis allows us to consider the question of hacktivism from a truly monistic angle. Whereas Deleuze and Guattari's distinction between subjection and enslavement is still predicated upon the notion that a subject may exist as a self-contained, 'molar' entity, the notion of transindividuality presupposes instead a subject that in being *more than itself* can access the collective via the metastability of the technical object. From this angle, the hacktivist DDoS is a transductive operation only insofar as the poles of hacking and activism do not stand in an instrumental relationship to one another – i.e. the activists do not need the hackers to make their political action more effective and the hackers do not need the activists to prove their superior technical knowledge. Rather, within the hacktivist transduction, hackers and activists coevolve in a process that is indissolubly social and technical and in which the notion of political will is rethought vis-à-vis a networked infrastructure that increasingly determines the conditions of its exercise. Far from being value-neutral, such infrastructure carries within itself unfulfilled potentials that are constantly actualized by the inventive and organizational capacities of the connected many.

From this point of view, asking whether a technology is useful to achieve an objective is less important than asking whether it has a high degree of technicity, that is, whether it is truly open to its becoming. Whereas the Free and Open Source Software community has turned the question of openness into a foundational principle of its ethos and modus operandi, in this article I have explored a technology whose design is opaque and whose assemblage is largely a byproduct of involuntary actions. Instead of condemning the botnet for its dubious politics, I have suggested that its resilience may lie in the a-subjective nature of desire – understood as a production process that couples the human and the nonhuman. Following accelerationists a la Nick Land, one may be tempted to 'remove the controls' of the subject altogether and celebrate the botnet as an instance of a self-reinforcing cybernetic intensification that tends towards the absolutely nonhuman. Yet in referencing Simondon's theory of the subject I have intended to emphasize that deindividuation is only an intermediary step towards the collective individuation whereby the individual discovers itself as more-than-one, that is, as a subject open onto the infinite. Whether such discovery is pursued through an inventive technical practice and/or direct participation to collective life, these more-than-human becomings set in motion conjunctive syntheses of which the hacktivist subject is a transitory-yet-ineliminable byproduct – a subject that may no longer master its actions, but that makes experience of itself through their unpredictable outcomes.

Notes

1. Previous DDoS attacks had been mostly organized by Usenet users to retaliate against spammers for the violation of newsgroup netiquette. For example, in April 1994, Usenet users organized an email bombing campaign against a US immigration lawyer firm that had used a simple script to post the same message to roughly 6000 newsgroups. See Brunton (2013: 53–62).
2. The netstrike was conceived by internet artists Tommaso Tozzi and Stefano Sansavini. The former has run a bulletin board system called Hacker Art BBS since 1990.
3. While these derivative versions partly improved on the FloodNet's technical efficiency, they also kept emphasizing analogies between online and offline protests. In particular, groups such as the Electrohippies and the Federation of Random Action launched a series of virtual sit-ins simultaneously with the street protests organized by the alter-globalization movement in the early 2000s. In some cases, this analogy was built directly into the protest tools. For example, during the 26 September 2000 demonstrations against the World Bank in Prague, the Federation of Random Action – a group based in Southern France – and affiliate toyZtech released a chat software that enabled users to ping the IMF and World Bank's servers every time the hacktivists typed key words such as 'poverty,' 'finance,' 'investment,' and 'financial power'.
4. For a technical description of Trinoo (or trin00), see the CERT® Incident Note IN-99-07 available at: www.cert.org/incident_notes/IN-99-07.html.
5. The Internet Relay Chat, or IRC, is an internet protocol introduced in the late 1980s that facilitates real-time communication among users in textual format. Since, as Coleman notes (2012), in IRC a great deal of power is concentrated in the hands of the administrators who install, configure, and maintain the server, some IRC networks affiliated with Anonymous (such as VoxAnon) have developed a code of conduct that regulates the power of administrators. This was not the case with AnonOps, whose administrators did not share their knowledge of the secret use of botnets with the many Anons who participated in the distributed-denial-of-service attack on PayPal on a voluntary basis, exposing themselves to the risk of reprisals.
6. Olson reports that Civil and Switch employed 30,000 and 1300 zombie computers, respectively, for the DDoS on Paypal.com (2012: 117). Network security analyst Sean-Paul Correll reports that the number of computers connected in the voluntary LOIC botnet oscillated between 500 and 1700 on 7–8 December (Correll, 2010).
7. In the aftermath of the 8 December DDoS on PayPal the AnonOps IRC servers came repeatedly under attack and often became slow or inaccessible. Olson (2012: 129–30) reports that some of these attacks were orchestrated by Civil and Switch in retaliation for the lack of gratitude of their former allies. Other reports point in the direction of Aiplex Software, an Indian company that Anonymous had DDoS-ed a month earlier in support of the bittorrent site The Pirate Bay. Others indicate The Jester, a self-styled patriotic hacker who had also DDoS-ed Wikileaks.org on 28 November for 'attempting to endanger the lives of our troops', as he claimed via Twitter the same day. These reports do not necessarily contradict each other. On the contrary, they demonstrate how common the use of botnets has become in contemporary cyberwarfare.

References

Assange J, et al. (2012) *Cypherpunks: Freedom and the Future of the Internet*. New York: OR Books.

Barthélémy J-H (2012) Glossary: Fifty key terms in the work of Gilbert Simondon. In: De Boever A, et al. (eds) *Gilbert Simondon: Being and Technology*. Edinburgh: Edinburgh University Press, pp. 203–231.

Brunton F (2013) *Spam: A Shadow History of the Internet*. Cambridge, MA: MIT Press.

Calce M and Silverman C (2008) *Mafiaboy: How I Cracked the Internet and Why It's Still Broken*. New York: Penguin.

Chopra S and Dexter S (2008) *Decoding Liberation: The Promise of Free and Open Source Software*. London: Routledge.

Coleman G (2012) Our weirdness is free: The logic of Anonymous – online army, agent of chaos, and seeker of justice. *TripleCanopy*. Available at: http://canopycanopycanopy.com/contents/our_weirdness_is_free (accessed September 2014).

Coleman G (2013) *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton, NJ: Princeton University Press.

Coleman G (2014) *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London: Verso.

Combes M (2013) *Gilbert Simondon and the Philosophy of the Transindividual,* trans. LaMarre T. Cambridge, MA: MIT Press.

Constantin L (2010) Anonymous DDoS tool gets botnet capabilities. *Softpedia*, 27 September. Available at: http://news.softpedia.com/news/Anonymous-DDoS-Tool-Gets-Botnet-Capabilities-158163.shtml (accessed April 2014).

Correll S (2010) Tis the season of DDoS – Wikileaks edition. *PandaLabs blog*, 4–15 December. Available at: http://pandalabs.pandasecurity.com/tis-the-season-of-ddos-wikileaks-edition (accessed April 2014).

Deleuze G (2004) On Gilbert Simondon. In: *Desert Islands and Other Texts 1954–72*, trans. Taormina M. Los Angeles: Semiotext(e), pp. 86–89.

Deleuze G and Guattari F (1983) *Anti-Oedipus: Capitalism and Schizophrenia,* trans. Hurley R et al. Minneapolis: University of Minnesota Press.

Deleuze G and Guattari F (1987) *A Thousand Plateaus: Capitalism and Schizophrenia,* trans. Massumi B. Minneapolis: University of Minnesota Press.

Deseriis M (2015) *Improper Names: Collective Pseudonyms from the Luddites to Anonymous*. Minneapolis: University of Minnesota Press.

Deseriis M and Marano G (2008) *Net.Art: L'arte della connessione*. Milan: Shake.

Di Corinto A and Tozzi T (2002) *Hacktivism. La libertà nelle maglie della rete*. Rome: Manifestolibri.

Dominguez R (2003) Illegal knowledge? Strategies for new media activism. *Electronic Book Review*, 30 July. Available at: www.electronicbookreview.com/thread/technocapitalism/mediactive (accessed April 2014).

Dominguez R (2009) Inventing the future of online agitprop theater. *Proceedings of the Modern Language Association of America* 124(5): 1806–12.

Galloway A (2004) *Protocol: How Control Exists After Decentralization*. Cambridge, MA: MIT Press.

Galloway A and Thacker E (2007) *The Exploit: A Theory of Networks*. Minneapolis: University of Minnesota Press.
Greenberg A (2012) *This Machine Kills Secrets: How WikiLeakers, Cypherpunks, and Hacktivists Aim to Free the World's Information*. New York: Dutton.
Hansen M (2012) Engineering pre-individual potentiality: Technics, transindividuation, and media. *SubStance* 41(3): 32–59.
Jordan T and Taylor PA (2004) *Hacktivism and Cyberwars: Rebels with a Cause?* New York: Routledge.
Kelty C (2008) *Two Bits: The Cultural Significance of Free Software*. Durham, NC: Duke University Press.
Latour B (1994) On technical mediation: Philosophy, sociology, genealogy. *Common Knowledge* 3: 29–64.
Latour B (2005) *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford: Oxford University Press.
Lazzarato M (2006) The machine, trans. O' Neill M. *Transversal*, October. Available at: http://eipcp.net/transversal/1106/lazzarato/en (accessed April 2014).
Massumi B (2012) 'Technical mentality' revisited. In: De Boever A, et al. (eds) *Gilbert Simondon: Being and Technology*. Edinburgh: Edinburgh University Press, pp. 19–36.
Olson P (2012) *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. New York: Little Brown & Co.
Parikka J and Sampson TD (eds) (2009) *The Spam Book: On Viruses, Porn, and Other Anomalies from the Dark Side of Digital Culture*. New York: Hampton Press.
Pasquinelli M (2008) *Animal Spirits: A Bestiary of the Commons*. Rotterdam: NAi Publishers/Institute of Network Cultures.
Rao J and Reiley DH (2012) The economics of spam. *The Journal of Economic Perspectives* 26(3): 87–110.
Rossow C et al. (2013) SoK: P2PWNED – Modeling and evaluating the resilience of peer-to-peer botnets. Paper presented at the 4th IEEE Symposium on Security and Privacy, San Francisco, CA, 23–24 May.
Samuel A (2004) *Hacktivism and the future of political participation*. Unpublished PhD thesis, Harvard University.
Sampson TD (2012) *Virality: Contagion Theory in the Age of Networks*. Minneapolis: University of Minnesota Press.
Sauter M (2014) *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet*. London: Bloomsbury.
Simondon G (1958) *Du mode d'existence des objets techniques* [On the mode of existence of technical objects]. Paris: Aubier.
Simondon G (1989) *L'individuation psychique et collective* [The psychic and collective individuation]. Paris: Aubier.
Stone-Gross B et al. (2011) The underground economy of spam: A botmaster's perspective of coordinating large-scale spam campaigns. Conference paper presented at the 4th USENIX Symposium on Large-Scale Exploits and Emergent Threats, Boston, MA, 29 March.
Toscano A (2007) The disparate: Politics and ontology in Simondon. Conference paper presented at the Society for European Philosophy/Forum for European Philosophy annual conference, University of Sussex, 9 September 2007.

Tozzi T (2001) Tre film: I botti di capodanno, l'arte e il netstrike [Three films: The New Year's fireworks, art and the Netstrike]. *Cut-Up* 2. Available at: www.tommasotozzi.it/index.php?title=Netstrike_(1995) (accessed April 2014).

Van der Wagen W and Pieters W (2015) From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. *British Journal of Criminology* 55(3): 578–595.

Wagenaar P (2012) *Detecting botnets using file system indicators*. Master's thesis, University of Twente, Netherlands.

Wiener N (1948) *Cybernetics: Or Control and Communication in the Animal and the Machine*. Cambridge, MA: MIT Press.

Zittrain J (2008) *The Future of the Internet – And How to Stop It*. New Haven, CT: Yale University Press.

Marco Deseriis is Assistant Professor of Media and Screen Studies at Northeastern University. His research explores cultural and political dimensions of internet-based activism, the production of new forms of subjectivity in the network society, and experimental forms of authorship. His monograph *Improper Names* (University of Minnesota Press, 2015) examines the contentious politics and struggles for control of a shared alias from the early 19th century to the age of networks. Deseriis' current research project, for which he has been awarded a Marie Curie research fellowship by the European Commission, focuses on the political values embedded in online decision-making software adopted by European 'techno-parties' such as Podemos, Five Star Movement, and the Pirate Parties.