4 Closer to the Metal

Finn Brunton and Gabriella Coleman

Introduction

Our project in this chapter is to reflexively break down the analysis of information and media infrastructure that we have developed, in our work as scholars, into its component parts. We do this to better understand the strengths and flaws of our approaches to working on subjects like Anonymous (the online activist group) and spam (nuisance messages and unwanted advertising online), and what these approaches might offer scholarship more generally. We assert the value of getting closer to the metal, and understanding in depth the technical architectures and processes that underlie online phenomena, but also assert that this dive into hardware is not a simple revelation of some true, foundational reality. When we peel back that deepest layer of materiality, we find people and practices underneath: populations of users, and the "superusers" who operate close to the metal in their work, including system and net administrators (sys/net admins), hackers, and spammers in complex, contingent, ambiguous relationships. The layers of hardware, users, and maintainers that make up many Internet phenomena are, in turn, fashioned into stories, theories, and concepts by which many others—from scholars to journalists to designers to politicians—take them up and turn them to various purposes, a fashioning which often dangerously and damagingly oversimplifies what is actually happening.

Consider, as a parallel, Lisa Gitelman's *Always Already New,* in which she seeks to "bedevil the strict dichotomy of production and consumption" (2006, 60) that characterize much of the received history and conceptions of media technology. To put it most crudely: a brilliant lone inventor, or a group in a garage, invents the technology. Masses of people consume it, and have their experiences mediated by it—and soon they inhabit a different world as a consequence. The producers create, and from their labs and workshops come tools, formats, and systems that make publics as a thresher makes grain from a field of wheat. Bedeviling this inaccurate and oversimplified story, Gitelman brings in the users—"diverse, dynamic, and disaggregate" (61) groups who are actively involved in shaping the features, the values, and the future of the systems they use. Her multilayered understanding of media systems is built on the historical example of how phonography comes about. This chapter concerns itself with the contemporary Internet, and two very different phenomena that happen there, but Gitelman's structure provides an excellent introduction to our argument, in goal as well as in structure. Gitelman asks, "Who made the phonograph?" and the answer turns out be much more extensive than the roll call of Edison and workers at Bell and Berliner. In our work, we ask "Who makes spam?" and "What makes Anonymous possible?" and find answers of technical and social complexity that suggest consequences and a model for how we study current and future media technologies.

Let us unfold these simple questions, first, into their component parts. Our initial answer opens into three distinct but overlapping frames, each implying the next, and each with relevance for studying media.

Materiality: The Hardware Story

To answer the questions, "Who *makes* spam?" or "What makes Anonymous possible?" you must start with the making, with the computers, servers, switches, cables, filters and algorithms, the protocols and mail standards. The infrastructure must be accounted for, alongside the screens, software, and users. To discuss the infrastructure also entails discussing the groups (and their labor) along with institutions that produce, regulate, and maintain it: the sys/net admins and IT and telecom professionals. These imply a second frame.

Users and Superusers: The Social Story

The obvious answer to "*Who* makes spam?" is that it is made by many orders and assemblies of users. Discussing the infrastructure in detail reveals that there are differences of access to and capability with the hardware, starting with those system administrators. There are the diverse families of users discussed by Gitelman (2006) who make various contributions to what the technology becomes, and to this array we would like to add the "superusers," a concept we will discuss in detail. "Superuser" is a term from computing for a special account meant for administrative functions (different operating systems use different designations, such as root, admin, baron, or supervisor). Computers and computer networks offer many more degrees of control than a phonograph or a magazine, and while all users play a significant role in the adoption and meaning of a technology, some can disproportionately produce functionality or wreak havoc. This includes the invention of new forms of social organization and labor that can take advantage of the material properties of the hardware, as we will see with Anonymous.

Concretion: The Facile Story

Finally, our final frame entertains more conceptual issues about categories and conceptual stabilization. Spam and Anonymous are spoken of as though they were single, self-consistent blocks of stuff, and made into stable, concrete objects that can be addressed with one name, in an act of misplaced concretism.[1] These stabilizations, too, are central to the making process and there are multiple sources with different agendas: academics, journalists, and law enforcement come most to mind as they distinctly represent and make Anonymous and spam. This making, whether in the form of law or journalistic rhetoric, must be borne in mind because it can interfere with how we answer the question of the ways these phenomena are produced.

In other words, hardware always entails institutional, structural, and designed potentials and constraints. Users and superusers take material objects up for many purposes and with many levels of agency. The things that happen then get rhetorically and discursively packaged, especially by the mass media, in the case of Anonymous, for still other groups to interact with and exploit. None of these frames alone provides a satisfactory entry point in itself to the questions of “Who makes spam?” or “What makes Anonymous possible?” Materialism is necessary, getting down to assembler language and undersea cables to produce an accurate sense of the substratum of a complex event—necessary, and often overlooked or marginalized, but not sufficient. The users and superusers have to be brought in, with their plethora of means, motives, and opportunities; no phenomenon would exist without them.

They, too, are necessary but not sufficient for a complete picture. The complete picture includes its own blind spots, occlusions, and range of focus, in the practices by which we as scholars research, document, and conceptualize our subjects. We need to close the loop by describing how the story of the phenomenon is made and told by others and by us, sometimes too easily and too simply. This awareness of how we make our model and construct our history—what gets included and why—feeds back into our analysis of hardware and our study of users. We need to reexamine where we place significance, where we set our starting point. (Someone from a sociological background can see in these three frames a modified and particular form of the natural, social, and discursive answers to the question of agency, linked together into a loop.)

The three parts that follow address each of these frames and help answer our initial questions about spam and Anonymous. The first takes the issue of hardware analysis and materiality, and demonstrates both the importance and the limitations of such an approach by itself—that we get down to the deepest, abiding bedrock layer of the material, peel it back, and find people, societies, and discourses at work. The second concentrates on Anonymous and the role of the technologists (user and superuser communities, sysadmins, discussants on an IRC [Internet Relay Chat] channel) in constituting the movement and its strategies, building on their technical fluency and varying control over the hardware, and on the role of secrecy and legal pressure in their practices. Finally, the third section takes up spam to explore how we build oversimplified conceptual models of complex and multifaceted technical events, and how those models can be productively bedeviled (to take Gitelman's [2006] term). To be clear, even as each section emphasizes its respective question, it also addresses the other two. Each frame—of hardware, of users, of stories—implies and affects the others. "Getting close to the metal" means getting close to the narratives and the people who tell them. Only with all three frames of reference in mind can we start to work at the breadth and detail appropriate to the polyphonic, massively multiuser, and materially intricate phenomena occurring on networked computers now.

Hardware, or the Concurrent Realities of Infrastructure

Where does infrastructure stop? For a start, keeping the system up, and keeping up with the system, requires power of at least three kinds. First, of course, is electrical: coal, diesel, sometimes nuclear, sometimes renewables. The clean, disembodied, virtual cyberworld produces a lot of coal smoke.[2] Second, it requires the production and maintenance of systems and software, which implies the third—a massive, often hidden, quantity of labor conducted by armies of net, system, and database administrators. A typical day for a system or net administrator might entail verifying backups, monitoring performance and connectivity, account provisioning, escalated support requests, and monitoring script output. Some days will be dominated by fixing problems and troubleshooting, trying to figure out why a server went down. Others are spent working proactively by, for instance, devising a backup scheme to time when backups happen, when old ones should be deleted, and then to automate the process. The infrastructure itself runs from that CAT-5 Ethernet cable plugged into the computer or the router through the jack in the wall over many different kinds of cables and lines provided by a proliferation of services in different countries, some monopolistic, some happily complying with governmental warrantless information requests, some filtering and blocking access, some public-private partnerships going through neoliberal convulsions. By occupational necessity, the system administrator is often conscious of the politics that run through the cable, undergird the co-location facility, and lay behind retaining (or not) server logs.

The cables likely pass through a co-location center, which houses noisy servers, where trunks of wiring run through the racks overhead or under the floor, and massive diesel generators sit on standby to assure redundant power. The co-location center is a site of many intricate stakeholder agreements and alliances. It may well be an "Internet Exchange Point," where the enormous Internet Service Providers (ISPs) and telecommunications carriers exchange data across their borders of proprietary ownership in the "Meet Me Room." (The Meet Me Room in the massive Southern California co-location center One Wilshire in Los Angeles is, in inches or centimeters, the most expensive real estate on Earth.[3]) From there, the request for a page may very likely go to one of the massive server farms—many of their locations kept top secret—with ranks and ranks of immaculate machines mounted into their racks in anonymous windowless buildings, blue LEDs glowing, in the permanent roar of the air conditioning, carefully laid out to ensure the flow patterns of cool and hot air. The cost of cooling a big server farm has led to the initiative to site them in locations like Iceland, where the ambient temperature suits them, or to the idea of "data furnaces," where those same racks, mounted in the basements of apartment buildings, vent waste heat by flue (Liu et al. 2011).

Depending on what you request, or to whom you're sending email, your packets may well pass through one of the major fiber optic "backbone" lines on the world's sea floors, and make landfall in Ajigaura, Porthcurno, Mombasa, Chongming, or span the Suez Canal (where they can be knocked out by a stray anchor), each with their own border-crossing issues of political context. System administrators install and tweak filtering software so that when your email arrives in your inbox, it does so only with only a trickle of spam instead of the torrent being sent every day, and your government may engage in filtering on a far, far larger scale.

We can go further, getting more material, beneath all the labor hours and BTUs, into the chips themselves. "Getting close to the metal" is a phrase with a rich connotative history. It means getting “deep” or “close,” in the spatial language of programming, below the mediating layers of higher-level languages (much less the distracting, iconographic candy of the graphical user interface, the glossy streamlined chassis for computing-as-appliance). It means the work one does speaks as directly as possible to the underlying structure of the hardware and the labor directed at working with it. For instance, the memory management properties of the programming language C make it possible to get to grips with an approximation of what’s actually happening inside the RAM chips in the computer, rather than pushing all that behind the curtain of mediating layers of management code. Using C can bring you closer to the metal, in that sense—to a version of interaction with the aluminum or gold and silicon in the thing itself. There are practical reasons for seeking this closeness or depth, mostly to do with exerting very fine-grained control over resources and functionality, with the corresponding danger of being able to make much riskier mistakes.

However, there is also a kind of crudely Platonic satisfaction to the idea of getting beneath the “fake” scrim of the graphics and the fussy abstractions of the higher-level languages. (It’s a satisfaction generally not shared by actual working programmers and software engineers, who have to make pragmatic production decisions.) One can get down to the ultimate, unitary material reality of hard drive sectors and the queuing of instructions on chips, down to the wires, transistors, and “vias” where two layers of a chip connect and transact—into the realm of the Johnson-Nyquist noise, the thermal agitation of the electrons in a conductor at equilibrium inside the chip. It’s hard to get more ontologically fundamental than physics, the drift and diffusion, heat, and electrostatic fields in the diode: no more language games, no more yarn-spinning in the agora. Bedrock at last! And what do we find there?

We encounter the multiple, sometimes contradictory, and sometimes coexistent experiences that obtain on the network infrastructure. Some of these realities—different kinds of subjectivities, publics, societies, and modes of living on the hardware—may be entirely distinct but nonetheless thrive together, like commensal bacteria in which the byproducts of one happen to create a suitable environment for the population of another. Others exist in tension or mutual ignorance and then, at the first moment of encounter, struggle to exterminate one another. There is a sysadmin experience, various hacker experiences (open source, black vs. white hat vs. grey hat), an Anonymous experience for many different values of “Anonymous,” and likewise for spammers; an experience for “civilian” users who just need to get by, an experience for telecom executives, one for law-enforcement personnel and cryptanalysts and eavesdroppers and so on. These many distinct social realities are at every point mutable, some more so than others. They change with time and scale, and go through flip-flops where the content, shaped by the infrastructural context, becomes the context in which the content is designed and altered.

Writing in lower-level languages and tracing the hops across the network, observing the material at work, is vitally important. It helps us see more and in more detail about network activities. However, this necessary access does not provide a unitary much less single truth pertaining across the board to every last action, interaction, and place online. These demand awareness of the diversity of perspectives and uses available, sometimes gracefully coexisting, sometimes in conflict. It might also mean tactically emphasizing one perspective over others, especially in the event of its historical marginalization, as was the case, until quite recently, with the labor involved in the Internet's infrastructure (which we will address in the following section). When we get closer to the metal, we enter a domain of many potential forms, capacities, and uses, and must be conscious that our trace of the material is one path among many coexisting virtual paths. Getting into the chip and the switch is merely the first step on this journey.

Anonymous, or Sysadmins and Superusers

Unless otherwise noted, descriptions of Anonymous in the upcoming section are drawn from Gabriella Coleman's (2012, 2013) previous research.

Moving onto the study of users plunges us into the deep end of these diverse social relationships and cultures of users and superusers installing, maintaining, configuring, and using hardware. How do they constitute and understand themselves? What is necessary to stage a successful event online? As we will discuss, Anonymous touches on the importance of infrastructure (and differing degrees of access to and control of that infrastructure), on the complex agency of various users and stakeholders, and on the conceptual and narrative problems around how to define what we mean by "Anonymous." In the following sections we will discuss technical dimensions that contribute to the visibility and stability of Anonymous, and then trouble this perspective by briefly turning to its obverse—the maintenance of secrecy and invisibility.

Weapons of the Geek: Anonymous and Popular Misrepresentations

Anonymous is one example of a burgeoning arena of political life: interventions staged by geeks and hackers. These individuals not only understand how the Internet works but also culturally constitute themselves by spending copious time online with each other as they make, tinker with, and argue about technology. As Chris Kelty has shown, many care deeply about keeping the technical architecture of the Internet open so that it can be modified, extended, and altered (2008). A good portion of these geeks, from Bangalore to Sydney, will rise up, especially when the Internet and the values associated with it like privacy and free speech seem to be in peril; a smaller class can actually subvert the Internet's routers and protocols. The short history of geek and hacker politics has already shown that there are many ways to defend the Internet, from writing open source software, to joining the Pirate Party and donating to the Electronic Frontier Foundation (EFF) and activity like this only seems to be increasing.

Anonymous is part of this wider political constellation and distinctive for being scalable, irreverent, and hard to comprehend. Indeed, the very name used by the online activists *Anonymous* bears the difficulty in profiling this entity and those that make up its ranks. Though rather opaque in its constitution, it has achieved thunderous media notoriety due to the blizzard of activist interventions between 2008 and 2012 enacted in its name, from humiliating hacking assaults against security firms to orchestrating nonviolent street demonstrations, from opposing any bill that whiffs of censorship, to allying itself with local groups, as it did with the nonprofit Food not Bombs in Orlando, Florida, after members of the charity were arrested by police.

In contrast to open source software, let's say, which is straightforward to define and easy to study, Anonymous is resistant to the kinds of stable categories that we commonly insist on for description and analysis. Not only is impossible to gather basic—much less extensive—statistical data about users, but also some Anons seed misinformation as a counter-espionage tactic. Taking stock of their unexpected metamorphosis from Internet trolling to insurgent activism, the numerous regional and international nodes that compose this network, and the string of operations they delivered in the last three years, one certainly fumbles to bundle it all up into the linear and straightforward narrative so valued by academic analysis.

Yet this sense that they are at root *amorphous* (one of the most common descriptors hung onto them in the news and academic pieces) rests on woefully ignoring the most basic of technical and material realities about them. By painting Anonymous as, foremost, nebulous, we empirically misrepresent them. While this poses a problem for academics, this omission troubles us more for its broader implications. As researchers who work on a topic of great interest to law enforcement, it is difficult not to directly broach the broader ethical implications of leaving the "metal" out of this picture; to only highlight their spectral dimensions, we inevitably drift into hyperbole, exaggerating the extent to which people find them threatening, adding to the air of mystery surrounding hackers who fly under that banner, feeding into the hysteria that law enforcement (and the defense contractors selling security and "anti-hacker solutions") self-consciously seek to cultivate.

To be sure, Anonymous is not a singularity, but is comprised of multiple, loosely organized nodes with various regional networks in existence. No one group or individual can control the name and iconography, much less claim legal ownership over them, and as such their next steps are difficult to predict. Although many individual participants therein do resist institutionalization or even defining their norms, there are logics at play and stable places for interaction. Operations don't simply spring out of the ether and can be easily linked to a particular network, such as AnonOps, Anonset, or VoxAnon (to take three of the most important ones today). At minimum these networks usually will lay claim to, or deny, being the source of an operation. Anons are also not completely or always as veiled, as they are often portrayed: there are regular participants, cloaked under pseudonymity rather than anonymity, and often they are available on stable Internet Relay Chat servers where one can interact with them every day.

Having a firm grasp of basic sociological dynamics and the technological components of operations goes a long way to help us understand what they have done, what they are capable of doing, and what they will likely not (or simply can't) do. Take, for instance, the following common mantra: Anonymous is so unstable and incoherent that any individual can take its name for good and for evil. "They are chaotic good like Robin Hood, and there is chaotic evil as well . . . There are some people that just want to see the world burn," notes Josh Corman who has written extensively (and often quite insightfully) about their actions.[4] While there have been a handful of incidents we can describe as uncharacteristically un-Anonymous or as led by one individual (as was the case with the lone anti-abortion hacker who targeted Britain's largest abortion clinic), this doom-and-gloom prediction of chaos unleashed by evil hackers remains largely unfulfilled, though it looms in the public anxieties of Anonymous as excessively dangerous, in need of a Tora Bora spelunking mission to destroy them before they crack the earth in half.

However, in the astonishing number of Anonymous-led operations of the last three years, there has never been a single large-scale diabolical operation, nor has any existing network ever expressed the desire to do something as rash and problematic as taking down the power grid, as the

National Security Agency purported in February 2012.[5] The absurdity of this claim was put into (comic) relief by one participant who quipped: "That's right, we're definitely taking down the power grid, we'll know we've succeeded when all the equipment we use to mount our campaign is rendered completely useless."

Surface technical knowledge about their operations is imperative to assess their political tactics, but these basic technological facts rarely make their way into public and academic debate. Take for instance one common tactic deployed by AnonOps, the distributed denial of service (DDoS) attack; it is often incorrectly likened to a hack that *destroys* or *damages* servers or data. This digital protest tactic, when successful, essentially squats and blocks access to some of the Internet's biggest domains, but only their Internet-facing websites. By design, if companies are following basic security best practices, core infrastructure such as financial payment processing and trading networks is not sitting wide open on the Internet waiting to be attacked. If it were, any security professional would describe such a setup as reckless malfeasance, and those sites, where downtime spells financial hemorrhage, would have been attacked to shreds long before Anonymous came on the scene. Their DDoS tactics are a political stunt; the sites that are more vulnerable to DDoS tend not to be actual important infrastructure, just symbolic of that infrastructure.

Most accounts make Anonymous out to be more mysterious than it is, distort the nature and effect of many of their digital interventions, and also overlook the ways in which Anonymous is also quite accessible, knowable, and predictable. If we were to use most writings on Anonymous as guide, one would think they would be impossible to find. It is for this reason that nearly every time Coleman has been interviewed by journalists about Anonymous, she is asked, quite sincerely: "And just how do you find Anonymous?" Her reply (usually given while staring at Anonymous participants on her screen): "I talk to them for too long every day, on Internet Relay Chat."

IRC and Sysadmin Ethics

Anonymous, like so many domains of geek and hacker political action, is partly made possible by what we might think of as surplus technical capacity, such as the labor of system or net administrators. Many of these individuals gain, develop, and refine skills at work, which are then mobilized politically by a much smaller cohort; some of these even do activist work at their day job since many employers cannot distinguish between organizing sales backups and configuring an IRC server. To the untrained eye this technical language—it might be source code, or configuration files, or scripts—just looks like extremely complicated text, and many sys/net admins take advantage of this gap in digital literacy to accomplish activist work on their employers' dime.

In the case of Anonymous, system and net administrators, among other tasks, install, configure, and maintain Internet Relay Chat servers, one of the main platforms used by distinct Anonymous networks. Once they install an IRC server, their work is not over. Often aided by a small team of individuals with similar skills, these individuals act as part plumber, part groundskeeper, and part ninja, fixing problems, maintaining the system, and fending off endless attacks. For instance, in the last year a number of the largest and most stable IRC networks—AnonOps and VoxAnon—were routinely taken down by DDoS attacks; operations came to a screeching halt. Many of these individuals also deploy their extensive and intimate knowledge of servers, networks, botnets, security, and vulnerabilities to take part in a distributed denial of service attack or hacking attack, two common tactics used by Anonymous (not all of the net or system administrators contribute to illegal actions and some Anonymous network vehemently oppose any and all illegal tactics).

Even if much within Anonymous feels and is impenetrable, these individuals and the teams tasked with doing the work of maintenance and upkeep on IRC servers are some of the more active players on these networks. Some of the networks even erect web pages proudly announcing the "staff," and these individuals are usually "operators" of important channels; as on all IRC networks, operators can ban users, grant other users operator status, and set or change the channel topic. It is simply no mystery who these people are, for their nicknames are marked by some symbol such a star or flag designating such status.

Those who install an IRC server in some respects play a godlike role, having literal superuser access to the server and thus direct control over this dominion. They can scan the traffic coming in and out of the server, they can decide to log (or not) incoming IP addresses and whether or how to cloak the addresses, all of which have serious implications for law enforcement (this is not unique to Anonymous). They can even snoop on all private conversations, although certain encryption tools can make it a more difficult endeavor.

Indeed, *all* system and net administrators who tender and tend to servers housing web content, email, and databases have access to some of the most intimate (or most boring) details of our lives as recorded in email and chats. It should come as no surprise, then, that the profession of system administration has chartered a code: “The System Administrators’ Code of Ethics.”[6] Among other topics, including law and policy, this document prominently features privacy: “I will access private information on computer systems only when it is necessary in the course of my technical duties. I will maintain and protect the confidentiality of any information to which I may have access regardless of the method by which I came into knowledge of it” (League of Professional System Administrators 2006). On the other hand, Anonymous’s technical elite are keenly aware of ethical implications of their technical power, though their thoughts and opinions tend to emerge only under certain conditions, usually strife. Take for instance this scathing critique culled from a web page, since taken down, which takes issue with the admins who run AnonOps, one of the most populated and popular Anonymous IRC networks in recent years:

- If there are no leaders, then who is there to wrest control from?
- If there’s [sic] no leaders, why couldn’t [sic] everyone read PMs [private messages] in realtime?
- If there’s no leaders, why couldn’t everyone set the target for the LOIC hivemind?
- If there’s no leaders, why do opers [operators] have to be respected, and why can I be kicked/banned for mentioning [name deleted in original posting] too many times? Why can I be banned for making a joke that [name deleted in original posting] doesn’t like?

As the list indicates, most accusations are directed at the system and net administrators who manage and own resources. Misgivings over AnonOps ran deep, owing to numerous security breaches that put participants at risk for using a piece of DDoS software (LOIC), and because an irascible administrator was regarded by many as particularly power hungry and erratic. By this time, hacking, which once occurred less frequently and certainly covertly had become an overt activity led by small groups bearing distinct names, like Antisec. They hacked for political purposes, largely to expose security vulnerabilities or search for evidence of corporate malfeasance (Coleman 2013).

By the fall of 2011, in response to these AnonOps shortcomings and to the small, necessarily clandestine Antisec crew that was behind a string of hacks, some disaffected Anons—many with significant technical skills and capacities—conceived of and built an alternative network called VoxAnon. Officially launched on February 12, 2012, VoxAnon did something new in the short history of Anonymous: its founders released a constitution explicitly outlining the purpose of the network and the role that technical guardians should (and should not) play. It is worth quoting it at length, for it gives a clear window not only into how VoxAnon’s creators strive toward a moral commonweal but, more relevant to this chapter, how close they are to the machine—they hold a keen awareness of the ways technological capacities, affordances, realities, and skills impinge on the ethical realities they seek to engender.

Constitution of VoxAnon

1. This network upholds a policy of unconditional free speech, unless that speech poses a direct threat to the network. Such a threat must be proven.
2. Network administrators must not/are not allowed to interfere in channel management unless required to do so in order to prevent a direct threat to the network, or if the channel owner explicitly requests for a network administrator to do so.
3. You have the right to privacy in private channels. No oper may join a private channel unless invited, or to prevent a direct threat to the existence of the network.
4. Network business, channel business, and organization of operations must be kept completely separated at all times.
5. In channel/operation business, a network administrator is neither more nor less important than the user.
6. Network business and discussion by administrators is to be discussed in a publicly viewable channel, unless there is a specific well-argued reason to discuss it in private.
7. Except for situations that pose an immediate threat to the network, all network-related decisions have to be made by the administrator team as a whole, and not by individual network administrators.
8. Under no circumstances should network administrators be able to view, intercept, or manipulate personal messages sent over the network.
9. Network administrators are forbidden from giving out personal information of any user for any reason, even legal. (VoxAnon 2012)

Does the existence of this constitution mean that VoxAnon lives up to the leaderless ideal of Anonymous while AnonOps fails to do so? It is rather more complicated than this binary formulation. It is too early to tell whether the constitution will act as a guide for action or whether it merely expressed frustration at a given historical moment over existing power dynamics; we suspect the latter given how Anonymous resists institutionalization. The significance of the critique and constitution lies in how they reveal certain native understandings about the close relationship between political authority and technical labor and structures; but technical affordances also contribute toward the fragmentation of power, so that even in AnonOps, where technical elites hold more power and authority, power gets dispersed as well.

On IRC, where many operations are coordinated and discussed, users are generally afforded the freedom to initiate their own operations and channels. While the network founders and staff can and do ban individuals or a channel, or discourage an operation from flourishing, most IRC networks have a long tradition—and this is no different with Anonymous—of a laissez faire, hands off approach to the creation of channels. While those who manage and control technical resources do wield extra power, there is no one group with the authority to control and command the dozens of operations, much less control other networks in existence.

Still, when it comes to single operations, there usually are, as one Anon put it, ad hoc leaders who, if they stick around and continue to work, become prominent and trusted figures. Every operation has its own history and organizational culture, and of course the technologically naive rely on participants with technical skills. Individuals with fewer technical skills become prominent operators and ad hoc leaders, especially those who pour significant time into the network and who are adept rhetoricians (Coleman 2012).

Finally, while technical operations—hacking, launching DDoS—are crucial to Anonymous, so too are nontechnical ops: this entity is just as much a well-oiled populist and distributed PR machine as is any other more traditional organization. It is made possible by the labor of geeks, hackers, and activists of all stripes who at the drop of a hat can configure servers and provide each other with infrastructure—but who also create stirring press releases and propaganda posters, edit videos to promote their cause, and deface web servers and steal sensitive content from corporations and governments, or failing that, momentarily bring websites down entirely using denial of service attacks. While these skills may be essential to carry out an Anonymous operation (as I have discussed earlier) there are still no particular abilities required of participants to join the political carnival; one must merely desire to self-identify as "Anonymous"—one of the core reasons it has so easily spread across the globe, from Japan to Brazil.

Fascination with Secrecy

If there is a certain degree of clarity one gains by paying attention to system and net administrators and the technical power they wield, for much of the time and in many other contexts the waters within Anonymous are still murky. To veer toward laborers and their machines will yield sociological dividends, but only to a degree; scholars can grasp the sociology of Anonymous but it is rather partial and incomplete, largely because Anonymous is also built on a foundation of mystery.

To research Anonymous is to descend into a rabbit hole and find oneself in a maze, difficult to navigate, always under construction, and permeated with secrets: Who is who? Who talks to whom? Who does what? This mystery is partly hinged to the very technical affordance of IRC, which is built with the flexibility for someone to log on as multiple individuals; you can also watch people talking to each other on public channels, but there are multiple hidden discussions as well. Rumors of infiltration abound; such rumors proved real in early March 2012 after news broke that Sabu, one of the most notorious hackers of the Antisec crew, had been working since at least fall 2011 as an FBI informant. You never know whether the person who has befriended you on Internet Relay Chat has done so because that is part of their infiltration. And when someone tells you something you never know whether it is the truth or strategic disinformation they are counting on you to disseminate.

Part of the allure of participating in Anonymous is intimately bound with what sociologist Georg Simmel describes as the "fascination of secrecy" and the closely related desire for disclosure and at times betrayal it engenders (Simmel 1906). Over time the researcher comes to hold and bear secrets and have secrets disclosed to them. Although many operations are open to all to participate, there are many necessarily clandestine elements to Anonymous, especially the hacking operations, making parts of it feel somewhat like a secret society. And yet, despite knowing some secrets are in fact true—or they get verified over time—there is so much we don't know or can't verify; this too is also the state of affairs many active and long-time participants find themselves in, even those with significant technical power. Venting frustration over this situation to participants (many of whom are part of the technical elite) gets the earnest, consolatory reply that they feel the same way. That is to say that Anonymous is also built on a foundation of duplicity, in the sense that what we know, see, and feel is false or ineffable or unverifiable, a confused gossamer of deceptions, indirections, stretched truths, and blatant lies, mixed with facts and earnestness.

What the preceding discussion verifies is that Anonymous is anything but Cartesian. In fact, its nature is liminal, "betwixt and between," neither one thing nor the other. Its actions and sympathies straddle the lines between logical and illogical, principled and irreverent, unpredictable and predictable, and visible and invisible.

Spam, or the Problem of Concretism

Earlier in this chapter, we raised the problem we call "misplaced concretism": assuming that something multiplex, mutable, and richly concurrent is simple, coherent, and unified. Because something has the same name over time or for many manifestations, it is thought to be the same thing regardless of elapsed events and different forms, and that consistency becomes part of how the narrative of that thing is created. This process of making a complex phenomenon into a simple object is distinct from blackboxing in the sciences, in which we deliberately bracket some intricate process while concentrating on the inputs and outputs. Rather than blackboxing with the understanding that we aren't clear on what's going on in the box, misplaced concretism assumes that we know what this event is when we make a single, simple noun of it. It makes a claim for comprehensiveness and stability and therein lies the problem. Phenomena like Anonymous and spam are not the kind of complex, difficult, but inert objects we're used to, but rather are protean sociotechnical tangles running on politically laden infrastructure and updating in real time. Having gotten close to the hardware and its users, we must finally get close to the operation of the words and concepts we use to capture, describe, and change technologies and users.

Let us take, as a practical matter toward a theoretical end, the question of how one begins researching spam's history, that is, how spam got made, and who and what made it. We could begin by gathering traces of network history, building chronologies, and collecting instances, which sidesteps the first, obvious problem: professional spammers are not voluble or forthcoming about their work (for obvious reasons). Before the field had become almost wholly criminal, and driven by malware, there were many interviews with "Internet marketers," but some of the most significant people in the business are in hiding, in jail, or operating behind layers of technical secrecy. They are visible and traceable only through the work of police and security services who monitor and occasionally capture them—much as we now know about early Gnostics through the documentation of their heresy by the Christians in the process of their eradication. Along with journalistic work (most notably that of McWilliams 2005) and a few ethnographies of unusual cases like the low-level 419 spammers in Nigeria and Ghana (Burrell 2008; Smith 2007), the best sources came from anti-spam projects—like a spammer's computer hacked by a vengeful, pseudonymous sysadmin in 2000, with the contents posted online.[7] And one must also collect spam itself, which seems trivial: what other research materials arrive unbidden at our inbox and screen, in ceaseless waves, every day?

What becomes immediately clear in doing such a survey is that the meaning of "spam" is wildly varied, and its many genres and values have shifted dramatically over time. Nobody can settle on what spam is, as we can settle (to some degree) on the meaning of "kilogram" or "cirrus cloud," and the working definitions we do have change as fast as does the network itself. This is not to say that the word "spam" as used was meaningless, but rather that there was some generally agreed-upon body of things that were considered spam—spam mail, Twitter spam, spam web pages, and spam blogs ("splogs"), and so on—and in this agreement lay three issues. First, the whole continuum of things considered "spam" covered enormously different technical infrastructures and social offenses, from simple mass-mailing scripts to enormously sophisticated global botnets with military applications; while there are common elements among them, their behavior and mechanisms are as different as a hot air balloon is from a Predator drone. Second, while it would be easy to find a reasonable, canonical example of "spam" for each format, there was enormous trouble with the edge cases, things that were spam for some and not others, creating a space for negotiation that rendered most of the silver-bullet solutions for spam (legal, political, technological) ineffective. Third, the meaning had changed dramatically over time and on different computer networks; the semantic drift, and the changes in the practices described by the word, had rendered conversations only a few years apart completely incommensurate.

Was spam commercial? Not at first, no. In fact, it was a virtually meaningless term, pure noise: a chorus adopted from a *Monty Python* sketch by early online users to flood chat channels with repetitive language—SPAM SPAM SPAM SPAM SPAM SPAM, like an air horn blown in the midst of a conversation. From there, "spam" came to mean making duplicate copies of messages or text across the network, and taking an unfair share of the scarce bandwidth. (Indeed, there are early documents concerned with appropriate behavior on Usenet—shades of the VoxAnon constitution!—which explicitly distinguish spam from commercial messages [Pfaffenberger 1996].) It could be targeted or indiscriminate, about pills or mortgages or politics—or pornography, another category of human activity with grave definitional problems. Speaking purely semantically, it was all too flexible: a noun, both collective and singular ("spam" in general versus "this spam I got this morning"), a verb, and an adjective. Spam was both a word for bandwidth-hogging garbage and the garbage itself, and this ambiguity stays with it as it is applied to a steadily expanding range of sociotechnical problems online.

Indeed, many of the problems dogging early developers of spam-filtering technology revolved around that range of problems, and the variant understandings different users had of spam. No one had a "representative" corpus with which to train the filter, both for procedural reasons (you need a mix of representative, authentic non-spam messages, many of which will be personal and potentially embarrassing) and because it proved quite difficult to draw those lines. One of the first major anti-spam corpora was constructed from the internal email of Enron Corporation, gathered during the investigation into the company's criminal business practices. (It was the equivalent to an archeologist's midden, enabling researchers to work with everything that would normally be valueless and discarded, providing insights by virtue of its accidental nature.) Figuring out which stock tips and mass-mailed Christian homilies were spam, and which part of Enron's internal culture, became a stumbling block for evaluating the filters.

Let us set this aside, though, and select an example of a spam message that everyone can agree on, a classic, instantly recognizable come-on for Viagra, say, that arrived in our in boxes this morning. We can bracket all the definitional and terminological uncertainty. What made this message, and what gave it its distinctive technical and linguistic properties? Here, again, we encounter the problem of concretism. Obviously the spammer made the message—and yet so many additional elements did, as well. It was almost certainly sent from an innocent user's compromised computer, taken over by a malware attack, and surreptitiously added to a large network of remotely controlled computers called a botnet. It was sent as part of a campaign shaped by economic and legal forces, using software that has evolved in the culture of malware programmers. We could break out some of the factors as follows:

- covert discussions and Command and Control instructions sent over Internet Relay Chat, to coordinate the machines sending messages as part of the botnet
- botnet architecture, which is built in ways that rip off, compete with, and defend against other botnets
- the semi-secret markets for selling and exploiting stolen credit cards, whose dynamics affect the choice of types of messages (if the message is the pretext for credit card theft), or
- the evolving relationships between banks willing to transact certain kinds of online purchases, and gray market and black market pharmaceutical providers (if the message is, in fact, trying to sell pharmaceuticals)
- black markets for stolen identity information
- markets for renting capacity on botnets for messages for third-party clients, and, in turn:
- third-party spam clients, and their economics—whether or not certain pharmaceuticals are promising a return on investment at a particular time, for instance
- the larger ecosystem of insecure and ubiquitous Windows boxes, which can be commandeered to act as spam-sending machines—which touches on developed and developing world economics and software cultures
- malware engineers and programmers, and their culture
- the coevolution of spam filters and the polymorphic messages made to beat them

And so on. Every element has its role to play in the constitution of this particular instance of spam. There are underlying economic, technological, social, and legal developments which are factored in—and the shifts in power, influence, and access on the part of various of groups of users and superusers, from spammers themselves to developers of unethical software, illicit Internet Service Providers, and customers and those exploited to make the whole business worthwhile. Spam manages to be at once casually common—everyone receives it—and systemically rare, in that producing a comprehensive overview (that critical mass within which explanation emerges) is laden with snags and preliminary questions whose answers, in the manner of Hofstadter's strange loops, must be given before the question can be properly proposed.

The most useful starting point when one faces this question—"Who makes *spam?*"—is to address the question itself. Latour speaks of the task of "how to assemble, in a single, visually coherent space, all the entities necessary for a thing to become an object" (2007, 142). He is using these two terms in a particular way. *Thing* is a thickly described, contextually embedded matter, in the way the phrase is used by Heidegger—the thing, whether a pair of boots or an urn, folds in the material history and the ontological domain in which it exists, speaking of a way of life and a relationship to many other entities, and so on. *Object*, meanwhile, is thinly describable and idealized, almost invisible, a ready-to-hand hunk of something whose larger existence and construction is of no concern to us. We can address it, we can move it around, we can accomplish what we need to with it. The literally Earth-changing history of the globalized, thick thing that is the automobile becomes the car-object that we drive to the store.

Consider spam in this light. We can start from a single question ("Who sent me this spam?" as Gitelman asks, looking at the context of cultural data in new media systems) and turn it on its head (2006, 155). How did the profoundly weird phenomenon of spam become as banal as it is? Which is to say: what parts have we allowed to become obscure, and what complexities are we ignoring, blackboxing, or consolidating whose particular operations would illuminate the whole of the event?

Conclusions

Hardware, the underlying material stuff, turns out to be full of politics and negotiations rather than crisp ontological certainty. Anonymous, the mysterious storm cloud of geek ire, has had nuanced and vibrant internal cultures of debate whose users and superusers are articulate about even the nature of technical power and of the secrets they keep and selectively reveal. Spam, the noun, verb, and adjective which everyone recognizes without being able to precisely and entirely define, is a moving space. It draws a line around certain overlaps, where law, common online practice, technological and financial innovation and international politics meet, an intersection of hardware, users, and concepts feeding back and forth. The work of studying these events lies partially in our patience with their complexity, ambiguity, and layered character.

In working on phenomena like Anonymous and spam, we are careful to put off what in the lexicon of quantum mechanics is called "collapse"—when several possible states condense down at observation into one. The work we have described here implies both a methodological and a theoretical approach to forestalling this collapse, keeping the superposition of simultaneous meanings, values, and implications in play. We do this to compensate for the difficulties in getting a complete picture—with the secrecy, the simultaneity, the obscurity—but also because it is more accurate. There is no Anonymous, no spam, no Internet; there are, rather, many of each, simultaneous, all true at once and all tangled up together. Is the Internet making us stupid or making us smart? Is it empowering dictators or liberating populations? Is it destroying privacy or encouraging a proliferation of new identities and personae? Is it the domain of bullies and trolls or the framework for new, global, voluntary communities? Yes, all of the above, and more. The loop of hardware–users–theories makes it easier to sustain this collapse-resistant inquiry.

This raises the issue of time, an overlapping element in our master question of "who makes," and the smaller questions of hardware, users, and stories that it breaks out into. Both our subjects and our approach entail thinking in a distinctive temporality with two different properties. First, there is simultaneity: for many network events, including those described here, much of consequence is happening all at once, on an enormous scale, with nested feedback and overlapping interdependencies. This is particularly salient with Anonymous, which bears a singular name but is simultaneously composed of multiple nodes. Hardware, users, and the stories users and observers tell are all affecting each other, up and down the stack. Taking questions like "Who makes spam?" or "What makes Anonymous possible?" as loops of related answers, whose circulation doesn't stop, helps us create better descriptions. This brings up the second temporal issue in our work: the answers remain fundamentally provisional. While we should strive to reach a stable point of analysis which can accommodate different perspectives—material, social, historical—we will only remain there as temporary visitors. Prompted and provoked by a different set of concerns, or an unpredictable series of events that can dramatically shift possibilities (such as happened with Wikileaks and the technological politics of leaking [Brunton 2011] or when Anonymous unexpectedly took on the project of leaking [Coleman 2013]), our objects of analysis will move forward and force us to catch up. We may get closer to the dynamics of the machine and closer to the fact of the metal, but our work is asymptotic: we will never quite arrive.

Notes

[1] Thanks to Geof Bowker for "misplaced concretism," an excellent turn of phrase.

[2] Greenpeace International, "Make IT green: Cloud computing and its contribution to climate change." Paper presented at Greenpeace International Conference, Amsterdam, 2010. http://www.greenpeace.org/international/Global/international/planet-2/report/2010/3/make-it-green-cloud-computing.pdf, accessed May 16, 2012.

[3] Triple8 Networking, "Data centers." http://www.triple8.net/about_datacenter.htm, accessed April 12, 2012.

[4] Robert Lemos, "Anonymous must evolve or break down, say researchers," 2012. http://www.darkreading.com/advanced-threats/167901091/security/vulnerabilities/232900561/anonymous-must-evolve-or-break-down-say-researchers.html, accessed June 3, 2012.

[5] National Cybersecurity and Communications Integration Center, "Assessment of anonymous threat to control systems." Bulletin A-0020-NCCIC / ICS-CERT –120020110916, September 16, 2011. As released by Public Intelligence, http://publicintelligence.net/ufouo-dhs-bulletin-anonymous-hacktivist-threat-to-industrial-control-systems-ics/. Accessed November 22, 2011.

[6] "The System Administrators' Code of Ethics." League of Professional System Administrators, 2006. https://lopsa.org/CodeOfEthics, accessed May 10, 2012.

[7] Elías Halldór Ágústsson's website, Beyond Enemy Lines. http://elias.rhi.hi.is/beyond_enemy_lines.html, accessed December 5, 2011.