5

ANONYMOUS, THE TRANSDUCER

> Identity. One of our most precious possessions. You believe we all have one, but you are sadly mistaken. Identity belongs only to those who are important. Those who have earned it by struggle and blood. Those who matter. You my friend, do not. Identity is a fragile and weak thing. It can be stolen or replaced. Even forgotten. Identity is a pointless thing for people like us. So why not let go of it and become Anonymous?
>
> —ANONYMOUS

The improper names discussed so far in this book have been introduced to fulfill specific aesthetic, political, and economic functions. Whether completely fictional or inspired by existing individuals, they are the offspring of human imagination, language, and communication. In this chapter, I am going to discuss the case of a shared pseudonym that displaces this exquisitely human ontology as it was originally descriptive of a software function. As the tag that marks the unsigned comments on the imageboard 4chan—an Internet forum that requires users to begin a discussion by posting an image—"Anonymous" was soon appropriated by those users to coordinate actions that require the participation of many. Thus, on one hand, Anonymous is a tag that designates an Internet user without attributes that may distinguish it from any other user. On the other hand, Anonymous functions as a collective assemblage of enunciation that entails coordination, collaboration, and intentionality.

My wager is that the problematic of Anonymous lies at the intersection of an impersonal, potentially deindividuating technology such as the imageboard and human subjectivity and will. In this chapter, I broaden this initial claim to suggest that Anonymous expresses the convergence of a technological drive toward indetermination with the human belief that open technologies are conducive to a freer society. More precisely, Anonymous emerges from the mutual constitution of these poles in a technosocial assemblage that is both techno-logically indifferent to the meaning and consequences of its actions and ethically committed to them.

I base this paradoxical claim on Gilbert Simondon's notion of transduction. Simondon introduces this concept to refer to an operation that progressively structures a physical, biological, technical, or social domain that is filled with potentials and in a state of "metastable equilibrium." The transductive operation, argues Simondon, coincides with a transition phase whereby the dimensions of such a domain emerge as correlated and in tension within a system that is unstable and incompatible with itself. Such instability (or metastability) implies that while some dimensions of the domain become individuated, others may remain in a potential state and give rise to further individuations.[1]

My claim is that Anonymous may be considered itself a metastable system that undergoes multiple individuations. In particular, I will show how Anonymous has undergone at least three transition phases since its inception around 2005. The first phase coincides with the transition from Anonymous as a default function of the imageboard 4chan to Anonymous as a collective assemblage of enunciation. Such individuation emerged from the confrontation of those who insisted on using personal identifiers in the imageboard and those who argued for complete anonymity as a more truly egalitarian mode of communication. Once Anonymous emerged as a "we," it further individuated between those who inscribed its actions within an ethical and political horizon and those who refused any moral justification for them. Finally, Anonymous underwent a third individuation as the name was contended between those who used it to denote secrecy and mastery of a superior technical knowledge and those who attached it to social movements whose politics is transparent, participatory, and nonelitist.

RAIDING *TIME* MAGAZINE

In March 2009, *Time* magazine launched its third online poll to determine the "100 Most Influential People" on the planet. If the list of candidates was filled with politicians, CEOs, spiritual leaders, scientists, and pop stars, one name stood out for its short, enigmatic quality: moot. The alias of the then twenty-one-year-old Christopher Poole, moot owed its notoriety to the Internet. More precisely, he had been catapulted to stardom by 4chan.org, an addictive Internet forum he had himself launched from his New York apartment in 2003. Thanks to a simple interface and the lack of registration, 4chan has attracted in a few years millions of users, who exchange images and short texts on subjects ranging from Japanese anime to fashion, weapons, animals, music, toys, porn, and video games. As the *god* of 4chan—as system administrators are referred to in Internet jargon—moot sits at the very top of the imageboard. Thus, when *Time* launched its poll, the 4chan users seized the opportunity to make their deity known to the rest of the world.

In selecting moot as a candidate, the editors at *Time* had overlooked an important element: 4chan users rarely play by the rules. Rather, they prefer to set their own rules for whatever game they decide to play. This is particularly true of the 4channers who hang out on /b/, the random board of 4chan.[2] Also known as /b/tards, the dwellers of this board launch calls to action and challenges that can mobilize thousands of users on a whim. In the case of the *Time* 100 poll, the /b/tards first decided that moot had to win the contest by any means necessary, and second, that that they would have inserted a secret message in the poll so as to prove that it had been manipulated. The message was to be created by ranking twenty-one selected candidates so that the initial of each first name would have spelled out the phrase "mARBLE CAKE ALSO THE GAME" (where *m* stood for "moot," *A* for "Anwar Ibrahim," *R* for "Rick Warren," and so forth).[3]

In the beginning, the challenge was made easy by the lack of any authentication software. Anyone could cast a vote simply by requesting the URL associated with a candidate. The 4channers seized this opportunity to craft automated voting software that could cast dozens and even hundreds of votes per minute. Some of these autovoters alternated votes for different candidates to avoid detection. Others cycled through different proxy servers so that the votes appeared to be coming from multiple IP addresses. Furthermore, the autovoters were often fired by unknowing Internet users through "spam URLs," which had been embedded by the /b/tards in various Internet forums.[4] If these tricks worked for a while, the *Time* staff eventually realized that something was wrong with the poll. Thus, after erasing millions of votes and restoring the poll to a previous (albeit not entirely untampered) count, they placed a reCAPTCHA authentication test on the poll.[5] As a result, although moot still maintained a comfortable lead over the other candidates, the secret message was compromised as too many votes had been cast by users who were not affiliated with 4chan.

The /b/tards first countered the staff's move by trying to break the reCAPTCHA system through ad hoc software. After several failed attempts, they realized that the only way to restore the message was to switch to manual voting.[6] In the final days of the poll, with the help of an interface that allowed them to speed up the manual input of CAPTCHAs, hundreds of volunteers were able to cast nearly two hundred thousand votes. This was still far fewer than the millions of votes produced by the autovoters in the first days of the poll but enough to restore the message. On April 27, 2009, the magazine closed the poll and announced the result. Although *Time* claimed that its staff had neutralized several attempts to hack the vote, the final ranking unequivocally showed that the contrary was true.

LULZ, TROLLS, AND THE RISE OF A-CULTURE

Even though it is very unlikely that moot would have ever earned such a prestigious title had 4chan users not hacked the vote, mARBLE CAKE ALSO THE GAME was a monument to the influence that 4chan exerted and continues to exert over Internet culture. Upon its launch in October 2003, users began flocking to the board, making it in few years the most popular U.S. Internet forum and one of the largest imageboards in the world.[7] Such popularity was due to a number of factors, including the lack of a registration process and the almost complete anonymity the forum ensures. Whereas the rise of social network sites such as MySpace, Facebook, and Twitter has produced a significant shift in online culture toward mostly known and mostly persistent online identities—that is, toward a reduction of the gap between real-life identities and online personae—4chan provides a safe haven for the experimental forms of subjectivity that had permeated the Internet cultures of the 1990s.

This is particularly true of /b/, the very first board of 4chan. If nowadays 4chan lists dozens of thematic forums, its first board was and remains dedicated to everything that does not fit into a category.[8] Because of its open and undefined nature, /b/ soon became an incubator for the experimentation of new forms of communication and subjectivity. Generating more than one-third of the entire 4chan traffic, /b/ is the source of sight gags, catchphrases, and popular Internet memes such as the LOLcats, the pedophile mascot Pedobear (a cartoon used, often ironically, to alert moderators to the presence of child pornographers), Anonymous (itself a meme), and crudely designed comics such as Rageguy and Trollface.

The latter is often associated with the presence of "trolls," an emerging class of online pranksters and troublemakers as old as the first Internet communities.[9] Whereas in the early 1990s, trolls mocked newcomers who lacked any sense of netiquette on Usenet newsgroups, in recent years, trolling has expanded to encompass a host of ethically questionable activities. These can be divided into two main families: making the life of individuals miserable and targeting online communities. In the first case, trolls' tricks range from finding the phone numbers and home addresses of specific persons to bombard them with unwanted deliveries and (threatening) phone calls to gaining unauthorized access to social media accounts to running fake blogs in the name of the target person. In the second case, trolls have been known for disrupting Listservs, multiplayer online games, blogging communities, classified boards, and even desecrating virtual memorials dedicated to missing persons.[10] By posting messages that are inflammatory, offensive, off-topic, and ultimately aimed at undermining trust among the members of an online community, trolls force the latter to introduce procedural rules that may reestablish "rational" and effective forms of cooperation and deliberation.

On /b/, however, trolling is so widespread that users—and especially new users—often wonder whether the community has any ethical foundation whatsoever. To a first-time visitor, /b/ presents itself as a barrage of shock-for-shock's sake images, flame wars, sexist and racist slurs, supposedly real "first-person accounts" of socially stigmatized behaviors, Internet drama, and other ostensibly futile message threads. David Auerbach notes that the main purpose of this "economy of offense" is to cultivate an elitist culture that reinforces the bonds among the /b/ dwellers while keeping at bay those who do not share the general libertarian mind-set.[11] To maintain and reinforce this line of demarcation, the /b/tards subject all contributions to an accelerated process of *détournement* and textual poaching.

The term that best describes the affective dimension of this semiotic composting is *lulz,* a corruption of the acronym *lol* (laugh out loud). Julien Dibbell writes that if in its strictest sense *lulz* means "laughs, jest, cheap amusement," in a broader sense it "encompasses both the furious creativity that generates /b/'s vast repertoire of memes and the rollicking subcultural intensity they inspire."[12] Gabriella Coleman adds that being a form of enjoyment and bliss that "celebrates its own raw power," the lulz is "divorced from any moral hinge."[13] The morally ambivalent character of the lulz may explain why /b/ can be simultaneously exhilarating and repulsive, illuminating and debasing, so that the user is constantly forced to ask herself whether a line should be drawn and where.

Yet every attempt to raise objections on an ethical ground is likely to attract even greater hostility. As this often cited post clarifies, /b/tards' actions and sentiments are—or should be—inspired only by the amoral force of the lulz:

> You COMPLETELY miss the point of /b/. /b/ is not Fark "oh hay guys i found a cute link ha ha." /b/ is not Slashdot's pseudo-intellectual discussion. /b/ is not LiveJournal, SuicideGirls, or HotOrNot. /b/ is a place for people to be monsters- the horrible, senseless, uncaring monsters that they really are.
>
> Tsunami owns the Asian continent and we laugh. Psychotic emo takes his sickness out on a cat and we laugh. A man rapes his granddaughter and we laugh, and ask for more. Suicide, homicide, genocide- we laugh. Racism, sexism, discrimination, xenophobia, rape, and baseless hate- we laugh. We are mindless "me-too"ism; we are irrational preference; we are pointless flamewars; we are the true face of the internet.[14]

It is worth noting that for being a "horrible, senseless, uncaring monster," the poster can properly articulate and reflect on phenomena that most truly sexist and racist individuals would probably be unable even to name. To be sure, Lisa Nakamura has pointedly noted that "the line between someone who is a racist and someone who behaves like a racist is pretty thin, especially in online discourse, where pretty much what you write is what you are."[15] And in his critique of cynical reason, Peter Sloterdijk has argued that self-awareness and cynicism often enable the kind of emotional detachment that allows individuals to engage in unethical behavior.[16] Perhaps, then, the lulz epitomizes what Franco "Bifo" Berardi has described as the lack of sensibility of a generation of digital natives that has lost "the ability to empathically understand the other and decode signs that are not codified in a binary system."[17]

In fact, the lulz is based on trolling, a technique or language game that requires unambiguous responses from other players to function. As infamous troll Andrew "Weev" Auernheimer points out, trolling "is a method, a style of rhetoric and action" that is based on the ruthless exploitation of Internet users' tendency to take themselves too seriously:[18]

> You look for someone who is full of it, a real blowhard. Then you exploit their insecurities to get an insane amount of drama, laughs and lulz. Rules would be simple: 1. Do whatever it takes to get lulz. 2. Make sure the lulz is widely distributed. This will allow for more lulz to be made. 3. The game is never over until all the lulz have been had.[19]

These rules suggest that trolling functions as positive feedback. Each action triggers a response that feeds back into the originating input, increasing the instability of a system. In this sense, the lulz is the exact opposite of a cybernetic system. If cybernetics is the ultimate science of control and negative entropy, lulz and trolling push systems toward turbulence and chaos. In this respect, the lulz is a "force which goes to the limit of what it can do, [a] force which affirms its difference, which makes its difference an object of enjoyment and affirmation."[20] At the same time, the coldly methodic character of trolling suggests that the lulz follows a *techno-logic*—a logic that embeds human as well as technical communication protocols.

We will return to the techno-logic of the lulz later in this chapter. For now, it is sufficient to note that once the lulz is understood as a destabilizing force and trolling as a noise-making technology, a purely semantic reading of offensive discourse leaves way for an analysis of its performative efficacy. Furthermore, to complicate things, in /b/, cynicism and cruelty often coexist with intimate discourse and care; /b/ can in fact host prurient revelations of dirty secrets and confessions of criminal acts, but also requests for help and advice. Yet because it is impossible to know whether these accounts are true, dramatized, or entirely fictional, belief is inextricably tied to the suspicion that self-disclosure might in fact conceal role-playing and trolling. In this sense, Auerbach is right to highlight the contiguity between 4chan and subcultures such as the sci-fi and anime fandoms, fantasy RPGs, cosplayers, and furries, which are all heavily invested in role-playing and masquerade. While the language game of these communities requires participants to leave reality behind according to specific rules, imageboards allow them to enact their fantasies in a social space that is not only removed from reality but also unpredictable and unscripted.

Auerbach sees 4chan's "economies of offense, suspicion, and unreality" as the engine of an emerging *A-culture,* which stands at odds with the reputation economy of the Web 2.0. A-culture, argues Auerbach, is offensive, cynical, and detached from reality because those who make it are not bound to any particular identity. At the same time,

> because the community is so autonomous from the real world, there is great opportunity to continually redefine one's role in it and even redefine the nature of the community itself. A-culture is a space for playing with unrestricted notions of identity and affiliation and for the establishment of a private set of in-jokes and references that come to constitute a collective memory.[21]

Such collective memory is not directly archived on 4chan. Because imageboards generate a high volume of traffic and are usually run by volunteers, they rely on a limited server capacity. This means that the older discussion threads are erased from the server to make room for the new ones. Hence the users who want to save old discussion threads have to recur to alternative archiving websites.[22] In other cases, /b/'s obsessions are duly annotated and turned into articles that are posted to satirical wikis such as Encyclopedia Dramatica (ED). Such transcription, however, is not without consequence, as ED stabilizes and therefore endows with an aura of legitimacy what would otherwise quickly fall into oblivion. While ED's layout and user-generated content resemble on a superficial level those of Wikipedia, the outcome is its polar opposite. In fact, ED has been aptly described as "Wikipedia's evil twin" for its "seemingly endless supply of twisted, shocking views on just about every major human tragedy in history."[23] Yet despite its seething satire and crude imagery, ED does not lack guidelines. But if Wikipedia contains the contributors' subjectivity by founding its editorial process on rationalist principles such as neutral point of view, verifiability, and no original research, ED's predilection for lulzy stories and Internet drama exalts on the contrary the contributors' quirkiness, irreverence, and cruelty—all qualities that besides being quintessentially subjective inevitably yield highly contested narratives.

In the previous chapter, we noted how the Luther Blissett Project (LBP) had theorized mythmaking as a cooperative and agonistic process whereby participants collaborate and sometimes clash over competing versions of a story. We have also seen how a faction of the LBP succeeded in stabilizing a version of the myth through narrative and performative closure. In the case of 4chan, ED, and other A-culture websites, such closure seems nearly impossible. This is partly due to the higher number and cultural heterogeneity of the participants and partly to the fact that trolling and the lulz subvert the community from within. To be sure, 4chan has created over time its own myths. But rather than relying on anthropomorphic storytellers, 4channers have entrusted their collective voice with a function of the software that runs the imageboard. This collective assemblage of enunciation emerged after a prolonged struggle among /b/tards over the meaning and function of anonymity in an online community.

ANONYMITY, EPHEMERALITY, CONDIVIDUALITY

Even though the *Time* 100 hack was organized by /b/ users, it was claimed and signed by Anonymous. The distinction between a /b/tard and someone who is affiliated with Anonymous can be thin, yet it is not insignificant. As previously noted, Anonymous is the tag that marks all the unidentified users who post on 4chan. Because /b/ users are not given the option to register—and are discouraged by the community to use other personal identifiers—each /b/ user *is* Anonymous as she posts on the board. To be sure, anonymous enunciation does not correspond to technical anonymity, as users can still be identified—and have been identified in a number of circumstances—through their IP numbers by the administrators of the website.[24] Yet /b/'s distinctive technoculture has emerged over time through a series of battles around the value and significance of anonymity in online discourse.

Even if anonymity is the default option, in the beginning it was not encouraged on /b/. On the contrary, moderators often nudged users to fill in the name field or identify their posts with a tripcode—a form of pseudo-registration that allows users to establish an identity without storing data on the server. As the number of 4chan users continued to climb, the ratio between anonymous users and those who relied on a pseudonym or tripcode increased. In 2005, the first flame wars erupted between the so-called namefags and tripfags on one side and the Anons on the opposite side.[25] While the former argued that only a recognizable user can take responsibility for her statements and actions, the latter believed that complete anonymity on the board ensures a more egalitarian form of communication, as posts are judged for their merit rather than a poster's reputation.

The Anons found an ally in Shii, a 4chan moderator who saw anonymity as an antidote to the vanity that characterizes pseudonymous forums. An admirer of 2chan, the largest Japanese Internet forum, Shii believed not only that registration kept away knowledgeable posters with little time on their hands but that complete anonymity enabled a more authentic social interaction.[26] As the founder of 2chan Hiroyuki Nishimura had pointed out in an interview with the *Japan Media Review* in 2003,

> if there is a user ID attached to a user, a discussion tends to become a criticizing game. On the other hand, under the anonymous system, even though your opinion/information is criticized, you don't know with whom to be upset. Also with a user ID, those who participate in the site for a long time tend to have authority, and it becomes difficult for a user to disagree with them. Under a perfectly anonymous system, you can say, "it's boring," if it is actually boring. All information is treated equally; only an accurate argument will work.[27]

In July 2005, Shii removed the name field and the possibility of using tripcodes from /b/. Forced anonymity was implemented until March 2007, then was removed and reinstated by moot several times. In the meantime, the culture of /b/ clearly shifted, with the vast majority of users now preferring complete anonymity.

It is worth noting that in the same years as the culture of anonymity became prevalent on /b/, Facebook went from a social network site accessible only to U.S. students to a service open to everyone with a valid e-mail address. Although there is no direct causal relationship between the rise of Facebook and that of 4chan, these two phenomena can be seen as interrelated. In contrast to Facebook's self-conscious reputation economy, 4chan has been described as a "place to be wrong" and "the id of the Internet."[28] These two opposite technocultures are enabled by specific software features. Facebook's functionalist interface revolves around individual profiles, counts and displays social connections, identifies the author of each action, and archives users' interactions. By contrast, imageboards do not store user credentials, let users contribute to a discussion thread without identifying themselves, and erase older messages as soon as the server capacity is reached.

This means that imageboards are characterized by the *anonymity, condividuality,* and *ephemerality* of social interaction. If anonymity constitutes the default option and the prevalent form of authorship in the imageboard, condividuality describes the process whereby discussion threads take on a life of their own. As technosemiotic assemblages, discussion threads are made of several dividual contributions that are not attributable to individuals or collectives who work on the basis of a shared vision. In fact, condividuality does not presuppose a community, only a concatenation of parts. This is precisely what enables the more generative threads to transmute into memes, which are sampled and remixed in virtue of their open and modular structures. Furthermore, the ephemeral nature of discussion threads sets in motion distinctive forms of cooperation for the production of relevance.

While Facebook measures status and influence by quantifying social relationships and social sentiment, 4chan users determine what matters for the community by replying to specific message threads. Replies can in fact refresh a thread and "bump" it to the front page, whereas the less popular threads sink to the back pages until they are erased from the server.[29] Bernstein et al. suggest that the high volume of posts combined with deletion set in motion a "powerful selection mechanic," which would explain "the site's influence on internet culture and memes."[30] In other words, /b/'s production of memes can be expressed as the ratio between the attention time spent by the community on a single thread and the competition among multiple threads to capture and retain that attention: the higher the ratio, the more likely a thread is to morph into a meme.

Bernstein et al.'s reliance on the notion of selectivity is clearly indebted to Richard Dawkins's theory of memes. In *The Selfish Gene,* the British ethologist proposes the institution of a new scientific discipline for the study of cultural evolution, which he calls *memetics.* Borrowing from evolutionary biology, Dawkins argues that in the same way as a gene is responsible for the transmission of hereditary traits in living organisms, a meme—be it an idea, a skill, or a fashion—is a "unit of imitation" whose replication and diffusion can explain cultural evolution.[31] The role of memetics would be to analyze how the intrinsic features of a meme make it more or less responsive to the selective pressures of the cultural environment. Yet memetics is not without shortcomings and has never achieved the scientific status Dawkins had hoped for it. In particular, it has been noted that by defining memes (as well as genes) as "replicators," Dawkins endows them with a virtual agency that is independent of context. "This tacitly suggests that the system in which a replicator is embedded can be treated like a passive vessel," notes Terrence Deacon.[32]

Imageboard culture shows that the opposite is true, as Internet memes emerge organically from discussion threads that are condividual modulations of an image-concept. Furthermore, Internet memes are a cultural form that is improper in character. Although to be identified as such, a meme must have recognizable features, its referents keep shifting as the meme is copied, forwarded, and remixed in different contexts. Even more, memes' dividual and punctual iterations often acquire meaning only in relation to one another. Thus, even though memeticists describe memes as discrete and bounded units, such units are never fully individuated and identical to themselves. Following Simondon, we might say that (Internet) memes are filled with potentials that become individuated at each iteration of the meme. Because the meme is more than one and not fully coincident with itself, it does not simply adapt to the selective pressures of the environment. Rather, the meme is in a coadaptive relation with the information environment; that is, it affects the environment as much as it is affected by it. In some cases, Internet memes may even stand in a *transductive* relation to the information environment; that is, they bring about the reciprocal individuation of dimensions that did not exist before.

For example, Anonymous allows for the experience of anonymity online to be named as *a shared experience.* Once anonymity becomes Anonymous, it also becomes pseudonymous. That is, it is no longer an undifferentiated or anomic social phenomenon, but something that can be mobilized and contended by different parties towards a specific goal. Thus, by providing a *minimum threshold of subjectivation,* Anonymous makes it possible to articulate a double differentiation. On the outside, it denaturalizes the reputation economy of the Web 2.0 as individuality and persistent identity appear now as related and in tension with collective individuation and ephemeral subjectivation. On the inside, the shared pseudonym enables the emergence of further individuations—or its contention among subjects who attach opposing and irreconcilable meanings to it.

ONLINE RAIDS AS A FORM OF MACHINIC PLAY

The shift from Anonymous as a simple tag to Anonymous as a collective force was not only evident from the fact that 4chan users adopting a tripcode were chastised as egomaniacs. As soon as Anonymous became a "we," it began to be used in conjunction with sudden attacks against specific individuals and organizations. Especially in the period 2005–8, these online "raids" do not seem to be inspired by anything but the personal enjoyment of their perpetrators. Beginning in 2008, however, a political wing of Anonymous emerges. First through a series of coordinated actions against the Church of Scientology, and then against governments and corporations that censor and restrict access to information and information technology, Anonymous becomes an increasingly organized and global political movement. As we shall see, this led to a schism within 4chan between those who continued to plead allegiance only to the lulz—the so-called lulzfags—and the new moralfags, who attached an ethical and political commitment to their actions.

Among the lulzy interventions of the early period, it is worth mentioning the raiding of the Habbo Hotel, a social network site for teenagers whose main hub is designed as a virtual hotel. Since 2005, rumors had spread on 4chan that the moderators of Habbo used their power to ban black avatars from the game.[33] In response, 4channers flooded the site several times, creating scores of identical black avatars sporting large afros and wearing gray business suits. In these purportedly antiracist protests, avatars formed swastika-like patterns that prevented other avatars from accessing the pool, which was declared "closed due to AIDS." As the game moderators banned the black avatars from Habbo for their disruptive behavior, they were accused of being racist. The "Pool's Closed" raid even led to the organization of a street rally in front of the headquarters of Sulake, the Finnish corporation that runs the game.

In other circumstances, raids target specific individuals, using a whole arsenal of tricks such as coordinated phone pranks, sending unwanted pizza deliveries, and publishing personal addresses, phone numbers, or credit card and social security numbers—a practice known as doxing. Among these attacks, the raid on white supremacist Hal Turner's radio show, the arrest of alleged Internet pedophile Chris Forcand, the trolling of a virtual memorial dedicated to a seventh-grader suicide named Mitchell Henderson, and the hack of the Epilepsy Foundation website provide an array of case studies that well illustrate the moral ambivalence of the lulz.

In December 2006, Anonymous began flooding with prank phone calls the radio show of white supremacist and Holocaust denier Hal Turner and took his website offline with a distributed-denial-of-service attack (DDoS), a network attack that consists in jamming a server with an excessive number of bogus requests.[34] Turner reacted by suing 4chan and four other websites for copyright infringement and financial losses presumably derived from the outage of his server but was unable to obtain a court injunction, and the case was dismissed in late 2007.[35] In the Chris Forcand case, some Anons chatted with this alleged Canadian pedophile, posing as underage girls under the pseudonym "serious"—a practice known on 4chan as pedobaiting. After Anonymous published the chat logs on the Web and forwarded them to Forcand's church, the Toronto Police Department got interested in the case and eventually arrested Forcand.[36] This episode led the press to refer to Anonymous as a group of "Internet vigilantes."

If the Habbo Hotel raids, the Hal Turner raid, and the Forcand case seemed motivated—at least superficially—by political and ethical concerns, the cases of Mitchell Henderson's suicide and the raid on the Epilepsy Foundation website left many baffled for their lurid moral implications.

Upon Henderson's tragic death in April 2006, his classmates created a virtual memorial on the social network site MySpace. The web page came to the attention of /b/ through MyDeathSpace.com, a website that collects virtual obituaries. For reasons that remain unknown, some /b/tards decided that Henderson had killed himself over a lost iPod and began trolling the memorial. In the following months, Henderson's parents were harassed by anonymous phone calls. Young callers claimed to be "Mitchell's ghost," to be calling from the cemetery and to have found his iPod, and so forth.[37]

The attack on the Epilepsy Foundation website in March 2008 also seemed characterized by a basic lack of empathy for human suffering. In this case, hackers purportedly associated with Anonymous inserted flashing animations in a support message board for people affected by epilepsy. At least one forum visitor later claimed to have experienced a seizure.[38]

Although the identity of the perpetrators of the Epilepsy Foundation raid is uncertain, some claim that the raid was organized by the amoral faction of Anonymous in response to the hacktivists who had launched a global campaign against the Church of Scientology few weeks earlier.[39] Thus, in early 2008, Anonymous no longer designates a collective assemblage of enunciation but two opposing assemblages—the so-called moralfags and the lulzfags. Given that neither of these two factions could prevent the other from identifying itself as Anonymous, the raids of this period can be seen as agonistic challenges over the mode of disposition and usage of the improper name. Even though the moralfags were also capable of lulzy actions,[40] my wager is that these challenges are a form of play whereby the community of Anonymous users began to draw internal boundaries that did not exist before.

I use the term "play" here in an ambivalent way, to indicate a creative activity that can have both constructive and destructive outcomes. Forefathers of contemporary game studies, such as Johan Huizinga and Roger Caillois, define play as a free and voluntary activity that creates a separate order from reality. Caillois acutely observes that players form a magic circle either by playing according to rules that create fictional worlds or by imitating real life in games such as children's make-believe.[41] Whether governed by rules or make-believe, for Caillois, play's creative power can have a "civilizing quality" only if it is embedded in purpose-oriented activities. In particular, the exuberant and turbulent nature of children's play tends to take a more structured form over time, as players set up conventions through the mastery of techniques and utensils, and pure expression leaves way to the pleasure of solving increasingly complicated problems.[42]

Caillois's insights are useful in thinking of 4chan raids as a unique mix of unruly forms of play and purpose-oriented activities. In fact, raids such as those on Hal Turner, Habbo, and *Time* magazine all have clearly defined objectives. This means that while trolling and role-playing permeate 4chan's economy of unreality at every level, they do not prevent

4channers from designing games of their own. Such games are rule bound as conventions emerge over time through the exchange of tips and knowhow among /b/ users—a pragmatic knowledge that is occasionally archived on websites such as ED, chanarchive, and *Know Your Meme*. Paradoxically, however, the ephemeral and antagonistic nature of raids makes them playable only within and against other (language) games. They are played within another game as raiders mimic the behavior of avatars, radio listeners, or poll respondents to gain access to a regulated environment. And they are played against such spaces as they aim at subverting their internal norms and dynamic.

Perhaps, then, 4chan raids can be described as a form of *machinic play*—a concept that encapsulates both the ability to subvert the rules of technosocial machines that have been engineered to do something else and the acquisition of pragmatic skills that enable the development of new machines and new language games. Bringing together some of the concepts developed so far in this chapter, we may define online raids as a form of play predicated upon five distinctive features:

1. *Antagonism*. As sudden assaults on a website, forum, game, show, or individual, raids aim at dismantling a structured space. Likewise, in its "pure form," play is an unruly and confrontational activity that bubbles up from common concerns about freedom to move.
2. *Anonymity*. The primary function of an online raid is to mobilize communities that have a strong anti-individualistic ethos and forcefully deny the reputation economy of the Web 2.0. Play knows nothing of names and reputations, as it is only concerned with the production of its own becoming.
3. *Transitivity*. In an online raid, players act as uninvited guests or spoilers in other "magic circles." This means that machinic play is not only self-referential and internal to an assemblage but is the line of flight that opens up the assemblage to other assemblages.
4. *Ephemerality*. Raids are characterized by their unpredictable and nomadic quality. As both Huizinga and Caillois point out, play cannot structure itself in a game with fixed rules without ceasing to be play.
5. *Pragmaticity*. Ephemerality does not mean that a technical, aesthetic,

> and political knowledge cannot be handed down. Through repetition and the mastery of techniques, play calls forth a practical knowledge that invokes its own rules. Yet such knowledge remains productive only insofar as it keeps privileging the virtual over the actual, difference over repetition, invention over normativity.

As we shall see in the next section, the emergence of a political wing of Anonymous was bound to accentuate this tendency toward the creation of organized forms of play by incorporating the raid into structured operations and long-term campaigns. Such operations were going to be informed by broad ethical principles that were shared by most Anons. These included the renunciation of personal publicity (a practice shamed as "namefagging"), a refusal to attack the media, and an unyielding commitment to exposing the secrets of those in positions of authority.

FROM THE LULZ TO SERIOUS BUSINESS

On January 15, 2008, the news website Gawker published an internal promotional video of the Church of Scientology titled "The Cruise Indoctrination Video Scientology Tried to Suppress."[43] In it, a wide-eyed Tom Cruise professes his faith in the futuristic religion created by science-fiction writer L. Ron Hubbard in the 1950s. Mixing omnipotent statements ("We are the authorities in getting people off drugs. We are the authorities on the mind. . . . We are the way to happiness, we can bring peace and unite cultures") with an absolute belief in the technology, writings, and policies of the founder, Cruise's strange monologue became an immediate sensation.[44] Contributing to its popularity was not only the actor's celebrity status but the knowledge that the whistleblowers who had leaked the video—many of whom were former Scientologists—had encountered difficulties releasing it. Since Scientology is known for aggressively pursuing anyone who makes an unauthorized use of its materials, several news organizations that had received the video had backed down, until Nick Denton, the founder of Gawker, decided to publish it.

By the evening of the same day, /b/tards were discussing the possibility of organizing a raid against Scientology. The original post that launched the discussion thread read,

> I think it's time for /b/ to do something big.
>
> People need to understand not to fuck with /b/, and talk about nothing for ten minutes, and expect people to give their money to an organization that makes absolutely no fucking sense.
>
> I'm talking about "hacking" or "taking down" the official Scientology website.
>
> It's time to use our resources to do something we believe is right.
>
> It's time to do something big again, /b/.[45]

Even though many initially doubted that 4chan had the capacity to take on a well-funded organization such as Scientology, it soon became clear that the support and enthusiasm for taking action exceeded by far any prior raid. In the matter of few days, Project Chanology—a pormanteau of "4chan" and "Scientology"—was born and quickly spread to other boards, such as 711chan, eBaum, and YTMND.

The first actions unfolded along rehearsed patterns, such as a series of DDoS attacks against the Scientology servers, prank phone calls at the Dianetics hotline, and the transmission of black faxes to dry up print cartridges. More interestingly, the participation of thousands of users required a whole new level of coordination that could not be sustained only through imageboards. Since 2007, some Anons had begun setting up Partyvan, a network of Internet Relay Chats that had precisely the function of connecting users of different imageboards. Because of its flexibility, the IRC protocol enables the creation of multiple text-based chats that users can easily join by creating a handle. The Project Chanology IRC channels included #xenu and #target for general discussion, #press for announcements and press releases, and #raids for the coordination of specific actions.

On January 21, the Anons in #press uploaded a short video clip to YouTube. One of the better known documents produced by Anonymous ever since, "Message to Scientology," showed footage of ominous clouds brushing a desolated industrial landscape. After threatening to destroy and expel the Church from the Internet ("for the good of your followers, the good of mankind—for the laughs"), a robotic, computer-generated voice continues:

> We cannot die; we are forever. We're getting bigger every day—and solely by the force of our ideas, malicious and hostile as they often

> are. If you want another name for your opponent, then call us Legion, for we are many.[46]

Appropriating a passage from the New Testament in which Jesus encounters and exorcises a man possessed by the evil spirit Legion ("My name is Legion: for we are many"), Anonymous links its own "immortality" to the numeric force of its army—a rhetorical strategy that had also been adopted by the Luddites. But rather than threatening the physical destruction of machinery, Anonymous claims to draw its power from its ability to become a signifier for every form of revolt. In the last passage of the message, Anonymous identifies with the so-called SPs, an acronym that in Scientology's jargon stands for "suppressive persons"—that is, antisocial individuals and former insiders who turn against the Church:

> We are your SPs. Gradually as we merge our pulse with that of your "Church," the suppression of your followers will become increasingly difficult to maintain. Believers will wake, and see that salvation has no price. . . . Yes, we are SPs. But the sum of suppression we could ever muster is eclipsed by that of the RTC. Knowledge is free. We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.[47]

Thus Anonymous embodies both a Christian demon that is multiple and the plurality of the enemies of Scientology (the SPs). At the same time, Anonymous claims to be a collective entity, a "we" that unifies or at least brings in relation with one another these multiple constituencies. In the introduction to this book, I used Deleuze and Guattari's concept of the collective assemblage of enunciation to describe a nonreferential and noncausal mode of connecting signs and actions, language and praxis. I have also argued that the Luddite movement was an assemblage in which threatening discourse (language) was linked to yet relatively independent from the destruction of machinery (praxis).

Likewise, "A Message to Scientology" inaugurated Anonymous's praxis of announcing operations by means of YouTube videos. Whether such announcements are actually followed by concrete actions is less relevant than their performative ability to engender reality effects. For example, the immediate popularity of the video drove thousands of users to Partyvan, which collapsed for the excessive traffic immediately after. As soon as the network was restored by the Partyvan administrators, the Anons in #press created the channel #marblecake, which became an organizational hub for the entire project. In this restricted IRC channel, the decision was made to take the protest from the Internet to the streets.[48] By dividing up the network into city-based channels, the organizers were able to both unclog the main Partyvan channels and facilitate the formation of affinity groups based on physical contiguity (something that contradicted A-culture's supposed autonomy from real-life relationships).

On February 10, 2008, an estimated seven thousand demonstrators staged simultaneous protests against the Church in more than one hundred cities across the globe. The protesters sported masks resembling Guy Fawkes, a seventeenth-century British revolutionary turned into a pop culture icon by the 2006 Hollywood movie *V for Vendetta* and then transformed into a 4chan meme associated with epic failure.[49] Holding up signs that read "Religion Is Free $cientology Is Neither," "Scientology=Epic Fail," and "Don't Worry We Are From the Internet," the protesters denounced the Church's manipulative practices and the intimidation of former affiliates. A second wave of street protests took place on March 15, with participation matching or exceeding that of the previous month. As the Anons forged bonds with older generations of anti-Scientology activists, international days of protest continued to be held in the following months, tapering off only in the summer. What had begun as an online protest organized by a largely apolitical and recreational social network had morphed into a full-fledged global activist campaign.

Although there are many reasons for such a rapid twist of events, it is worth noting that the conflict between Scientology and Anonymous was not entirely new. Project Chanology was in fact the latest iteration of a long-running war between the Church and the Internet, which had begun in the mid-1990s when dissenters had leaked some of Scientology's most secret texts onto the Usenet newsgroup alt.religion.scientology. If Scientology had failed at suppressing the circulation of those texts at the time, it was not more successful with the Tom Cruise video. In both cases, the Church's attempt to enforce its IP rights had clashed with the cyberlibertarian ethos that is prevalent among geeks and hackers. As Coleman points out, the conflict between Anonymous and Scientology is rooted in the antipodal cultural relationship between the hacker ethics—with its emphasis on producing open, accessible, and workable technologies—and a secretive religion such as Scientology, which releases proprietary technologies that do not work and cannot be improved by its affiliates.[50]

Above all, Project Chanology marked a new transition phase in Anonymous. If, until 2008, raids and pranks were mostly driven by the lulz, with Project Chanology, Anonymous began to resemble an organized political movement. This is clear from the advanced usage of IRC for organizational purposes and the emergence of a self-appointed group of organizers who took on multiple tasks, such as dividing up the network into regional chat rooms, distributing guidelines for the street protests, setting up discussion forums, writing press releases, holding regular meetings, and coordinating the work of many others. Predictably, it did not take long before some Anons accused the organizers of #marblecake of being "leaderfags," that is to say, of violating Anonymous's anticelebrity ethos for their self-serving political agendas. Yet the emergence of an informal leadership within Anonymous was less a by-product of personal ambition than of the exponential growth of a network that now mobilized thousands of participants. In fact, the simple need to set up an infrastructure to facilitate the remote interaction of such a large group of hacktivists entailed the emergence of hierarchies based on technical competence.

To begin with, as Coleman notes, in IRC, a great deal of power is concentrated in the hands of the administrators who "install, configure, and maintain the server."[51] Identified by symbols such as "@" and "+o," IRC administrators and operators own various privileges that allow them to invite users to, kick users off, and ban users from a channel (or a network); give users enhanced status; and even read users' private messages.[52] Second, the continuing presence of certain monikers in an IRC channel allows users to tell the regular hangers-on from the occasional visitors. Such presence is particularly relevant during and after a DDoS attack or other operations that entail legal risks, as it tells participants who is willing to run such risks and who is not. Third, in IRC, moderators can easily create private and invite-only channels wherein actions are planned behind closed doors by a selected few. In contrast to imageboards—where message threads are visible to everyone—this feature of IRC is conducive to the formation of affinity groups that can act autonomously within a larger operation or assume a leading organizational role (as in the case of #marblecake). As we shall see, this technoelite played a crucial role in operations such as Operation Payback, Operation Avenge Assange, Operation Tunisia, and Operation HBGary Federal, among others.

To sum up, if in 4chan the characterization of Anonymous as a leaderless "swarm," "horde," or "hive mind" is supported by software that enforces almost complete anonymity, in IRC, pseudonymous personae acquire a distinctive status within the network. This means that imageboards and IRC function as two distinct authorizing contexts and machines of subjectivation. Although it is true that anyone is formally free to borrow the moniker Anonymous, when the improper name is mobilized in conjunction with impromptu actions such as the 2006–8 raids, it comes to designate a *swarm* whose complex behavior emerges from the distributed coordination of relatively simple tasks, such as operating an autovoter, posting a link, launching a DDoS tool, sending a fax, or making a phone call.[53] By contrast, when Anonymous is associated with prolonged and sophisticated campaigns, such as Project Chanology, it designates a *network* whose organization requires a more advanced specialization of tasks and functions. In such a context, individuals with strong technical, cooperative, affective, and linguistic skills tend to emerge for their ability to program, hack, and configure software; share technical expertise; think strategically; coordinate and motivate others, and so forth.

Before moving forward, allow me to clarify an important point: I am not trying to set up a simple dichotomy between the emergent behavior of the swarm and a supposedly hierarchical configuration of (hacktivist) networks. As Alexander Galloway and Eugene Thacker point out, networks can accommodate both centralized and decentralized topologies, control and emergence, regulation and the free flow of information. Yet, whereas swarms exist only in time—that is, as dynamic assemblages that are constantly evolving and self-adjusting—we are used to map networks as topologies that are synchronically apprehended. Galloway and Thacker note that the spatialization of networks is more the result of a modeling effect of graph theory—which attributes a place and an agency to each node—than an immanent property of networks.[54] Nonetheless, my argument here is that the technocultural features of IRC enable a form of organization that, though not static, is certainly more structured than the one enabled by an imageboard.

In *A Thousand Plateaus,* Deleuze and Guattari juxtapose the smooth and the striated to describe two different typologies of space: smooth spaces, such as seas and deserts, lack stable markers, are constantly changing, and as such can only be navigated and crossed by sailors and nomads; by contrast, striated spaces are the segmented and measurable spaces over which the modern state exerts its sovereignty.[55] Extending this metaphor to network-based subjectivity, we might say that the imageboard is a *smooth machine of subjectivation* in which each post contributes to and is an expression of Anonymous. Conversely, the IRC network functions as a *striated machine of subjectivation* in which pseudonymous users contribute to Anonymous as an open reputation but also grow a personal reputation through their individual contributions.[56] Lacking an archive and the name of an author, the imageboard is always resetting itself—its message threads are like waves and dunes that can only be interpreted and crossed, not owned. With its multiple entry points, local and global servers, public and private channels, IRC's topology resembles instead an urban space whose dynamic evolution is facilitated by administrators and operators with varying degrees of authority.

It is opportune, however, to consider the smooth and the striated as abstract categories, as in reality the two often overlap. As a feature of the imageboard software, Anonymous functions as a collective and impersonal assemblage of enunciation whereby message threads materialize and go out of existence. Yet if, on one level, Anonymous is the name of an unpredictable and radically forgetful discursive space, temporary patterns and refrains—such as catchphrases, memes, and raids—do emerge and leave traces over time. In this respect, Anonymous is always *a* particular Anonymous or an assemblage of dividuals whose interventions are individuated, traceable, and memorable.

Thus Anonymous swings between two poles. At one end of the transductive operation, there is the pole of smooth discourse and pure anonymity. As a function of the imageboard software, Anonymous is the line of flight that opens up discourse to its own timelessness and ambiguity, making it impossible to order it and archive it through discrete publications and individual attributions—what Michel Foucault called the modern "author-function."[57] At the other end, there is the pole of striated discourse and (shared) pseudonymity. As an improper name that is borrowed by a network of users to organize specific actions and operations, Anonymous traces recognizable patterns that cut through the chaos of the imageboard as a subjectless assemblage of enunciation.

The coexistence and hybridization of these two poles—a smooth, anonymous, discursive space and a striated, pseudonymous discourse—may explain why seemingly incongruous definitions of Anonymous as swarm, collective, hive mind, meme, movement, and network are not necessarily incompatible. The fact that these two regimes infuse the same improper name may also explain why Anonymous is simultaneously constituent power and permanent subversion, culture hero and amoral force, a collective "united as one and divided by zero."

BOTNETS WITHOUT BORDERS

On September 5, 2010, Girish Kumar, managing director of the Indian firm Aiplex Software, declared to the online news agency DNA that his company had been conducting DDoS attacks against Torrent websites that did not comply with copyright notices for newly released Bollywood films.[58] Few days later, Kumar repeated the story to the *Sydney Morning Herald,* adding that Aiplex had also been hired by Hollywood film companies and was ready to provide its services to the Australian film industry.[59]

Although the film industry had long been suspected of resorting to extralegal measures to take down large Torrent sites, such as the Pirate Bay and Demonoid, Kumar's unusually candid statements provided the first piece of evidence that this was the case. Given the popularity of the Pirate Bay—the self-styled "world's most resilient Torrent website"—among 4channers, the idea of retaliating against Aiplex quickly gained traction on /b/. From there, it bounced on various IRC networks, where Anonymous begun discussing how to coordinate a DDoS attack against the Indian firm. Since late August, some Anons meeting on the IRC server OccultusTerra had been planning a DDoS against the Office of the U.S. Trade Representative (ustr.gov) to protest against ACTA, the Anti-Counterfeiting Trade Agreement, which had caused an international uproar for the sweeping regulations it would have enforced if approved. The IRC operators had immediately shut down the channel dedicated to the coordination of the DDoS for planning an illegal action.[60] This was not atypical for IRC servers, and the planning of the DDoS against Aiplex faced the same obstacles.

To circumvent these obstacles, "the Anons jumped from IRC network to IRC network, pasting links to the new rooms on 4chan and Twitter each time they moved so others could follow."[61] This constant drifting did not prevent them from setting up the initial targets and logistics of what came to be known as Operation: Payback Is a Bitch in a few days. Although the initial participation in this operation was not comparable to that in the early phases of Chanology, Anonymous could count on an infantry of a few hundred LOIC users recruited mostly through 4chan and an artillery of a few botnets. The LOIC, an acronym for Low Orbit Ion Cannon, is an open source application that enables users to flood a target website with junk packet requests to make it unreachable.[62] While the effectiveness of LOIC is provisional on the synchronic participation of hundreds or even thousands of users, depending on the robustness of the target host, a botnet is a network of tens of thousands (sometimes even hundreds of thousands) of infected computers that is controlled by a single operator. As we shall see, the coexistence of these two kinds of weaponry—one distributed and requiring the participation of many, the other centralized and controlled by few—was bound to spark numerous tensions within Anonymous.

In the beginning, however, most Anons seemed more excited with the availability of botnets than concerned with the differential levels of power generated by the limited availability and secretive use of these tools. On September 17, 2010, the first target of Operation Payback, the Aiplex Software website, was knocked offline—supposedly by a single Anon with a botnet.[63] Unsatisfied, Anonymous invited all LOIC users to target the websites of antipiracy lobbies such as the Motion Picture Association of America, the Recording Industry Association of America, and the International Federation of the Phonographic Industry, giving them an initial combined downtime of more than thirty hours in two days.[64]

On September 21, Anonymous expanded its operations to ACS:Law and Davenport Lyons, two law firms known to the British public for pursuing thousands of file sharers. As ACS:Law struggled to put its website back online after several hours of downtime, it accidentally made available a large backup file. The file contained company e-mail that showed how the methods used by the firm to demand out-of-court settlements from presumed copyright infringers overstepped legal boundaries and amounted to a form of blackmail. Furthermore, it exposed unencrypted Excel spreadsheets with the personal information of thousands of Internet users that ACS:Law had accused of illegally downloading music or adult material.[65] This alleged breach of the U.K. Data Protection Act prompted an investigation by the Information Commissioner's Office into ACS:Law. As a result, in February 2011, the company CEO, Andrew Crossley, decided to shut down the firm.[66] A year later, the Solicitors Disciplinary Tribunal ordered Crossley to pay a hefty fine and suspended his license for two years.[67]

Galvanized by the success and publicity, Anonymous extended Operation Payback to any country where Anons could identify appropriate targets. In October and November, several antipiracy lobbies and copyright authorities were DDoSed and knocked offline, including the British BPI, the Australian AFACT, the Spanish SGAE, the Italian FIMI, the French HADOPI, the Portuguese ACAPOR, the U.S. Copyright Office, and the Dutch BREIN.[68] By coordinating in IRC and using social network sites and imageboards to publicize their actions, organizers undertook a variety of tasks, which ranged from selecting targets to recruiting activists to deploying a robust communication infrastructure. In other words, Operation Payback showed that Internet users were able to organize and confront the organized interests of copyright holders at a global level without recurring to any institutional mediation.

Such organizational effort was by no means linear, as the Anons had to confront several technical and political hurdles. On a technical level, in the very first days of Payback, the #SAVETPB public IRC channel had itself been disrupted by a DDoS attack and flooded with hundreds of fake usernames controlled by a botnet.[69] Evicted, once again, by the IRC hosts that received takedown notices, a group of IRC administrators affiliated with Anonymous decided to create an independent chat network by pooling different servers to which they had access.

On November 3, 2010, AnonOps, the first IRC network entirely affiliated with and controlled by Anonymous, was launched. The importance of this event cannot be overstated, as it brought to an end, at least momentarily, the nomadic phase of Anonymous. Rather than constantly hopping from one network to another, the Anons could now rely on their own infrastructure—an infrastructure that had to be managed, maintained, and defended by possible counterattacks. This means that IRC operators and administrators not only wielded power over communication among IRC users but also retained exclusive access to strategic resources such as domain names and servers. In this way, the needs of cyberwarfare created a technoelite whose power sharply contrasted with Anonymous's horizontal structure and democratic decision-making processes.

Throughout the course of Operation Payback, this technoelite met in a secret IRC channel called #command. Even though some organizers would occasionally be recruited from the public #SAVETBP, this invite-only channel functioned as an organizational hub that remained invisible to most Anons. It is in this channel that key decisions on what to target and for how long were made, often by taking a formal vote among the organizers.[70] And it is here that elaborate discussions on Payback's strategic direction inevitably unfolded. While in the beginning the organizers had declared that the operation had "no time frame" and would have continued indefinitely, in early November some of them begun to wonder whether Payback could have yielded tangible political results.[71] As a result, the Anons meeting in #command decided to issue a list of demands to governments worldwide, which called for an immediate cessation of the piracy lawsuits and for a progressive reduction of the copyright life-span rather than its abolition.[72] This unexpected move was supported by a joint letter of the British and U.S. Pirate Parties that urged Anonymous to cease all DDoS attacks immediately and to remain "within the bounds of the law" in the common fight for copyright reform.[73]

Unsurprisingly, Payback's "reformist turn" was met with skepticism and even outrage by the Anons who had been mostly relying on the public AnonOps channels to coordinate the attacks. Not only had the organizers refused to consult the other Anons, but the very existence of a #command channel clashed, once again, with the notion that Anonymous was an entirely horizontal and self-organizing swarm. Furthermore, the list of demands went almost completely unnoticed by the press. While DDoS attacks and website defacements provided fodder for sensationalist headlines, the notion that Anonymous had formulated rational if not reasonable demands did not really fit the story line of the shadowy hacker network all intent on spreading havoc online.

Yet Anonymous's demands were rational—so rational that, by November 2010, the lulzy, Dionysian drives that had infused the first phase of Anonymous seemed to have evaporated. The fact that Anonymous was increasingly acting as an organized political actor became clear as soon as its path intersected that of whistleblowing website WikiLeaks.[74] On November 28, 2010, the organization led by Julian Assange released a first batch of 220 U.S. State Department classified diplomatic cables as a preview of the world's largest leak of classified material in history. The so-called Cablegate immediately attracted the ire of the U.S. government, and in early December, EveryDNS and Amazon cut their web hosting services to WikiLeaks. Shortly thereafter, citing presumed violations of their terms of service, PayPal, Visa, and MasterCard also cut their finance services to WikiLeaks. To some activists, these concerted actions appeared to satisfy specific government requests in retaliation for the violation of state secrets. For many others, the very fact that PayPal continued to process donations to organizations such as the Ku Klux Klan while cutting them to an organization that had not even been formally indicted was morally unacceptable and outrageous.

In late November, the organizers in #command were already debating how to proceed after their leading role had been contested by the vast majority of Anonymous and participation in Payback was dwindling. It did not take them long to realize that the uproar caused by WikiLeaks was a golden opportunity to take the operation in a new direction. On December 4, the day after PayPal had cut its funding to WikiLeaks, Anonymous DDoSed and took down *The PayPal Blog*. In the following days, AnonOps targeted postfinance.ch—a Swiss bank that had cut access to the WikiLeaks defense fund—the registrar EveryDNS, and the official website of Senator Joe Liebermann, who had encouraged Amazon to cut its hosting to WikiLeaks. On December 7, the AnonOps servers came themselves under a massive DDoS counterattack that knocked them offline for several hours. The same day, complying with a European arrest warrant issued by the Swedish authorities for sexual misconduct, Assange turned himself in to a police station in England.

The news of Assange's arrest made a sensation on a global level. As AnonOps set its target on the websites of Visa, MasterCard, and PayPal for the newly christened Operation Avenge Assange, thousands of users joined the #operationpayback channel on AnonOps. The salience of this moment is captured by an Anon in a IRC conversation with Gabriella Coleman:

> A: and within a few hrs
> A: it went viral
> A: we sat and watched numbers [of IRC channel population] rise
> A: from around 70
> A: which was about the lowest we had ever been
> A: we were saying wow it's gonna be 500 soon
> A: (our previous high was ~700)
> A: then we passed that
> A: then we hit 1000
> A: then the madness broke
> A: and we got to >7000
> A: we had to suddenly increase server numbers
> A: and it was a crazy crazy time
> A: we were stunned and a little frightened tbh [to be honest][75]

As the network administrators scrambled to increase the server capacity to avoid AnonOps crashing from excessive traffic, they were quietly joined in #command by two botnet operators, Civil and Switch. Each botmaster controlled a network of thousands of infected computers, which were operated directly through private IRC channels.[76] Furthermore, many LOIC users had set their clients in the HiveMind mode, a feature of the software that allowed the operators of the #loic channel to set all clients on the same target and operate them remotely at once.[77] Thus the AnonOps operators could now rely on the combined power of a few hundred synchronized LOIC clients and roughly thirty thousand zombie machines controlled by the two botmasters.[78]

Such firepower was badly needed to take down PayPal, a portal that, unlike Visa.com and Mastercard.com, is used by millions of users worldwide for all sorts of financial transactions. It is to be noted, however, that with the exception of a dozen organizers meeting in #command, the LOIC users were completely unaware that the botnets operated by Civil and Switch contributed about 95 percent of the total firepower of the DDoS attack. Parmy Olson notes that this lack of transparency was not considered problematic by the core organizers:

> 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 zombies computers or real volunteers.[79]

Such lack of transparency not only affected the ability of LOIC users to make informed decisions about their participation in the DDoS but also exposed some of them to the risk of legal prosecution.[80] Because LOIC does not obfuscate the users' IP numbers, only those Anons who knew how to cloak their IPs participated in the attack without fear of reprisal. The others were simply advised to respond to a possible investigation by denying any knowledge of the software and blaming it on a "botnet virus."[81]

Yet while the opacity of AnonOps's decision-making process and the existence of hierarchies based on technical expertise were not unproblematic, the notion that thousands of Anons who participated in the operation were simply "manipulated" is not accurate either. In fact, many decisions made in #command were based on ideas that were discussed in the public channels. Furthermore, many Anons took on tasks whose coordination was not centralized. These included writing press releases, making propaganda videos and digital flyers, recruiting other hacktivists through social network sites, talking to reporters, and so forth. And yet, AnonOps's choice of recurring to DDoS attacks to redress grievances turned the #command channel into a necessary hub for the coordination of attacks that mobilized a range of technical competences and resources.

As previously noted, the botmasters Civil and Switch controlled their networks of zombie computers through regular IRC channels. In the same way as BillOReilly, the main operator of the #loic channel, could visualize a list of all the LOIC clients that were set in HiveMind mode, so Civil and Switch could visualize a list of all the active infected computers in their botnets and operate them through private channels. Hence, from a technical standpoint, whether the machines were voluntarily connected to the LOIC botnet or involuntarily connected to a malicious botnet did not make any difference.

From a political standpoint, however, the fact that thousands of users were actively involved in the operation did make a difference. In fact, it was the LOIC users' motivation and purpose to turn the DDoS on PayPal into a political event. As we have seen, a company like Aiplex Software also rented and operated botnets in the service of the copyright industry, yet its motivation was financial rather than political. Furthermore, botnets are used not only for DDoS attacks but also and foremost to relay large volumes of e-mail spam. From this point of view, networks of infected machines appear to be neutral resources whose political or economic function is ultimately determined by their mode of employment.

This instrumental reading, however, tells only one part of the story. Botnets have in fact a political economy of their own. For example, the market value of a botnet depends not only on the number of zombie computers but also on their geographical location. Loads of infected machines in the United States and Europe are significantly more valuable and expensive than those in Asia because they rely on more stable connections and are available for longer periods of time.[82] Furthermore, because bots are neutralized by antispam filters, owners have to frequently replenish their load supplies as well as ensure that the botnet command-and-control servers are properly obfuscated and can quickly migrate when detected. Hence botnets are dynamic assemblages whose composition, value, and performance depend on numerous factors—including their fast-evolving topology, their owners' purchasing power, the demand for DDoS and spam services, the market price of payloads, and the technolegal power accorded to antispam firms within a given jurisdiction.

From this angle, botnets are not merely tools. Rather, these nonhuman operators exhibit an autonomy that poses an ongoing threat both to Internet security and the network economy. To grasp the nature of this autonomy, we have to consider that infected computers are never just infected by accident. Although computer literacy certainly decreases the chances of malware penetration, Internet users often *seek* and *enjoy* free access to resources—be they proprietary software, music and video files, e-books, or live streaming events—that are distributed through inherently insecure platforms.[83] And even when they do not enjoy such exchanges, the users still play an active role in turning their computers over to the botnet. The fact that not all users are equally aware of these security risks is less significant than that a large portion of Internet transactions occur outside of sanitized commercial platforms. From this point of view, the botnet seems to capture and organize libidinal flows that exceed and bypass the logic of exchange value.

Matteo Pasquinelli has introduced the expression *libidinal parasite* to describe symbiotic organisms—such as porn videos, Second Life avatars, and other popular Internet phenomena—that drive the network economy by accumulating "libidinal surplus-value."[84] Drawing from the work of Michel Serres on the tertiary logic of parasitism, Pasquinelli argues that these immaterial parasites channel libidinal surplus toward an expansion of the technological and material infrastructure that makes up the Internet. In this respect, their function is ultimately productive in that it increases the demand for new hard drives, servers, PCs, routers, media players, and so forth. Yet not all digital parasites transfer energy from the immaterial to the material in a productive way. Botnets, for example, parasite the bandwidth and processing power of millions of machines that inflict economic losses to companies and end users on a daily basis. In fact, it is estimated that the e-mail spam handled by botnets is a negative externality that costs the net economy a hundred times as much as what it generates for the spam industry.[85]

Neither just a tool nor simply a productive machine, the botnet is thus both productive and antiproductive. It is productive in that, to survive and grow, it has to be profitably rented, maintained, disguised, and expanded. And it is antiproductive in that it forces software engineers, network security experts, firms, and users to spend considerable resources on containing its ability to jam and take over the network. From a cybernetic standpoint, the botnet is thus a *noise-making machine* that threatens the successful transmission of coded signals. Whether delivering spam or causing server outages and network freezes, the botnet is the noisy background against which functional communication occurs. At the same time, without noise, signal could not be defined as such in the first place. As Michel Serres notes, "systems work because they do not work. Nonfunctioning remains essential to functioning."[86]

As we have seen, the botnet's noise is nothing but a by-product of a libidinal economy whereby Internet users seek access to resources that are free and readily available yet unsafe and potentially dangerous. At the same time, the botnet stands in a transductive relationship to the liquid economy of desire, that is, it organizes and synchronizes libidinal flows that would otherwise remain separate. To be sure, the botnet does not directly control users' desire—only the processing power of machines that have been infected because of their users' desires. The botnet quietly brings this residual machinic libido under control and employs it for its own ends. It does so according to a logic that Serres would describe as inherently parasitical—a logic of "abuse value" that takes without giving and yet makes communication among otherwise incommensurable orderings possible.

From this point of view, the instrumental use of botnets (by or against the copyright industry, for or against WikiLeaks) is less significant than the fact that thousands of machines are connected to one another to open up a margin of indetermination within the system. In fact, it is entirely possible for the same infected computer to participate in DDoS attacks executed by opposing parties who can rent and operate the same botnet at different times. As we have seen, this undecidability also characterizes Anonymous and the improper name. Yet while authorizing contexts and communities of practice can circumscribe the mode of disposition and usage of an improper name, as nonhuman operators, botnets resist any ethical and social determination. In this sense, botnets share something with the amoral nature of the lulz, whose self-propelling logic makes it akin to a positive feedback that pushes a system toward instability.

If this is true, then Anonymous's more or less overt use of botnets complicates and risks to derail the ethical and political turn that began with Project Chanology. And this is not only because a single botmaster wields more technical (and therefore political) power than hundreds of Anons combined, but also because as a form of machinic libido that is out of control, the botnet injects noise into the very authorizing contexts (IRC for the most part) that are meant to contain the radical openness and ambiguity of the improper name. Whether such disruptions come from without, in the form of DDoS attacks conducted by sworn enemies of Anonymous, or from within, in the form of DDoS attacks conducted by former allies,[87] the use of botnets threatens the patient compositional work that subtends every form of activism. Thus access to a superior technical power can undermine the constitutive protocols of grassroots democracy and subject the community to the permanent subversion that is a hallmark of trolling and the lulz. In this respect, the botnet is nothing but a *machinization of the lulz*.

Herein lies the entire problematic of hacktivism. As a metastable system, hacktivism is in tension between the power of mastering technology proper to hacking and the cooperative competences required by activism. My wager is that, while in the period 2008–10, the transductive relation between these two poles expresses itself as a tension between the ethical nature of hacktivism and the amoral character of the lulz, beginning in 2011, this tension transmutes into a tension between the embodied, slow-paced, and democratic politics of social movements and the disembodied, fast-paced, and elitist politics of computer hacking. As we shall see in the next section, the more strictly political wing of Anonymous encountered and merged with grassroots social movements that occupied streets and squares in the Middle East, Southern Europe, and the United States. At the same time, the more technically skilled wing of Anonymous went on hacking sprees that were increasingly disconnected from political ideals and objectives.

FROM THE ARAB UPRISINGS TO OCCUPY

On December 17, 2010, twenty-six-year-old street vendor Mohammed Bouazizi set himself ablaze in front of the governor's office of the rural Tunisian town of Sidi Bouzid. Motivated by the local police's confiscation of his produce and wares, Bouazizi's extreme gesture sparked a wave of street protests.[88] The vendor's self-immolation was not the first of its kind, nor was this the first time Tunisians took to the streets to protest police abuses. What turned Bouazizi's sacrifice into a highly political gesture—a gesture that eventually came to signify the resistance of an entire people to political oppression—was that this time protesters took to the streets with "a rock in one hand, a cell phone in the other," as Bouazizi's brother later recalled.[89] Knowing that Tunisian media routinely ignored street protests, locals decided to film their own actions and post videos to Facebook, which, unlike most video-sharing sites, escaped censorship. From Facebook the videos were picked up by Al-Jazeera Mubasher, a satellite TV channel that specializes in airing raw, unedited footage. The sudden visibility of Sidi Bouzid's uprising allowed the protest to spread to other

Tunisian cities and snowball in what came down in history as the Jasmine Revolution.

Some Anons had already set their eyes on Tunisia in early December, after the dissident Tunisian blog Nawaat.org had published seventeen U.S. State Department cables released by WikiLeaks on a dedicated website called TuniLeaks.[90] The cables showed that between 2008 and 2010, the U.S. diplomacy expressed concern for the Tunisian government's violations of human rights and the growing unpopularity of the Ben Ali regime, which had ruled the country with an iron fist since 1987. Consistent with its record of aggressive Internet censorship, the Tunisian government swiftly blocked access to TuniLeaks and the Lebanese newspaper *Al Akhbar,* which had published the cables on its website.[91] It took a few days for the news to be reported by Western media. Furthermore, in early December, all AnonOps's efforts were still directed against the financial firms that had cut their services to WikiLeaks.

Yet as the revolt begun spreading from Sidi Bouzid to other cities, some Anons set up an #OpTunisia channel on AnonOps. Here they were joined by a few hacktivists based in Tunisia. It soon became clear that the government's acts of censorship went well beyond the obfuscation of WikiLeaks-related websites. In fact, the Tunisian government specialized in sophisticated phishing operations that consisted in stealing Internet activists' usernames and passwords by filtering their Facebook and e-mail accounts at the ISP level.[92] Anonymous responded to the censorship with a two-pronged approach. On one hand, two small hacking teams meeting in the invite-only #opdeface and #internetfeds channels attacked, took down, and defaced several government websites, including those of the president, the prime minister, the ministry of foreign affairs, and the stock exchange.[93] On the other hand, the hacktivists developed a plug-in for the Firefox browser that allowed users to disable the phishing scripts used by the government.[94]

The plug-in was both posted online and distributed via IRC as part of a "care package" for Tunisian protestors containing First Aid guides, anticensorship tools, and propaganda materials. Assembled with the collaboration of Tunisian Anons and partly translated into Arabic, the package was distributed by Anonymous and Telecomix—a hacktivist cluster many of whose affiliates had ties to the Pirate Bay. The set of PDFs contained in the package blended activist expertise on how to organize street protests and avoid arrest with hacktivist knowledge of how to anonymize online activities. For example, the eighty-one-page-long *Anonymous Security Starter Handbook* divides personal safety into "Physical Safety and Internet Safety. It is important to remember that these two spheres overlap: a lapse of internet safety could lead to physical identification. However, by keeping in mind a few important rules you can drastically reduce the chance of being singled out and identified."[95] Consequentially, the document provides sensible tips on how to anonymize Internet activities and avoid identification offline.

It is worth noting that the "Do Not List" for physical safety ("do not trust anyone to be who they say they are; do not give any personal information that could be used to identify you to anyone; do not mention anything about relationships, family, or relatives; do not mention ties to activist groups") shares the same paranoid logic of the "Do Not List" for Internet safety ("do not use any or all of your actual name in account and usernames; do not mention anything that could be personally identifying; do not mention time zones; do not mention physical characteristics or abilities; do not mention relationships, family, or relatives").[96] It is as if the economy of suspicion that characterizes the hacker underground has been generalized and extended to the entire social fabric. To be sure, in the context of the Jasmine Revolution, paranoia was not an invention of Anonymous but a widespread psychological condition that was amplified by the government's all-too-real arrests of bloggers (some of whom were related to OpTunisia) and political opponents.[97] Nonetheless, it is significant that Anonymous's contribution to the Tunisian revolution consists in sharing a knowledge that is not merely technical but infused by a cyberlibertarian ethos one of whose core principles is, in the words of Steven Levy, "mistrust authority, promote decentralization."[98]

The care package combines, in fact, a negative notion of freedom—as individual freedom from governmental control and coercion—with the more positive freedom to share ideas and know-how. Gabriella Coleman and Alex Golub point out that these two notions of liberty are embodied in specific hacker practices. On one hand, the ethics of "cryptofreedom" (as freedom from government control) can be traced back to the early 1990s cypherpunks, a libertarian network of programmers and civil rights advocates who aimed at achieving privacy through the proactive use of cryptographic technologies such as PGP software.[99] On the other hand, the ethics of sharing is most notably associated with the F/OSS community, or with the freedom to access, change, and distribute software by making its source code available to everyone.[100] Coleman and Golub add that these two strands of hacking sit, somehow uneasily, next to a third strand whose protagonists enjoy "the thrill of breaking rules and gaining access to forbidden knowledge not necessarily to make the world a better place or secure civil liberties, but for its own pleasurable sake."[101] This transgressive strand encompasses a host of practices such as phone phreaking, software cracking, social engineering, and trolling.[102]

It should be noted that although, on a practical level, these brands of hacking differ widely, their underlying ethos provides a common ground for their coexistence and hybridization. In fact, the ethics of cryptofreedom is functional to both the legal practice of sharing know-how and resources and the illegal practice of hacking into password-protected databases and private intranets. This Janus-faced politics is a distinctive trait of Anonymous and is clearly at work in OpTunisia. Indeed, both the antifishing Firefox plug-in and the defacement of the Tunisian government websites had been developed and carried out by the #internetfeds hacking team, which had first coalesced during Operation Payback. As we shall see, shortly after Operation Tunisia, the group revived Anonymous's lulzy origins by executing a series of spectacular hacks that received worldwide media attention. Meanwhile, other Anons continued building connections with Middle Eastern activists as the Jasmine Revolution sparked a cycle of uprisings in North Africa, the Middle East, and around the world.

Not only was the care package updated and distributed in several countries touched by the Arab Spring—including Egypt, Libya, Bahrain, Gaza, and Syria—but at the launch of each operation, new Anons from the Arab and Muslim world joined the AnonOps IRC network. During the Egyptian revolution, Anonymous and Telecomix worked together to provide alternative means of communication to protestors on the ground. After the Egyptian government blocked access to Facebook and Twitter in the initial days of the uprising, Telecomix set up proxy servers for publishing videos of the protests and made its IRC available for retweeting messages on behalf of Egyptian activists. On January 28, 2011, the Egyptian government made the historical move of shutting down Internet access for almost the entire country. In response, the hacktivists convinced two European ISPs to restore their old modem banks and faxed information into the country on how to access them. Land telephone lines were also used to fax medical information on how to treat tear gas, scramble communications, and set up local wireless networks that relied on cell phones and other available hardware. (The latter proved particularly useful in the overcrowded Tahrir Square.)[103]

The politics of facilitating access and providing secure communications to dissenters continued through summer 2011 as a growing number of Syrian activists joined Telecomix and Anonymous's IRC networks. In this case, hacktivists associated with Telecomix were able to hack into five thousand unsecured home routers and post messages on how to encrypt communications and safely browse the Internet. Furthermore, they published fifty-four gigabytes of Syrian Internet users logs that showed how the Syrian government was spying on its citizens using surveillance technologies produced by Californian firm Blue Coat.[104]

The Arab Spring changed not only the demographics of Anonymous but also the perception of what Anonymous was becoming and could become in the eyes of many European and U.S. hacktivists. The Egyptian revolution in particular forged bonds among hacktivists based in Europe and North America and Egyptian revolutionaries on the ground. In a video interview, longtime hacktivist and Anonymous affiliate Commander X recounts the significance of this encounter:

> Some of this shit is personal. And one of the things about the movement as a whole, when Egypt rolled around, is that Egypt broke us emotionally. Watching in real time, [on] the live feeds that we helped set up, Egyptians getting *massacred* with machine guns . . . it was different. And I have never in cyber-activism wept before. It has never *bothered me* like that, it has never been able to touch me the way Egypt touched me.[105]

The sudden realization that aliases and words flickering on a computer screen are linked to living bodies that are at risk of being arrested, tortured, and killed—bodies that often exposed themselves to such risks *because* of their online activities—helped Anonymous mature a new ethical consciousness. It was as if for the first time Anonymous was able to perceive the vulnerability of others, to see their faces through the moving images they had helped distribute to make state violence visible.

The term *face* does not refer here only to a part of the human body. Drawing from the work of Emmanuel Levinas on the face-to-face encounter and the nonreciprocal relation of responsibility, Judith Butler argues that the face designates a nonnarcissistic and ethical relationship to the other:

> Levinas tells us, in fact, that "humanity is a rupture of being." . . . To respond to the face, to understand its meaning, means to be awake to what is precarious in another life or, rather, the precariousness of life itself. This cannot be an awakeness, to use his word, to my own life, and then an extrapolation from an understanding of my own precariousness to an understanding of another's precarious life. It has to be an understanding of the precariousness of the Other.[106]

From this angle we can gauge the evolution of Anonymous's contribution to the Arab Spring from a solidarity based on the extrapolation of a preexisting knowledge (the pro-WikiLeaks anticensorship campaign) to an emotional understanding of what it means to live under an oppressive rule. It is significant that this rupture and "awakeness" are prompted by the visualization of images that Anonymous initially helps distribute, that is, that are meant for everyone to see. In this sense, Anonymous's media activism upsets the normative schemas of intelligibility that were imposed by government-controlled media over the uprising. If, as Butler argues, normative media power effaces the other to prevent symbolic identification with it, then by returning a face to protestors, Anonymous facilitated "our apprehension of the human in the scene."[107]

It is certainly not without irony that an elusive organization such as Anonymous—an organization whose name is improper, whose most recognizable image is a mask, and whose affiliates rarely, if ever, meet in real life—would put a "human face" on the Egyptian revolution. Nonetheless, this recognition of the other's vulnerability did have consequences for Anonymous's modus operandi and ethos. On a practical level, it became immediately apparent that the disclosure of personal information could expose protestors and cyberactivists to retaliatory actions by their government. This required caution and a new sensibility about the way potentially identifying information was handled—a sensibility that Anonymous had lacked when it encouraged the use of unsafe tools such as the LOIC software. It also meant that Anonymous would increasingly try to support and meet the needs of social movements on the ground rather than pushing its own agenda.[108]

On an ethical level, the Arab revolutions helped Anonymous understand that the cyberlibertarian dictum "information wants to be free" is neither a moral imperative nor a universal law. Rather, the hacker struggle for keeping information free and in common—a necessary condition for hacking—undergoes itself a mutation when it intersects with a fully embodied politics. And this is not only because the human body is vulnerable in a way that codes and machines are not but also because bodily signification implies an ability "to interpret signs that are not verbal nor can be made so, the ability to understand what cannot be expressed in forms that have a finite syntax."[109] If networked systems exchange information in a functional way—that is, either by ignoring the content of the data they exchange or by "understanding it" exactly in the same way—bodily communication calls forth a sensibility to the nuances of an utterance, the unstated and the unsaid.

It is by searching for this experiential knowledge that many Anons from Europe and North America decided to join social movements against austerity measures and for "real democracy" such as the Spanish 15-M and Occupy in 2011. In the encampments and general assemblies that mushroomed in hundreds of Greek, Spanish, and U.S. cities, Anonymous discovered a different kind of politics—a politics based on the art of listening, taking care of others, deliberating, arguing, camping, marching, and facing arrest. This was still a media politics, but a politics rooted in quite a different medium—the social body, with its visible stratifications and power relations, its spatial constraints and bodily affects. It was also a prefigurative politics that was less concerned with attaining specific objectives than with announcing a world-to-come in its daily deeds. In this respect, Anonymous's contribution to Occupy was more positively oriented at setting up communication infrastructures, sharing skills, and publicizing the protests than at DDoSing websites or breaking into computer systems.[110] Such slow-paced, transparent, and constructive politics stood in many ways at odds with the frantic, secretive, and spectacular politics that was emerging simultaneously from a different wing of Anonymous.

THE POLITICS OF INSECURITY

The year 2011 was thus a critical one for Anonymous. As Anonymous conjoined to social movements around the world, it began to undertake a politics that was deictic in character, that is, a politics that heavily relied on local conditions and contextual information. This was a politics that did not tackle global issues through localized interventions (as in the case of Project Chanology and Operation Payback) but that was inextricably tied to public spaces charged with a high symbolic power. I would like to call this pole of Anonymous's third transduction the *deictic pole* to refer to a form of hacktivism that is anchored to real-world referents and rooted in local contexts. At the opposite end of the transductive operation (as previously noted, transduction implies the mutual constitution of two poles) exists an *abstract pole* according to which hacktivism should be concerned only with its own advancement. This pole is abstract in that it is deterritorialized and more strictly technical. Indeed, 2011 marks also the year in which Anonymous begins breaking into protected systems with more regularity. If, until 2010, Anonymous had privileged forms of intervention that did not require advanced technical skills, beginning in 2011, more sophisticated hacking techniques, such as SQL injections and smurf attacks, were employed to jam servers and break into protected networks and databases.[111]

As previously noted, the hacking team that conducted most of these attacks coalesced during OpTunisia.[112] After hacking and defacing several websites of the Tunisian government, the group focused on what appeared to be an impending threat to Anonymous. In early February 2011, Aaron Barr, an executive at HBGary Federal, a U.S. private security firm, declared to the *Financial Times* to have identified the real names of the "core leaders" of Anonymous.[113] A few days later, the team compromised the HBGary Inc. (the parent company of HBGary Federal) website and e-mail server. After defacing the website with a pro-Anonymous message, the

Anons published more than seventy thousand internal company e-mails, hijacked Barr's Twitter account, and even claimed to have remotely wiped his iPad. The e-mails showed how HBGary Federal had been conspiring with other data intelligence firms to design a smearing campaign against WikiLeaks and its supporters.[114] The campaign was traceable to Booz Allen Hamilton, a government contractor and consulting firm working on behalf of Bank America to respond to WikiLeaks's announced release of two banks' internal documents.[115]

The HBGary Federal hack was significant in the short history of Anonymous for three distinct reasons. First, it marked a clear shift away from tactics of electronic civil disobedience to hacking. Although most Anons enthusiastically approved of the hack, the action was planned and executed by a handful of individuals coordinating via secret IRC channels on AnonOps. As rumors spread about the identity of the authors, the IRC pseudonymous reputation economy granted them celebrity status within the network—an apparent contradiction with Anonymous's anti-celebrity ethos. Second, the hack brought together political engagement and entertainment, hacktivism and the lulz, reconciling the ethical and amoral sides of Anonymous. In particular, the hijacking of Barr's Twitter account and a series of amusing anecdotes—such as HBGary's CEO's and president's failed attempts at convincing (via IRC) Anonymous to return stolen internal documents—made the hack both newsworthy and highly entertaining.[116] Third, the internal praise and media attention galvanized the group, pushing it toward more endearing challenges. Capitalizing on their celebrity status, and feeling restricted by the broad ethical principles underlying Anonymous, the six members who had originally met in #internetfeds decided to break off from the network and create a new hacking crew, the LulzSec.

Shorthand for "Lulz Security" (deriding cybersecurity), LulzSec changed in many ways the history of computer hacking—not so much for its technical skills but for the way it meticulously exploited media attention. Between May and July 2011, the group amassed a large "fan base" on Twitter as it publicly announced attacks on government, corporate, and news organizations, taking down or defacing their websites, dumping users' credentials, and leaking internal documents. Government targets included Infragard (a nonprofit organization affiliated with the FBI), the

CIA, the Serious Organised Crime Agency (a British law enforcement agency), the U.S. Senate, and the Arizona Department of Public Safety. Among the news organizations, LulzSec hacked the website of the British tabloid the *Sun,* publishing a fake article on the untimely death of media mogul Rupert Murdoch and defaced the PBS website to criticize a sensationalistic documentary on Chelsea Manning. Corporate targets included Bethesda Game Studios, the porn website pron.com, and Sony, whose subsidiary Sony Pictures Entertainment was hacked by LulzSec after the PlayStation Network had been DDoSed by Anonymous in retaliation for Sony's choice to prosecute hacker George Hotz. Accepting requests from fans via Twitter, LulzSec also took down the websites of multiplayer games such as Minecraft, EVE Online, League of Legends, and The Escapist as part of their "Titanic take-down Tuesday." Finally, teaming up with Anonymous and other hacking crews, the group spearheaded Operation AntiSecurity (AntiSec), a hacking movement that targeted law enforcement agencies and white hat security companies around the world.[117] Besides the aforementioned government targets, AntiSec hacked the defense contractor Booz Allen Hamilton, FBI contractor ManTech International, NATO, and intelligence company Stratfor, among others.

At first sight, it is difficult to make sense of LulzSec's hacking fury, as most of its actions seem disconnected from one another. With exception of the Arizona Department of Public Safety, which was hacked by a politically motivated hacker, Jeremy Hammond, in response to Arizona's racist immigration policy, the LulzSec core members' motivations for picking specific targets ranged from the purely entertaining to the vaguely political. Yet, as previously noted, trying to inscribe the lulz within a moral and discursive horizon may not be the most productive way of approaching a force that goes to the limit and seeks no justification outside of itself. Perhaps, then, LulzSec's hacking spree should simply be described for what it was: the selective exploitation of security vulnerabilities from a list of hundreds of vulnerabilities provided by automated scanning tools. To be sure, selection implies ethical judgment, and there is evidence of the fact that LulzSec's members occasionally decided not to deface or steal information from targets they had penetrated. Nonetheless, selectivity and self-restraint were only second-order postures, which derived from the power to hack anything that could be hacked.

Following McKenzie Wark, I use the term *hack* in its etymological sense, to refer to a cut that opens up information to its virtual dimension. "To hack is to release the virtual into the actual, to express the difference of the real," writes Wark.[118] The LulzSec crew expressed such difference by combining technical skills and PR skills, the elitism of the self-selected few and a crave for media attention. As we have seen, this dual politics was also present in Anonymous. But the LulzSec crew perfected it by wrapping their own exploits in a coherent narrative and aesthetics that turned hacking into a fashionable, sexy, and entertaining business. As the Sex Pistols of the Web 2.0 generation, the LulzSec reached stardom by disseminating mayhem, leaving the scene at the peak of its fame. When the group announced its disbandment at the end of June 2011, the notion that nothing on the Internet could be considered safe anymore had been propagated by thousands of media reports around the world.

The politics of insecurity promoted by LulzSec is thus a politics that privileges difference over repetition—the search for unknown vulnerabilities (zero-day exploits) over the repetitive patching of what is known to be vulnerable. The illegality of such politics makes it necessarily secretive and detached from wider assemblages. The individuals who populate the hacker underground grow, in fact, a reputation on the basis of the exploits they are able to claim and receive tips, tools, and offers of collaboration accordingly. In this respect, the reputation economy of the hacker underground necessarily revolves around proper (pseudonymous) names. At the same time, movements such as Anonymous and AntiSec allow for the circulation and exchange of know-how within wider reputational milieux. Anonymous in particular has made it possible to link the secretive, exoteric politics of hacking to a variety of social movements. To be sure, such links are often tenuous and purely symbolic. Yet the Middle Eastern uprisings have shown how Anonymous was able to bring electronic civil disobedience, network exploits, and a democratic politics of access within a common discursive space. Furthermore, as an improper name, Anonymous has suggested a common thread among struggles against oppressive governments, media censorship, intellectual property laws, restrictions on access to information technologies, and the network security industry.

ANONYMOUS AND THE VANGUARD-FUNCTION

To sum up, in this chapter, I have argued that the elusive entity we call Anonymous can be described, following Simondon, as a metastable system that keeps individuating itself as it passes through three distinct transition phases. On a first level, Anonymous expresses a tension between the potentially deindividuating power of information technology—as Anonymous designates a whatever Internet user—and the conscious use of the improper name for affirming a collective form of individuation. Such tension initially expresses itself as a conflict between the Anons and the so-called tripfags (users who recur to an identifier) on the imageboard 4chan. Once the Anons prevail, it continues through the coexistence and hybridization of an entirely anonymous discursive space in the imageboard and a pseudonymous reputation economy in IRC. The imageboard and IRC function as two distinct authorizing contexts and machines of subjectivation. With its anonymous, condividual, and ephemeral discussion threads, the imageboard is a smooth discursive space where each post contributes to and is an expression of Anonymous. Conversely, the IRC network functions as a striated machine of subjectivation where pseudonymous users contribute to Anonymous as an open reputation but also grow a personal reputation through their individual contributions.

Anonymous's use of IRC as an organizational platform corresponds to the need to coordinate operations that require a more advanced specialization of tasks than is required by raids, which coordinate relatively simple tasks. Such operations emerged in 2008 as Project Chanology also set in motion a political wing of Anonymous. In the second transductive operation, Anonymous was contended between those who attached an ethical and political commitment to the improper name and those who claimed that Anonymous should be concerned only with its own enjoyment, the lulz. In Deleuzian terms, the lulz is like desire—a force that affirms its difference by going to the limit of what it can do. In this sense, the lulz is not simply a depoliticized alternative to hacktivism. Rather, it is an élan vital that, by relying on different techniques and technologies—be they trolling, automated botnets, or hacking for its own sake—drives hacktivism as it destabilizes it from within.

The third transduction of the improper name is set in motion by the increasingly global reach of Anonymous. With Operation Payback and Operation Avenge Assange, Anonymous organizes Internet users at a global level against the organized interests of copyright holders and the governments that restrict the free flow of information. As the global struggle for liberating information from the fetters of private property and state control morphed into political support of the popular uprisings that began shaking the Middle East in early 2011, Anonymous underwent a new individuation. On one hand, the Anons who helped protesters circumvent censorship, surveillance, and Internet shutdowns matured an ethical consciousness rooted in a recognition of the vulnerability of the other. On the other hand, the hacking teams that came together around the same time went on hacking sprees that were deterritorialized and detached from a shared political strategy. Thus, with the third transduction, Anonymous swings between an embodied politics that is slow paced, participatory, and deictic—a politics that cannot be detached from local conditions without losing its referent—and an abstract politics that is fast paced, secretive, and deterritorialized.

It is important to underscore that this oscillation between situational experience and abstract knowledge is not simply ambivalent or undecidable. On the contrary, because transduction is the *common operation* of two heterogeneous realities, it denotes the emergence of a new form of individuation. In his book *Tweets and the Streets,* Paolo Gerbaudo describes the 2011 occupations of Tahrir Square in Cairo, Syntagma Square in Athens, Puerta del Sol in Madrid, and Zuccotti Park in New York City as the production of a new kind of space. Denominated by hashtags such as #sol and #tahrir, these occupied "trending places" are for Gerbaudo "fixed points that *transfix,* points that capture and attract internet publics from a distance."[119] Likewise, in the Guy Fawkes masks punctuating the streets of Cairo, Rio, Montreal, Istanbul, and Ferguson, Missouri, and in their associated operations, we can glimpse the emergence of an assemblage of enunciation whose embodied and informational dimensions are increasingly inseparable.

This does not mean that Anonymous's global operations, such as Project Chanology, Operation Payback, Avenge Assange, and AntiSec, have exhausted their trust. In fact, Anonymous may well be, as Wark suggests, the vanguard of the hacker class—a class that asks "the property question" as it struggles to keep information in common.[120] Yet it is undeniable that after 2011, Anonymous seems to add an informational layer to preexisting social movements rather than playing a leading or strategic role. Perhaps, as Berardi suggests, it is the very notion of the modern vanguard to have become obsolete altogether as it entails "an exaggerated notion of political will over the complexity of contemporary society."[121] Or perhaps the contrary is true. As Rodrigo Nunes points out, the current "twilight of vanguardism" only overshadows the proliferation of groups that are capable of taking on a "vanguard-function" within a networked politics that makes (temporary forms of) leadership potentially accessible to anyone.[122] In this sense, Anonymous is not expected to lead a revolution but only to provide leadership in certain areas, such as setting up secure communication infrastructures, unveiling the identity of police officers who are accused of wrongdoing, and gaining access to restricted information.

The shift from the modern Leninist vanguard to the postmodern networked vanguards, however, re-presents the problem of the political direction of a movement at a higher level, namely, how to organize the different groups that take on different vanguard-functions. This is fundamentally a problem of mediation, which, given the increasing centrality of networked technologies, is also a problem of mediation between human and nonhuman actors. Perhaps, then, the best way to conceptualize Anonymous is to think of it as a transducer, a converter of libidinal flows that run through human and nonhuman operators. We have seen how, as a machinic accumulation of libidinal surplus, the botnet organizes libidinal flows that would otherwise remain separate. This transduction occurs through the common operation of two heterogeneous realities, namely, Internet users' desire to access information and the technical power of distributed computing. These two poles converge in a metastable entity that evolves by responding to the changing circumstances on the basis of its own drive for self-preservation—a drive that feeds on a machinic, libidinal economy.

Likewise, as a metastable system that keeps individuating itself, Anonymous seems to possess an interior milieu, a memory of its prior individuations that functions as a medium and source of information for future individuations. Such memory is neither only technical nor only human, but expresses the mutual constitution of human and technical ensembles with a high degree of indetermination. According to Simondon, the machine with a superior technicality embeds "a certain margin of indetermination . . . that allows for the machine to be sensitive to outside information."[123] More than any specialization or automation, it is this margin of indetermination that allows machines to communicate with each other and with other beings. In this respect, at the most general level, Anonymous may be the name of an emerging *koiné,* a new lingua franca whereby machines' openness to the surrounding milieu meets the human belief that defending such openness works in the service of a freer society.

Such an encounter, however, is fraught with risks, at least for us humans. First, as we have seen, humans are behaving increasingly like machines—that is, as cruel, "lulzy" beings devoid of empathy. Second, the machinization of desire expressed by botnets disrupts the very authorizing contexts that are meant to trace an ethical horizon for the movement toward an open society. Third, the frantic search for the vulnerabilities in the machine may prevent us from recognizing other vulnerabilities—vulnerabilities that require a sensibility for that which cannot be encoded in a finite syntax. In this respect, Anonymous's ability to mediate between the technical and the human may also be seen as a potential for transducting different notions of otherness, technological and corporeal velocities, finite codes and sensuous languages. Such power may ultimately project the improper name beyond a properly human language and ethics—in a domain where humans and machines may be able to search for and affirm their freedoms only in relation to one another.