2
Hacking the Hacktivists

As this book's introduction discusses, the internet's decentralized architecture presents opportunities for nation-states, data-gathering corporations, and political movements. Yet it also has created opportunities for technology users and activists, who may resist forms of surveillance and tracking, concerned with the amount of data being gathered about citizens across seemingly many aspects of their lives.

The term "hacker" brings together a number of typologies, from "white hat" activists devoted to democratic principles and values to malevolent "black hat" hackers primarily interested in the subversive breaking of laws without a necessary commitment to democratic values. This chapter's interest is in exploring the dialectically related assemblages produced by both states and hacktivists as they engage in their work with digital technology. These assemblages, like the many others we share throughout this book, are not restricted to the internet itself in a closed sense, but instead bring network technologies into a dialogue with a number of other social and technical factors.

To best understand the game of cat and mouse around hacktivism we must see the internet in relation to a number of policing efforts, which place networked technology in a precarious relationship with several legal and technological practices. This chapter's contribution is to illuminate assemblages that are at the center of the hacktivist battle for a free and open internet and the values for which it stands. The

assemblages of hacktivism includes *legal statutes*, technologies of *encryption/decryption* that aid and disrupt surveillance, and three key practices employed by both hacktivists and states: *selfie-incrimination*, *versioning*, and *edgework*.

There are a multiplicity of states implicated in this discussion, from neoliberal democracies, such as in parts of Europe and North America, to networked authoritarian states that maintain strong ministries of information. Nonetheless, every nation-state, regardless of its intention or history, is in an interesting position today as it considers how to use digital technology to balance issues such as citizen privacy or civil rights relative to security and the desire to control and know about one's constituencies. This chapter considers how the use of technologies for dissent is shaping legal and policing practices in the United States and United Kingdom and, via their extra-judicial actions, worldwide. We note that though our focus is on neoliberal democracies, one can see battles with hacktivists also relative to a range of authoritarian regimes wishing to control and manipulate information.

Recent Histories of Hacktivism

Chelsea Manning leaked secret military documents to WikiLeaks and was sentenced to 35 years in prison in Fort Leavenworth, Kansas. Jeremy Hammond is currently serving 10 years in a federal prison for hacking and releasing documents about US military subcontractor Stratfor. Aaron Swartz received a felony conviction and was facing a prison sentence of 25 years for hacking documents out of JSTOR (a scholarly article database) when he committed suicide in 2013. While all three are American citizens, and therefore subject to American laws and punishments, the US administration pursues hackers located overseas for alleged criminal activities. Although their tactics are often technically illegal, hacktivists tend to be united by a common belief that it is more important to share information and fight for an internet that is public rather than honor private property or follow what they see as unjust laws.

The decentralized architecture of the internet has been exploited by both states and hackers in their ongoing battle

over the control versus liberation of information. The practices of neither, however, demonstrate an acceptance with the internet "as is". Instead both states and hackers exploit the internet's relationship to other technologies that allow for data to be either monitored or authored anonymously. In this sense, the internet is mutable due to being part of an assemblage inclusive of other systems and tools. Thus we see an ongoing battle around technologies to evade and support monitoring – from IP address-scrambling and email encryption to tools that aid surveillance.

Within the United States, practices of dissent such as civil disobedience were defended by the original writers of the US Constitution. Since the attacks of September 11, 2001, and likely as we move forward with the Trump administration, both domestic dissent within the United States and political upheavals outside of the nation have been increasingly labeled as forms of terrorism. Terrorism has emerged as a discourse to be broadly interpreted and acted upon by a range of governmental agencies, corporations, and media networks. The expansion and growth of the internet, via the world wide web and mobile platforms, has thus made it increasingly relevant as a battlefield between the visions of hackers versus the surveillance, digital propaganda, and "anti-terror" initiatives launched by governments and corporations.

Recently a number of hacktivists and communitarian activists have been prosecuted in high-profile court cases. Individuals like Edward Snowden, Julian Assange, Chelsea Manning, Jeremy Hammond, Barrett Brown, Ross Ulbricht, and others are being investigated or have been sentenced to prison. This includes a range of activists who push for governmental transparency and the creation of underground countercultural technology-mediated communities, such as the darknet marketplace Silk Road. The manner in which these hacktivists were investigated, prosecuted, and sentenced reveals the practices of a networked state on the edge of legality, or engaged in *edgework* (Fish & Follis 2015, 2016), practiced by both criminal investigators and hackers.

In this chapter we focus on politically motivated hacktivists of two kinds. The first are *crackers*, computer "geeks" who break into secure systems for the challenge and pleasure, and also in order to bring to the public various forms

of information. The second type of hacktivist could be seen as within the lens of *alternative computing*, including those who create illegal systems that are designed to challenge the legitimacy of the state or powerful corporation. The Silk Road is an example of the latter, but so too is WikiLeaks, the publisher of whistleblown information.

Central to the motivation for hacking is the pursuit of information that is often obscure or outright forbidden. For this reason, hacking necessitates a "politics of transgression" (Coleman 2003). This ethic often develops into a morality as it becomes socially adopted and transformed over time. On one level, hackers' technical imaginaries begin with discussions of computers, networks, protocols, and a distaste for proprietary software. On another level, hacker conversations reveal moralities regarding free speech, meritocracy, privacy, openness; and individualism. Hacker "morality" (Coleman & Golub 2008: 267) thus considers principles of selfhood, property, privacy, labor, and creativity for the digital age.

The quintessential hacker WikiLeaks editor Julian Assange has long argued for the importance of maintaining the transparency of the activities of those with power and privilege. He has stated that "the greater the power, the more need there is for transparency, because if the power is abused, the result can be so enormous. On the other hand, those people who do not have power, we mustn't reduce their power even more by making them yet more transparent" (Aitkenhead 2013). Hackers like Assange have seemingly embraced the challenge of "liberating information" to then force the powerful to be accountable for their actions. Like Assange, who is currently holed up on the third floor of the Ecuadorian Embassy in London, the hacktivists discussed in this chapter have been persecuted for their moral and technical imaginaries about how the world should be. While not all hackers, even the ones we highlight in this chapter, are the same in terms of their moral motivations and digital practices, we believe it is useful to identify shared elements whereby they and the systems they fight against incorporate the internet into an assemblage with other elements.

A common interpretation is to see hacktivism as a form of civil disobedience. Civil disobedience has a varied history across the world. In the United States, some scholars have argued

for the legality of this form of protest (Calabrese 2004), while others, such as the Metropolitan Police in the United Kingdom (Cluley 2011), warn potential digital protestors of its illegality. Hacktivist civil disobedience is thus an example of liminality, occupying a position that is at both sides of a boundary or threshold. Jürgen Habermas argues that "[t]he 'right' to civil disobedience remains suspended between legitimacy and legality for good reasons. But the constitutional state which prosecutes civil disobedience as a common crime falls under the spell of an authoritarian regime" (1985: 112).

The success of the prosecution, the rate of incarceration, and the draconian sentences handed down to hacktivists challenge the notion that the internet remains a place for transgressive political activism or civil disobedience. It is evidence that public speech in an increasingly digital world can be increasingly used to police, apprehend, and control. For a time online anonymity and pseudoanonymity were not difficult to achieve and with these tools evade prosecution. The assembled nature of the internet, a "heterogeneity of component elements" (Anderson, Kearnes, McFarlane, & Swanton 2012: 174), allowed for hidden spaces and darknets, and thus immunity. At the same time the increased existence of all sectors of society online – government, finance, civil society, private information – also made ripe the conditions for new forms of political activism focused on using computers and networks to open up and publicize otherwise private information, or to subvert systems of political and social power. These tensions between privacy and publicity are inherent in a system of such heterogeneous diversity. Government and corporate forces may push for transparency of citizen users and enemy states, though not for their own activities, as a matter of "national security." In this ideological confrontation, hacktivists are antagonists to the state, and competitors over the information commons. Thus the state has a vested interest in making the opaque conditions of the internet clear by bringing it into the light of law. State agents may attempt to incorporate the internet into an assemblage involving laws and interpretations that can then shape hacktivist persecution. In contrast, hacktivists attempt to develop assemblages around the internet that involve leakages, covert community formations, and pseudoanonymity.

This chapter analyzes hacktivists, how some have been caught, and the underlying ideology of the states that pursued them. We find that in addition to technological and legal elements, the hacktivist–state assemblage must include three extra-judicial practices: (1) *selfie-incrimination*, or self-disclosure on social media that unintentionally empowers surveillance systems; (2) *versioning*, or deliberate uses of technology to deceive one's adversary and therefore make one's identity vague; and (3) *edgework*, or technological or other practices that lie in the zone of liminal legality (Fish & Follis 2015, 2016).

Our conclusion is sobering. Our analyses of these assemblages reveal that the state retains an upper hand by defining the grounds of legality and that its use of non-technological elements such as the manipulation of the legal system (e.g. in the United States) or brutal killing of those who dissent (e.g. in Iran, Egypt, Saudi Arabia, and other countries) has paved the way for a world today where hacktivists are increasingly persecuted. Where this battle goes will in large part shape what type of internet the world will experience moving forward.

The Battle between Agency and Structure

A long-standing concern within social theory has been the relationship between *agency* and *structure* (Bourdieu 1990). In general, theorists have tended to prioritize the importance of one or the other of these as they speculate on the factors that constitute and shape social life. For example, scholars in cultural studies tend to emphasize the creativity, flexibility, and evasiveness of cultural practices, while others, such as functionalists, political economists, and Marxists, often ascribe a constraining or limiting role to individual agency because of the dominance of social and economic institutions (e.g. laws, courts, schools, government bureaucracies, the labor market, etc.). Though these forms of scholarship position agency and structure as oppositional and independent, we believe that an understanding of hacktivism and states must consider agents and the social structures within which they act as mutually constitutive (Giddens 1984).

Classical debates over agency and structure are complicated by the increasingly prominent role played by technology in social life. Here we find a parallel dynamic that maps onto the agency/structure binary. Hackers, for example, tend to argue that the internet embodies sacrosanct principles of freedom and autonomy. This posture is often technologically deterministic and teleological as they point out that the free play of technology and innovation drives history. Criminal investigators and lawmakers, on the other hand, often argue that the internet is a system capable of being regulated and modified in line with dominant social and institutional norms. In other words, they prioritize the social construction and regulation of technology as a necessary constraint on the anarchy of individual autonomy. The inability of the internet to fully support either vision is evidence of its generativity as well as its incompleteness. It speaks to how a far more insightful understanding of this networked technology infrastructure would consider it within an assemblage of other legal, technological, and policing factors and practices.

Following Anthony Giddens' (1984) work on structuration and Bruno Latour's (1996) analyses of scientific knowledge production, we see hacktivists, criminal investigators, and the practices engendered by the internet in a state of co-production. In this sense, the internet is being collectively reassembled via the ongoing battle between hackers and agents of the state. This is consistent with a number of studies, not solely of the internet, but within the larger domain of science and technology itself. For example, Latour (1996) revealed in his ethnographies of laboratories how an older version of elitist top-down science was replaced by a "collective experiment" in which scientists worked with policymakers and the public in forming scientific knowledge. We can look at this chapter's themes with a similar lens.

Relationships between hacktivists and states are not premised on an equal access to power but are rather characterized by inequality, friction, and conflict. Anna Tsing, in her ethnography of the relationships between environmentalists, indigenous people, and illegal loggers, identified the spaces where these actors meet as "zone[s] of awkward engagement" shaped by *friction* and the "awkward, unequal, unstable, and creative qualities of interconnections across difference" (2005: 4). These interconnections "remind us that heterogeneous and unequal encounters can lead to new arrangements of culture and power" (2005: 6). In this sense, the ways agents of the state and hacktivists reassemble the internet are relative to historical and ongoing relationships of power inequity. On the one hand, states use their immense technical and legal resources in order to create "lines of sight" that transect the internet, attempting to create new forms of visibility. Yet on the other, hacktivists have a moral interest in supporting privacy and evasion of surveillance.

Despite ongoing state initiatives to spy on, monitor, regulate, and control the "space" of the internet, it is not a terrain dominated by the state (indeed the reverse is in some respects the case). The state's tactics thus must involve reading and mapping the quickly shifting terrain of online interaction until openings appear in the hacktivist community that bring particular targets within its line of sight. It is here that the state can bring to bear its particular strategic advantage by proceeding under the mantle of its offline home terrain: its ability to exploit legal and policing factors.

The above is to say that until investigators are able to move proceedings offline, the state must approach the "space" of the internet much in the same way as hackers approach the terrain of the state. Both adversaries must be nimble, flexible, and mobile: their reassembled internets are configured by the tactics used to support their agendas and debilitate their adversaries. They must be nomadic, in essence defying what Gilles Deleuze and Félix Guattari (1987) have described as the "war machine" of the traditional state. Yet in the past nation-states have often not been able to appropriate the tactics of their nomadic adversaries owing to their bureaucratic histories and forms of structural overhead. All of that shifted in the Western world in the late 20th century, as we now describe.

Netwar

According to one classical definition, the state is an organization that successfully monopolizes the means of legitimate violence in a given territory (Weber 1946: 78). In this view,

a state is primarily defined through its institutional bureaucratic structure, its capacity to penetrate and organize social relations through institutions, as well as its instrumental use of violence and coercion to maintain authority (Mann 2012). Toward the end of the 20th century, this "Westphalian" model of the sovereign state (as autonomous and supreme within its territorial boundaries) was said to undergo a process of "downsizing" as a result of the combined pressures of the information age and globalization (Castells 1996). For a number of commentators writing in the 1990s, the scale of international cross-border flows, as well as the increasing global prominence of international organizations, multinational corporations, and other non-state actors, pointed to an eclipse or "withering" of the state on the global stage (Reich 1991).

However, the late 20th and early 21st centuries witnessed a dramatic expansion of the nation-state's punitive, repressive, and covert activities across the world, particularly within Western Europe and North America. The events of 9/11 and the ensuing Global War on Terror systematically eroded or blurred previously held distinctions between matters of external and internal security (i.e. the distinctions between war and crime, military and police, detention and imprisonment) (Bigo 2000). Discourses of terror, or, if you will, "shock doctrines," helped pave the way for this erosion of civil liberties and relative anonymity not just in the physical world but also in the relationship of citizen users with internet technologies.

These dynamics mark the origins of the "networked state." Key insights into this concept come from the work of David Ronfeldt and John Arquilla, collaborators at the US military-funded think-tank the RAND Corporation. Ronfeldt is a senior social scientist at RAND and Arquilla is a RAND consultant and professor of defense analysis at the Naval Postgraduate School. Their research on networked war ("netwar") and the networked military state ("counternetwar") draws from the sociology of networks and activism and is intended to inform the US military about how best to combat technology-facilitated terrorists, revolutionaries, and activists. Today, their ideas are operationalized against hacktivists, which may fall into any of these three categories as far as the state is concerned.

Whilst writing the papers analyzed below, Arquilla advised the office of Donald Rumsfeld, the Secretary of Defense under

George W. Bush. A supporter of preemptive war, aggressive cyber-attacks, and National Security Agency (NSA) wiretapping, Arquilla (2013) has argued for the importance of big data to "search out small cells that bedevil our era." These "small cells" include "peaceful social activists," Zapatista indigenous activists in rural Mexico, "malcontents, ne'er-do-wells," and "anarchist and nihilistic leagues of computer-hacking 'cyboteurs'." On the "bright side" are the "good guys" like RAND, the US Army, and the police state (Ronfeldt & Arquilla 2001: 2–3). In a sense, Arquilla's work supports the networked state to engage in efforts to root out and subvert the tactics of not just hacktivists but any form of opposition that takes on a networked form. Arquilla, Ronfeldt, and their colleagues at RAND recommend that the US military and state-based police and surveillance institutions restructure around the model of the network in order to respond to "adversaries" in the information age.

Beginning in 1993, these scholars began to define "netwar" to "refer to the emerging mode of conflict (and crime) at societal levels, short of traditional military warfare, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age" (Ronfeldt & Arquilla 2001: 3). Netwar is made possible by the proliferation of networked technologies which enable small groups or cells to organize and "swarm" in their coordinate attacks, an "amorphous, but deliberately structured, coordinated, strategic way to strike from all directions at a particular point or points, by means of a sustainable pulsing of force and/or fire" (Ronfeldt & Arquilla 2001: 12).

The recommendation from RAND to the US military is that governmental agencies should organize themselves in cell-like structures, so that they may more dynamically share information and be able to swarm upon targets. It is important that the state not abandon hierarchy entirely but blend hierarchies and networked organizational structures. In his study of post-Soviet economies, sociologist David Stark (2009) calls these mixed hierarchies and horizontalities *heterarchies*. The US Counterterrorist Center at the CIA is a good example of an adaptive heterarchy. The Israeli Defense Forces (IDF), likewise influenced by information theory, are also adopting a cell-based swarm approach to battle. In terms they appropriated from

Deleuze and Guattari, they have encouraged their soldiers to theoretically "deterritorialize" the urban fabric and literally "walk through walls" in order to apprehend the Palestinian opposition (Weizman 2007: 185).

Heterarchy is thus not merely a philosophical structure or formation but interwoven with three factors or practices that characterize the assemblages associated with the internet in an ongoing battle between the networked state and hacktivists. To spell this out further, we describe *selfie-incrimination*, *versioning*, and *edgework*.

Selfie-incrimination

Every day, it seems, another hack or leak occurs. In June 2015, Chinese hackers were able to gain access to the US Office of Personnel Management (OPM), acquiring the personal data of 4.10 million former and current employees (Nakashima 2015). The FBI says the leak was bigger, containing data from 18 million people (Perez & Prokupecz 2015). Yet when the US NSA and Chinese hackers are not exfiltrating personal information, technology users are voluntarily providing it to private Silicon Valley corporations, whose security is not always stellar. The users are being hacked themselves by consenting to have their data opened up for corporate monetization and political surveillance, often by signing onto bureaucratic and obfuscating terms of service.

One billion gigabytes are currently stored in data centers, the same as 67 million iPhones (Holt & Vonderau 2015). Every day, 350 million photos are uploaded to Facebook. Social media has become the platform for self-expression. The use of the word "selfie" increasing by 17,000 percent in 2013 and 50 percent of the photos on Instagram in the UK by 14- to 21-year-olds are self-portraits. We are thus living in an "infoglut" constituted by an abundance of self-expression (Andrejevic 2013), which in turn gives rise to "selfie-incrimination" when those deemed as criminals wilfully self-expose online.

Cynics see digital self-expressivity as narcissistic (Keen 2015), while, in contrast, optimists witness in the selfie craze the seeds of personal and community empowerment (Nemer & Freeman 2015). Regardless of the academic debate, law enforcement personnel are increasingly using social media to generate evidence and support policing activity (Risen & Poitras 2014). A recent US-based study concluded that 80 percent of investigators searched online for information about suspects (Zadrozny 2015). As a sergeant from an Arizona police force stated, "I think social media used properly could really be a very good tool to help us do our job and really cheap because it doesn't cost anything" (Fox10 2011).

At times, hacktivists themselves fall prey to the desire for self-expression. The most absurd case is that of Higinio O. Ochoa III, an associate of Anonymous. After cracking and releasing Arizona police officers' addresses and phone numbers, Ochoa proceeded to post a tweet linked to these documents under the Twitter handle @Anonw0rmer. Associated with the tweet was an image of Ochoa's girlfriend's breasts above a sign bragging about the stunt. Yet unfortunately for Ochoa, the image contained geolocatable metadata leading to his arrest (Diaz 2012) (figure 2.1).

In another example, selfie-incrimination played an integral role in identifying Ross Ulbricht, aka Dread Pirate Roberts, the "kingpin" of the online drug platform the Silk Road. On his LinkedIn page, Ulbricht described his work as "creating an economic simulation to give people a first-hand experience of what it would be like to live in a world without the systemic use of force" (figure 2.2). Ulbricht used his real name on a coder site to ask, "How can I connect to a Tor hidden service using curl in php?" "Curl" is the code used on Silk Road's web servers. Ulbricht's capture was the result of these breaches of private information on public networks, leading to his apprehension and a brutal sentence of life imprisonment.

Online platforms, while useful for personal communications, also thus assist criminal investigations. This is self-incrimination in action. Online platforms also can deceive through the use of fake profiles and misinformation. On the policing side, new skills of criminal investigation are needed, such as the investigator's knowledge of software code. Such expertise would allow a technical question asked by Ulbricht on the Stack Overflow forum to be linked to the underlying

Figure 2.1 Higinio O. Ochoa III's selfie-incrimination

technical architecture of the Silk Road platform. Thus, investigators need to shift their practices and formations in accordance with the netwar position we have described. Such evidence may not always be intentionally "'selfie"-based, but gathered inductively through a suspect's online activity across multiple digital platforms. Data aggregation and retention are

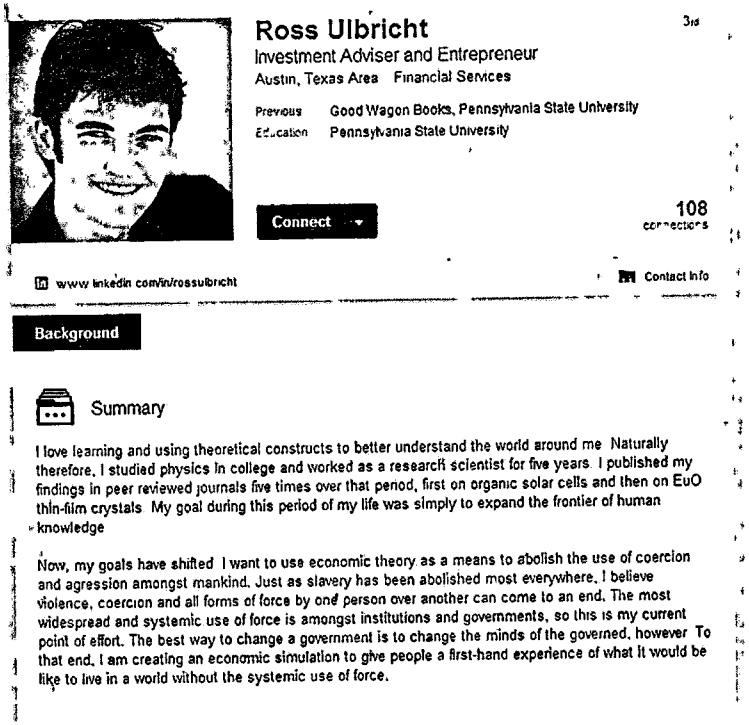

Figure 2.2 Ross Ulbricht's LinkedIn page

thus key in piecing together information garnered from selfie-incrimination.

One notable exception to selfie-incrimination might be the "semi-naked" (Coleman 2014: 183) hacktivist Barrett Brown, a freelance journalist who had written for *Vanity Fair*, the *Huffington Post*, and the *Guardian*. Though prosecutors originally charged Brown with ten counts of aggravated identity theft and two counts of credit card fraud for posting an HTTP link to leaked emails from Stratfor, these charges were eventually dropped when he pleaded guilty to the crimes of accessory, obstruction, and threatening a federal officer in exchange for a deal. Unlike other cases of selfie-incrimination, Brown attempted to take on a journalistic identity as a Constitutional

shield. And ultimately it was his publicity that made him an easy target. Being a cyber-activist with a link to a battery of controversial files and contacts in the journalistic community made him even more visible.

While it is unsurprising that an important step in an investigation is a Google search of a suspect's personal details, it is important to note how social media evidence is admissible in affidavits and other court documents. This is an example of how social media activity combined with legal statutes can contribute to an assemblage shaped by police and security forces.

In the past, states went to extensive lengths to make their populations legible and readable; state interventions in society (e.g. vaccination campaigns, conscription of soldiers) required the creation of "visible" units that could then be observed, identified, monitored, or manipulated (Scott 1998: 183–4). In "seeing like a state" (Scott 1998), citizens and constituencies could be classified and quantified, allowing them to be calculated and monitored to support how resources are distributed. One can view the history of citizen databases, lists, and census data in such a manner. Yet instead of gathering information through formal mechanisms of requesting citizen input, states can monitor the social media activity of their citizens to make them intimately legible. What is crucial here is not just that social media *per se* are premised upon visibility but that the legibility of individuals is a basic embedded component of online interaction. The lack of understanding around how citizen users are made legible through the monitoring of their data increases the likelihood of selfie-incrimination.

Versioning

A second theme to be considered around the hacktivist assemblage is *versioning*. The practice of versioning emphasizes the portabililty, process orientation, and performativity of software culture. Anonymity, pseudoanonymity, privacy, and secrecy may all be pursued in online spaces that do not have "real name" policies, such as Facebook. Despite the fact that users of social media accidentally or purposely deposit digital

artifacts (geolocation, IP logs, cookies) that can be traced back to individual users, some social media platforms continue to be spaces for identity performance. We introduce the term "versioning" in order to discuss how hackers' and criminal investigators' identities are mutable. This reflects the mirror image of selfie-incrimination, as it facilitates the ability to evade apprehension.

The ability to be anonymous online has increasingly resulted in the development of a culture of shifting identities. As we have alluded to, hacker culture contrasts greatly to the fixed way by which the state has traditionally seen identity and its linkages to textual evidence. The state has traditionally tended to identify its constituencies as sets of static identities, while the slipperiness of hacker identity speaks to a different mode of performance (Butler 1997). Hackers, in this sense, are postmodern; they are skeptical about the links between identity and what is said online. In this way, hacker culture personifies postmodern linguistics, whereby the signifier is disconnected from the signified (Derrida 1978). The clash over versioned identities represents a major flashpoint in the battles between hacktivists and states.

As our previous discussions of netwar suggest, cybercrime investigators increasingly use hacker practices and values. This involves entering into online spaces where hackers discuss their work, such as internet relay chat (IRC) rooms. To better aid their success, undercover cybercrime investigators may also perform versions of themselves in the pursuit of hackers. It is in this manner that versioning represents an important practice that must be considered when we think of the hacktivist assemblage.

The Silk Road case reveals how the pliability of identity is used both in investigations and in criminal acts. US Drug Enforcement Agency Special Agent Carl Force was employed in an undercover role in the Silk Road case, infiltrating Ulbricht, and posting under a number of fake names. But according to Tigran Gambaryan, special agent with the criminal investigation division of the Internal Revenue Service, his work was not only for the state but also for himself. In a statement, the Department of Justice described how Force, "without authority, developed additional online personas and engaged in a broad range of illegal activities calculated to bring him personal

financial gain" (Department of Justice 2015). Force allegedly took hundreds of thousands of dollars in the form of the anonymous currency bitcoin destined for the Silk Road and deposited this in his own personal bitcoin wallet. Using as many as three pseudonyms, he was accused of wire fraud, money laundering, and falsifying government documents before being convicted and sentenced to 78 months in prison in 2015.

Yet another agent investigating the Silk Road was US Secret Service Special Agent Shaun W. Bridges. Much like Force, Bridges supplemented his undercover work with the development of "additional online personas and engaged in a broad range of illegal activities calculated to bring him personal financial gain" (US District Court for the Northern District of California 2015). According to a criminal complaint filed against Force and Bridges, the latter stole $20,000 in the form of bitcoins from the drugs marketplace after gaining control of a Silk Road customer representative's account. Bridges then liquidated the bitcoins for $820,000 and deposited the sum in a personal investment account. Although seemingly empowered by their supposedly versioned anonymity, both Force and Bridges – much like the hacktivists discussed above – were victims of their own selfie-incrimination, with Bridges being sentenced to 71 months in jail in 2015 (Farivar 2015). In this sense, loose or careless versioning can quickly transition into selfie-incrimination.

Versioning, like selfie-identification, thus represents a critical snapshot of how two visions of a fragmented and generative – and, some may say, "broken" – internet contest one another. Fluidity, a natural state of the postmodern digital culture of hacktivists, intuitively blends well with an ever-changing landscape of software and technology. We think of platforms such as Facebook or Twitter as stable, yet with deeper scrutiny recognize that they, like other technologies, are shifting and mutable.

State agents have accordingly had to embrace such a dynamic techno-versioning culture in their networked organization structure, surveillance and apprehension practices, and attempts to manipulate judicial and policing systems. Yet how can the legal system, based on historical precedent and tradition, be versioned to make possible the reassembled internet that the state seeks? The answer is discussed around the concept of

edgework, the third and final component we identify as we think about assemblages of hacktivism and the state.

Edgework

Network theory has come to be a nearly ubiquitous linguistic and analytic approach toward understanding the social impacts and effects of internet and new technology use. In social network analysis, which as a structural analysis of social relations that existed many years before the advent of digital networked communications, individuals or entities are identified as nodes that then may intersect with others as demarcated by links.

In a network, the lines that link one node to only a single other are considered peripheral, or the *edge* of the network. They may be seen as less relevant or central in the ability to understand a sociotechnical phenomenon, and therefore unimportant in an analysis of the internet.

Perhaps surprisingly, however, the practice of surveying the edges of a network – and guarding its boundaries – is important for both internet and social media technology companies. For example, *edgerank* is the name Facebook gave to the algorithm that suggests supposedly relevant content on its news feed. Facebook's algorithm attempts to connect the separate nodes in what CEO and founder Mark Zuckerberg calls the "social graph," or the realm of all possible person-to-person connections. These algorithms make "ordering" decisions on relevance, yet how these decisions are made, including their epistemological bases, remains mostly invisible. While Facebook monitors and curates the social graph of each of its users, its methods remain mostly secret.

Not only are the edges of the network important on a commercial and technical level, but they are also essential in understanding the cat and mouse game of hacktivism and policing. Edgework, which synthesizes the concept of the edge from network theory and ideas from cultural criminology that emphasizes the powers of transgressing boundaries (Lyng 2005; Lyng & Matthews 2007), can be used to describe the way cybercriminal investigation explores the extremities of the

social graph and articulates what is legible and legal. In doing edgework, cybercrime investigators approach and appropriate methods from those already on the margins of legality. In attempting to transform the opaque into the transparent, and the anonymous into the identifiable, criminal investigators use edgework as a practice to fix and read a fluid and dynamic online world. Criminal investigators are making the unique cultures the internet encouraged through versioning and self-expression less legal and more vulnerable for policing and prosecution.

While they do this, criminal investigators skirt the edges of legality. As stated by James Chaparro, former Assistant Director for Intelligence for US Immigration and Customs Enforcement:

> There is always this balance of trying to be forward leaning in your investigative techniques and making sure you don't trample on rights at the same time. You want to stay well within the bounds of your legal authority because if you step over the line the evidence is going to be tossed, it isn't going to be admissible in court and you may wind up jeopardizing the outcome of an entire investigation. And so what I think agencies will try to do is they will want to step right up to the line, maybe get a little bit of chalk on their toes, but don't step over it. (Winter 2015)

Social media companies, criminal investigators, and hacktivists patrol the edges of the network, uncovering and translating otherwise private information and identities into public documents. This competition for resources has these actors at odds with each other and at other times as strange bedfellows. According to Julian Assange (2014), all three "collect a vast amount of information about people, store it, integrate it and use it to predict individual and group behaviour."

States, however, have tactics not available to hackers, namely the criminal justice system and greater financial and infrastructural resources with which to improve their position (Fish & Follis 2015, 2016). Through its edgework practices, the state may seek to curtail that which hackers see as a digital commons. Indeed, through the criminal justice system, "governments and corporations seek to erase the antagonistic history of the Internet, rewrite its rules to favor market and

corporate activity, and marginalize public goods online in favor of private property and commercial interests" (Beyer & McKelvey 2015: 892).). Thus, the race to uncover incriminating information as well as the battle to defend it through encryption have come to constitute the ever-receding *edges* of the internet and social media.

"Pushing the Boundaries" with the NSA and GCHQ

Considering selfie-incrimination, versioning, and edgework as factors to be considered in relation to technical, policing, and legal elements within the hacktivist–state assemblage, we now consider what these mean together in relation to a major contemporary hacktivism case.

We wish to explore what the documents released by Edward Snowden reveal about the methods of the networked state. Using the Snowden Surveillance Archive (SSA), which has digitized and made searchable all of the documents thus far revealed by Snowden, we were able to critically analyze documents containing key search terms such "hacktivism" and the hacktivist collective "Anonymous" and cross-reference these terms with NSA and GCHQ (Government Communications Headquarters) programs such as ROLLING THUNDER and divisions such as the UK's Joint Threat Research Intelligence Group (JTRIG), which targets hacktivists. The Snowden documents provide supportive insights into how selfie-incrimination, versioning, and edgework converge. These explorations and provocations of criminality reveal the extent to which the security state apparatus has targeted hacktivism as an excuse for dominating otherwise opaque areas of the internet.

A vivid example of the networked state's convergent uses of versioning and edgework is JTRIG, a section of the UK's GCHQ, the British partner in the Five Eyes global intelligence alliance focused on monitoring internet and telecommunication signals. JTRIG has the capacity for computer network attacks (CNA) and computer network information operations (CNIO). Their mission is described as to "Destroy, Deny, Degrade, Disrupt, Deceive and Protect" (The Intercept 2014:

slide 2). In a slide that features the logos of Twitter, flickr, YouTube, and Facebook, CNIO describes its mission as "propaganda, deception, mass messaging, pushing stories, alias development, and psychology" (The Intercept 2014: slide 4). It outlines its capacities for "disruption," including "masquerades, spoofing, [and] Denial of service" on phones, emails, computers, and faxes (figure 2.3). And finally, in another top secret document, JTRIG describes its "hacking process" under the acronym RICE for "(R)econnaissance, (I)nfection, (C)ommand and Control, and (E)xfiltration" (Kirsch et al. 2014: slide 10). Other documents mentioning JTRIG illustrate the unit's capacity to decrypt and de-anonymize The Onion Router (TOR), essentially an anonymizing browser system.

The network state monitors and learns from hackers and in the process explores the edges of legality. To do this it needs to go undercover in IRC chat rooms and closely watch hacker blogs. For instance, the INTOLERANT program enables the NSA to collect the emails of targets already hacked by hackers (NSA 2010). The program LOVELY HORSE directs agents to follow Twitter, IRC chat rooms, and more in order to

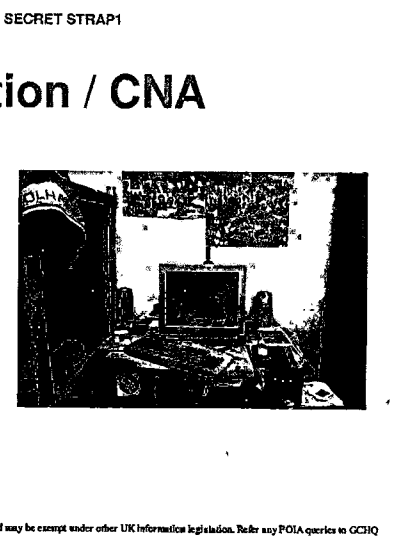

Figure 2.3 GCHQ's JTRIG computer network attacks (CNA)

monitor information activists and security researchers (LOVELY HORSE n.d.). Examples of Twitter accounts worthy of surveillance include several associated with Anonymous and WikiLeaks (Greenwald 2014). With these disruption and surveillance programs, the internet, far from being conducive for digital civil disobedience, is increasingly depoliticized in relation to social movements.

JTRIG is involved in secret online operations, including the infiltration and manipulation of targets' communications. The techniques include "false flag operations," fake victim blog posts, and the posting of negative information online with the goal being the use of social science and other methods to destroy the reputation of targets (JTRIG n.d.). These techniques are used "in lieu of 'traditional law enforcement' against people suspected (but not charged or convicted) of ordinary crimes, or more broadly still, 'hacktivism', meaning those who use online protest activity for political ends" (Greenwald 2014). The edginess of this work is not lost on the GCHQ, which titles a slide "Cyber Offsensive [*sic*] Session: Pushing the Boundaries and Action Against Hacktivism." Here JTRIG admits that it is on the *offensive* and *pushing* the *boundaries* by targeting people neither charged nor convicted and using techniques on the edge of legality.

WikiLeaks, the Pirate Bay, and Anonymous have all been targets of the NSA and GCHQ (Courage Foundation n.d.). For example, when a query was posed to a formerly classified NSA wiki, "Is it OK to target the foreign actors of a loosely coupled group of hackers...such as with Anonymous?", the response was: "As long as they are foreign citizens." This and other exchanges provide a detailed and compelling vantage point from which to see how the state works at the edges of technology and legality in an expanded pursuit of hacktivists. In these documents the NSA can be seen as a brazen – almost rogue – agency capable of writing its own rules as it explores the edges of legality and technicality (Greenwald & Gallagher 2014). In these programs, individuals associated with WikiLeaks, the Pirate Bay, and Anonymous who have not been formally charged with or convicted of anything are nonetheless targeted for surveillance, disruption, and prosecution.

In the above-mentioned ROLLING THUNDER program, GCHQ's JTRIG used a distributed denial of service attack (DDoS) – a way of coordinating multiple computers to flood

a site with requests and shut it down in the process – to close an Anonymous server hosting an IRC chat room (Hacktivism: Online Covert Action 2012; Schone, Esposito, Cole, & Greenwald 2014). An NSA slide titled "DDOS" is followed by a transcript from an IRC chat room, within which a user says, "We're being hit by a syn flood. I didn't know whether to quit last night, because of the DDOS." Such a DDoS likely compromised any other websites hosted on that server, silencing the freedom of speech of innocent users of the same server in the process. Scholars believe that hacktivists such as the PayPal 14, who were convicted of conducting a DDoS campaign in support of WikiLeaks, should be protected under the First Amendment of the US Constitution (Greenwald 2014; Leiderman 2013; Sauter 2014). According to this progressive interpretation, DDoS is a virtual sit-in and should be seen as an exercise in freedom of speech and freedom of assembly. However, when exercised by hacktivists, it is seen as an illegal affront to private property, although when used by the NSA, it is as something worth boasting about at a professional conference.

The appropriation of DDoS from its hacktivist roots thus represents a "(re)militarization of the internet" according to Molly Sauter (2014: 145). She writes, "[T]he use of these tactics in the name of law enforcement and national security is a deliberate move to extend the Hobbesian state monopoly on force to include code.... [E]xpansive definitions of what counts as 'weaponized code' or 'cyberweapons' could result in the widespread classification of civilians as 'cyberterrorists or enemy combatants" (Sauter 2014: 148).

The efforts by the cybersecurity divisions of the US and the UK reframe free speech, freedom of assembly, and civil disobedience as criminal activity, revealing how edgework and the judicial and policing systems shape assemblages that threaten the very basis of hacktivism.

Discussion

Versioning, selfie-incrimination, and edgework represent three important flashpoints in the ongoing battle over the form and meaning of the internet. They are critical points that shape and inform the assemblage that links the worlds of hacktivism and the state. They reveal how the internet fails to exist in a pristine vacuum but is instead interwoven within an assemblage of technical, legal, and policing practices and factors. The battle fought between hacktivists and state agents speaks to the historical amnesia each has, with their assumption that a decentralized networked architecture would enhance, respectively, either freedom, autonomy, and radical sovereignty or citizenship, legibility, and disciplining.

We spoke with former FBI agent Chris Tarbell, the man responsible for catching the hacker Sabu and turning him into an informant and also contributing to the arrest of Silk Road founder Ross Ulbricht. He described the near impossibility of avoiding self-incrimination.

> Perfect anonymity is kind of like perfect communism. It sounds ideal but it's really tough. You'd have to have a computer that you never touch any of your social media, any of your bank accounts, you'd have to pay for it through an anonymous payment system like bitcoins or something like that. You know when you get going, let's say I've observed people hacking into things, once they get going they kind of forget some of the stuff, they get excited about what they have broken into. They make that one mistake. Like a robber taking a glove off in the house to pick up the jewels he accidentally touches the door and there's his fingerprint. You know...one simple mistake.

According to Tarbell, to evade selfie-incrimination, hacktivists would need to engage with a deeply fragmented internet, one in which the computers themselves are not networked. Encryption in itself is not enough, nor is versioning. We must thus ask whether any assemblage involving the internet could ever aid the cause of hacktivism, and if so what that might look like. Are we truly in a post-privacy world? And if so, what types of public activity are safe?

What is needed from the perspective of the hacktivists is the reassembly of an internet around principles and practices of encryption, mesh networks, and other technical and legal factors and practices. For them, the internet needs to be demilitarized and extracted from the discourse of securitization, which positions the communication system as a subject of the

networked security state rather than as a space that is more radically democratic. Perhaps such an outcome will be facilitated if hacktivists themselves shift their use of rhetoric and symbolism, stepping away from the increasingly ominous and threatening "macrosecuritizing" discourse – which situates their work in the language of global war (Fish 2017a). What we do know is that the future of the internet will be shaped through antagonistic relationships and assemblages between hacktivists and states.

3

Media Activism: Shaping Online and Offline Networks

From the introduction onward, this book has discussed the power of myths in relation to the internet. As "the creative and symbolic dimension of the social world... through which human beings create their ways of living together and their ways of representing their collective life" (Adelman 1989: 83), myths have fueled the mistaken treatment of the internet as static, singular, immersive, and transcendent. When we subscribe to such myths, we may in turn lose our ability to see the internet as an assemblage, inseparable from peoples, places, laws, and environments. The two previous chapters have been devoted to revealing the assemblages within which internet technology is interwoven, from our discussion of the belief systems and environments of indigenous and cross-cultural communities to the legal systems and policing practices that afflict hacktivists.

This chapter takes aim at the internet and its relationship to political activism and revolutions. It considers fieldwork conducted in Egypt and the Occupy movement, as well as the important protests of the Indignados of Spain and the Chilean student movement. Its primary focus on the Arab Spring is all the more important given how the Middle East continues to be a region of great concern and misunderstanding. By showing how the internet's networks are refracted alongside activist assemblages of offline tools and environments, this chapter argues that we must do away with a narrative where