## Chapter 2

## A Taxonomy of Hacktivism

### Introduction

The "type" of hacktivism categorizes people: political crackers, performative hackers, and political coders. The "form" of hacktivism categorizes actions: site redirects, defacements, virtual sit-ins, etc.

This chapter provides a broad map of the hacktivist universe, of its participants and their activities. My purpose is to introduce the key lines of variation that define distinct types of hacktivism, and to provide a clear introduction to each of these types. To this end I describe three distinct types of hacktivism: political cracking, performative hacking, and political coding.

The distinctions among these three types are based on two dimensions of variation: origins and orientation. The first part of this chapter discusses each of these lines of variation. It begins by looking at *origins*: the political culture from which each type of hacktivism emerged. Hacker-programmer culture gave rise to political coding and political cracking; postmodern left culture gave rise to performative hacktivism.

**Table 5. Types of hacktivism by hacktivist origins and orientation**

**Hacktivist Origins**

| **Hacktivist Orientations** | Hacker-programmer world | Postmodern left (artist-activist) |
|---|---|---|
| Transgressive | **Political coding** | **Performative hacktivism** |
| Outlaw | **Political cracking** | *About this space*[5] |

[5] While it might seem theoretically possible for artist-activists to engage in outlaw forms of hacktivism, it is easy to see why such hacktivism has yet to emerge. The outlaw orientation of political crackers, which includes the assumption of greater legal risk and the not-unrelated effort at avoiding accountability, along with a propensity for transnational conflict and an avoidance of large-scale collective action, all run counter to some pretty central principles of postmodern left activism. Artist-activists tend to value mass, accountable action as more democratically legitimate, and eschew transnational conflict due to a more pacifist orientation.

Once I have reviewed the two worlds from which hacktivists originate, I move onto the notion of *orientation*: the playbook that defines different types of hacktivism, and that separates political coders from political crackers (even though both emerge from the same hacker-programmer culture). The transgressive[6] orientation of both political coders and performative hacktivists challenges the legal and political order, but still exists in relation to it and even shares some norms of the liberal democratic order, such as notions of legitimacy and accountability. Political crackers, in contrast, have an outlaw orientation that completely rejects the legal and political order, and seem to exist entirely outside of liberal democratic norms (though perhaps within the norms of some local or radical subcultures). In concrete terms, these differences translate into very different practices around legal risk, accountability, group size, and international cooperation, as seen below.

**Table 6. Characteristics of hacktivist orientations (transgressive vs. outlaw)**

| | | **Orientation** | |
|---|---|---|---|
| | | Transgressive | Outlaw |
| **Characteristics** | Legal risk | Legally ambiguous | Illegal |
| | Accountability[7] (naming practices) | Real names, traceable pseudonyms | Untraceable pseudonyms, anonymity |
| | Group size | Medium-size groups, dependence on mass participation | Solo, small groups |
| | Transnational cooperation | Multinational (working with hacktivists from multiple nations) | National (vs. own country)<br>Multinational (cooperating across boundaries)<br>International (mirroring international conflicts) |

[6] The distinction between the transgressive and outlaw orientations is a distinction of degree, more than of kind – I could describe these orientations as "transgressive" and "even more transgressive.". But to describe them as "conventional" versus "transgressive" would be to radically underestimate the degree of transgression involved in political coding and performative hacktivism.

[7] Variation in naming practices as a type of accountability claim is addressed in Chapter 5.

Once I have provided a brief overview of each of the characteristics that define different hacktivist orientations, I move quickly into describing each of the three types of hacktivism. Political cracking is the most legally risky, and probably the least effective, form of hacktivism: after a brief overview I provide a more in-depth description of one group of political crackers, the World's Fantabulous Defacers. Performative hacktivism looks a bit more like progressive street activism, but with a decidedly postmodern twist: here I provide a case study of the Electronic Disturbance Theater, one of the best-known groups of performative hacktivists. Finally, I introduce political coding, which focuses on political software development: the case study here looks at Hacktivismo, the leading group of political software developers.

These three types of hacktivism are not just useful intellectual constructs. They represent meaningful differences in the origins and orientations of different hacktivists, and translate into fierce internal debates. The later chapters on identity, policy circumvention, and online deliberation will all rely heavily on the differentiation among hacktivist types in order to address key questions in political participation.

And it is in the context of describing each type of hacktivism that we can best see how the difference between a transgressive and an outlaw orientation separates hacker-programmer-coders from hacker-programmer-crackers. The chapter concludes by underlining the commonalities in the shared transgressive orientation of political coders and performative hacktivists, while noting a couple of further distinctions that still separate them.

## Hacktivist origins

Hacktivists come from two distinct political cultures. One is the hacker-programmer culture, itself embedded in the broader social and political culture of the Internet. Another stream of hacktivists comes from the world of post-modern left, and its community of progressive artist-activists. These two backgrounds translate into very different identities – and very different kinds of hacktivist practice. As we will see in later chapters, there is some animosity between the two camps; hacker-programmers often see artist-activists as ignorant and careless about the infrastructure of the Internet, and as technically incompetent. Artist-activists often describe hackers as caring more about computers than people, and as technological elitists.

### *The world of hacker-programmers: a very brief history of hacking*

The world of hacker-programmers is a tightly networked community, although the explosive growth of the Internet has expanded that community to the point where ties have necessarily loosened. Its denizens are bound together by their immersion in the culture of the Internet, which generates its own behavioral norms, its own political worldview, and its own political agenda.[8]

---

[8] All of these aspects of hacker history and culture are well-documented online. Indeed, Internet culture sets a new standard for sociological documentation, since the culture has continually articulated, documented and discussed the evolution of its language, technologies and norms. The results of each development – and many of the discussions that drove the evolutionary process – have been preserved in media such as Usenet "Netiquette" guidelines (summarizing online behavioral norms), the Jargon file (tracking online terms and language use), and the Wikipedia (a communal project that documents everything from the overall history of the Internet to individual technical standards – and includes many offline cultural references, too).

The Internet culture in which hackers exist itself emerged out of hacker culture. Before the Internet, hacker culture existing as multiple cultures("Hacker culture") of computer scientists, research assistants, and hobbyists, clustered around whatever mainframes they could get access to. [9] The idea of linking these mainframes together initially arose in a RAND report to the U.S. Air Force, suggesting how communications could be constructed to survive a nuclear attack:

> The report proposed a communications system where there would be no obvious central command and control point, but all surviving points would be able to reestablish contact in the event of an attack on any one point. Thus damage to a part would not destroy the whole and its effect on the whole would be minimized.(Hauben)

In 1969, this abstract idea was given life as the ARPANET, and the disparate communities of hacker-dom were suddenly connected in what was for many years a very small network of users. But where the Advanced Research Projects Agency (ARPA) had envisaged its ARPANET as a means of pooling computing power, the law of unintended consequences took hold.

> By the second year of operation, however, an odd fact became clear. ARPANET's users had warped the computer-sharing network into a dedicated, high-speed, federally subsidized electronic post- office. The main traffic on ARPANET was not long-distance computing. Instead, it was news and personal messages. Researchers were using ARPANET to collaborate on projects, to trade notes on work, and eventually, to downright gossip and schmooze. People had their own personal user accounts on the ARPANET computers, and their own personal addresses for electronic mail. Not only were they using ARPANET for person-to-person communication, but they were very enthusiastic about this particular service -- far more enthusiastic than they were about long-distance computation. It wasn't long before the invention of the mailing-list, an ARPANET broadcasting technique in which an identical message could be sent automatically to large numbers of network subscribers. Interestingly, one of the first really big mailing-lists was "SF- LOVERS," for science fiction fans. Discussing science fiction on the network was not work-related and was frowned upon by many ARPANET computer administrators, but this didn't stop it from happening.(Sterling 1993)

---

[9] These early days are well chronicled; see (Levy 1984; Raymond 2000).

As much as the ARPANET – and later, the Internet[10] – reflected the interests and values of computer scientists, hobbyists and hackers, its characteristics also shaped them. Networks enabled instant, world-wide, synchronous or asynchronous communication – and for many years, that communication was necessarily in plain text form. Network communication demanded a common language, and English emerged as the dominant one. Networks were blind to characteristics like gender, race, age, and accent. Networks depended on common standards, so that different parts of the network could communicate. And networks thrived on access: access to computers (a rare and valuable commodity in the early days of the Internet), access to networks (in order to gather and share information), and above all, access to information itself: information on how to use the emergent tools of network computing.

From this drive for access emerged the "hacker ethic", whose core tenets were articulated by Steven Levy as:

> - All information should be free.
> - Mistrust authority - promote decentralization.
> - Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
> - You can create art and beauty on a computer.
> - Computers can change your life for the better.(Levy 1984, Chapter 2, "The Hacker Ethic")

These tenets constituted a worldview that has been described as inherently political, for,

> although hacking is often perceived as apolitical, hacking always tends to evoke political elements due to the nature of knowledge in our society. The quest for knowledge, which is an unmistakable core component of hacking, is a politics of transgression because the 'knowledge' that is sought is often inaccessible (or potentially so) at either a technological or legal level.(Coleman 2003)

---

[10] The transition from ARPANET to Internet took place in the 1980s with the development and proliferation of the TCP/IP networking protocol, until the ARPANET was finally decommissioned in 1990. (Leiner et al. 2003)

In concrete terms, the hacker "quest for knowledge" translated into a particular politics, which has to some degree become identified as the politics of the Internet more broadly. The motherhood issues for hackers – and the Internet community more generally – are:

- *freedom of speech*, and in particular the fight against online censorship, reflecting hackers' view that "information wants to be free";
- *privacy rights,* especially online, reflecting hackers' mistrust of authority;
- *intellectual property freedoms,* like the ability to share traditionally copyrighted text, music or video files online, again reflecting the view that "information wants to be free";
- *open standards,* which ensure interoperability of the Internet, as opposed to the private standards promulgated by Microsoft and others through the creation of for-profit networks and tools; and
- *free or open source software,* which permit various kinds of modification and distribution, reflecting hackers' quest to use technology for continuous improvement, and to continuously improve technology.

This political agenda manifested itself in a number of illegal hacking ("cracking") campaigns, long before the phenomenon of "hacktivism" is usually said to have emerged. When Kevin Mitnick was arrested and prosecuted for his hacking, thousands of hackers mobilized to support him – in many cases by defacing sites to add "Free Kevin" messages. Was this hacktivism, or plain old hacking? According to the hacker ethic, it is

a false distinction – because hacking is an inherently political act: the liberation of information.

In recent years, however, political cracking has shifted away from the hacker agenda, and political coding has emerged to champion Internet issues. This explains the focus of projects like Hacktivismo (which tackles Internet censorship) and DeCSS (which tackles the narrow construction of intellectual property rights). But the fact that political coders focus on Internet issues should not be taken as a lack of interest in "real world" politics. Over time it has become clear that hackers' online political agenda extends to a distinct perspective on offline issues, too:

> located somewhere between the secular or progressive pole on moral values and the laissez-faire pole on economic values, favoring freedom on both dimensions. Internet enthusiasts favor the private sector more than government intervention to produce economic equality, but they are also strong supporters of the alternative social movements that arose in the counterculture 1960s, such as those seeking to promote gay rights, pro-choice, civil rights, feminism, and environmentalism. (Norris 2001)

If it is hard to know where hacker politics ends and the broader politics of the Internet begins, that is because the hacker-programmer culture has a continually evolving relationship with the larger Internet. In the early years, hacker-programmers constituted the entire Internet community, so hacker politics *were* Internet politics. In the late 1980s and early 1990s, more Internet users came online, but these still tended to be people with a great deal of interest, skills, or enthusiasm for computing; they absorbed many of the norms and values of the hacker world, even if they did not engage in the same level of assisistance or tinkering with the Internet's software and hardware infrastructure. This Internet community has over time been enveloped by a much larger perimeter of Internet users, mostly coming online in the late 1990s or after, who see the instrumental value of the Internet. These users may contribute content or participate in online communities, but

their contributions and participation are defined by offline identities and interests (such as ethnicity, sexual orientation, or political affiliation) rather than by the culture and values of the Internet itself. Throughout each wave of growth, "white hat" hackers have seen it as their particular duty to protect the Internet from private sector encroachment, "newbie" carelessness, and destructive "black hat" hackers who fail to respect the hacker ethic.

People who live in this world might or might not call themselves hackers – many do not, citing media misrepresentation of what hacking actually means. Some call themselves programmers, coders, geeks, or nerds – and some do not use a label at all. But *all* of them identify very strongly with the "true" community of the Internet, as we can see from this programmer's reaction to the Internet's gradual dilution:

> When the Internet first formed, it centered on technical experimentation by academics, scientists, and students. The original connections were almost all free of charge; people recognized that connecting and communicating were really cool, and we helped each other in a general spirit of cooperation. We promoted free speech and grassroots access, because we recognized those things as valuable. Alleged Internet problems, such as child pornography, "bomb making instructions", hate literature, etc., were simply not issues. We could set up real-time chat connections across the continent or the world and get instant response. All the important networking software was freeware, distributed under a public license system where everyone was allowed to use, copy, and modify it at no charge.
>
> How different the situation now that internetworking is considered a hot global trend. More people want connections than there are connections available, so everyone has to pay….[Your organization] appears to be concerned about commercial exploitation of our natural environment, and about appropriate respect for our indigenous cultures. What about the endangered network environment? What about the first nations of the Net?… I'd urge you, since you no doubt feel you *must* discuss the Internet as a medium for activism, to also discuss responsible use and respect for the Internet's unique culture…. If not, then get off our land, get out of our culture, and go crawl back under a rock, because the last thing the Internet needs is more colonization. (Skala 1996)

*The world of artist-activists: an introduction to the postmodern left*

The postmodern left is a very loosely bound community that is defined by a combination of political beliefs, theoretical worldviews, and tactical innovations. I use

the term “postmodern” to distinguish this world from the broader progressive scene; this particular segment of the left is more creative in the forms of its activism, and more sophisticated in its understanding and use of communications. While some members identify primarily as artists, and others as activists, these particular artists blur the lines between performance and politics, while these particular activists do their politics in ways that are strongly shaped by a media-savvy artistic aesthetic.

I am not the first to apply the term “postmodern” to this slice of the progressive movement. Best and Kellner describe postmodern politics as

> a politicization of all spheres of social and personal existence. Postmodern models of politics are trying to redefine the "political" based on changes in society, technology, economics, and everyday life. (Best and Kellner)

In her critique of what she also terms the “postmodern left”, Wood describes its themes as:

> a focus on language, culture, and "discourse"…; a rejection of "totalizing" knowledge and of "universalistic" values…in favor of an emphasis on "difference," on varied particular identities such as gender, race, ethnicity, sexuality, on various particular and separate oppressions and struggles; an insistence on the fluid and fragmented nature of the human self…;and a repudiation of "grand narratives"…[I ]t should be obvious that the main thread running through all these postmodern principles is an emphasis on the fragmented nature of the world and of human knowledge, and the impossibility of any emancipatory politics based on some kind of "totalizing" vision. (Wood 1995)

Seippel usefully contrasts this postmodern politics with the postmaterialist orientation described by Inglehart:

> While the postmaterialist has a teleological and future-oriented belief in progress, the postmodernist is ultimately keen to cultivate the present, the fragment, the immediate; while the postmaterialist searches out the natural, true and authentic, the postmodernist explores the seductive surface; the postmaterialist is a stable, steady being, whereas the postmodernist is constantly changing, and finally, while the postmaterialist is out to realize himself, the postmodernist is merely out to express himself.

In practice, however, the political agenda espoused by this community is not unlike the agenda of the post-materialist left. The issues of greatest interest are

globalization, corporate power, human rights, civil rights, and the environment. As I will show below, this agenda is reflected in the targets selected by performative hacktivists: targets like Nike, the WTO, and the Mexican government (over the issue of the Zapatistas). Where the postmodern left differs from the broader progressive scene is thus not in its agenda, but in the theoretical lens through which it views that agenda, and thus, the tactics it adopts in that pursuit.

The worldview of these artists and activists is self-consciously shaped by the theoretical works of postmodern and critical theorists such as Baudrillard, Virilio, Foucault and Guattari. Best and Kellner, describing the world of what they call "postmodern politics," note that this world includes "the anti-politics of Baudrillard and his followers, who exhibit a cynical, despairing rejection of the belief in emancipatory social transformation, as well as a variety of efforts to create a new or reconstructed politics."(Best and Kellner) From Virilio, it takes its analysis of globalization as a temporal rather than spatial phenomenon:

> Virilio predicts that the globe will no longer primarily be divided spatially into North and South, but temporally into two forms of speed, absolute and relative. The 'haves' and 'have-nots' are then sorted out between those who live in the hyperreal shrunken world of instant communication, cyberdynamics, and electronic money transactions—and those, more disadvantaged than ever, who live in the real space of local villages, cut off from the temporal forces that drive politics and economics. (Bleiker 2002)

From Foucault it takes the notion of "revolution as spectacle."(Hanninen 2003) And from Guattari, it takes the notion of the body as the site of maximal social regulation, and posits the Internet's capacity for liberating actors from that regulation.(Ensemble. 2000) A final theoretical influence comes from the world of political theater; August Boal, in particular, is cited for his idea of theater as a way "to reinvent the past and to

invent the future." (Boal 1999)

This theoretical lens translates into specific kinds of political strategies and tactics that are much less tedious than the theoretical works that inspire them. The artist-activists of the postmodern left are more likely to bridge art and politics, turning politics into performance and performance into politics. For example, one ascendant tactic is "culture jamming, the practice of parodying advertisements and hijacking billboards in order to drastically alter their messages." (Klein 2000, p. 282.) Culture jamming is "itself a cutting and pasting of graffiti, modern art, do-it-yourself punk philosophy and age-old pranksterism."(Klein 2000, p. 282.) Another characteristic tactic of "carnivalesque resistance" are street protests "that rebelliously reinterpret the experience of consumers putting on garments in acts scripted to raise consciousness." (Boje 2001) A third innovation has been the creation of independent media centers (IndyMedia), whose mission "includes reporting on a wide variety of social injustices, covering social movement mobilizations, engaging in media activism, and embodying participatory democracy in its actions and media policies."(Morris 2002) While participants often describe these tactics with reference to postmodern theory, the practical significance of their innovative activism is that it attracts both more participation and more media attention by making politics look more like play.

While the artist-activist influence on hacktivism is most visible in the explict theorizing of those who come from an art or theater background, there is a growing number of hacktivists whose background has more in common with non-performative progressive activists. In June 2002, the Ruckus Society, which provides training in

disruptive protest techniques, held its first hacktivism training camp; this may well engender more hacktivism from traditional activist groups.

Even though the artist-activist world is truly a postmodern fusion of political art and political activism, people in this world tend to identify themselves as either artists or activists. But whichever label they use – or even if they eschew labels altogether, a not-uncommon postmodern position – they locate themselves within the broader "us" of creative progressives working for social change.

**Hacktivist orientations and types of hacktivism**

As presented at the beginning of this chapter, the two lines of variation among hacktivists (hacker-programmer vs. artist-activist origins, and transgressive vs. outlaw orientation) divide the world of hacktivism into three distinct types: political cracking, performative hacktivism, and political coding. *Political cracking* is undertaken by hacktivists from hacker-programmer origins, who have an outlaw orientation. *Performative hacktivism* is conducted by hacktivists from artist-activist backgrounds, who have a transgressive orientation. And *political coding* is undertaken by hacktivists with hacker backgrounds, who have the same transgressive orientation as performative hacktivists.

Four interconnected characteristics define the difference between the transgressive orientation of political coders and performative hacktivists and the outlaw orientation of political coders: tolerance for legal risk, naming practices, scale of collective action and propensity for multinational cooperation.

Hacktivists vary significantly in their willingness to engage in illegal or legally ambiguous activities. The outlaw orientation embraces forms of hacktivism that are clearly illegal, like site defacements, redirects, DoS attacks, and sabotage. The transgressive orientation challenges the law, but does not push that challenge to the point of immediate legal jeopardy.

In a related move, the transgressive orientation embraces accountability, while the outlaw orientation avoids it. In practice this means that while some hacktivists conduct their activities under their own names, while others hack anonymously, or using pseudonyms.[11] One hacker convention that has traveled into the hacktivist realm is the use of pseudonyms, or handles, in the execution of hacktions. Hacktivists frequently use handles like mor0n, metac0m, or nathan hactivist. (The use of numerals in place of letters is another hacker convention, dating back to the days when all Internet communication took place in ASCII, a standard set of alphanumeric characters.) Handles are a way for hackers or hacktivists to take credit for an online act, without necessarily being accountable for that act in an offline context. Note that the use of handles does not necessarily prevent the hacktivist from being identified by law enforcement authorities; while some hacktivists take care to keep their real identities secret, others are relatively open about both their handles and their real names.

Another variation is in the presence, absence, or scale of collective action. Individual hacktions may be undertaken by a lone hacktivist, a small group of hacktivists,

---

[11] The significance of anonymous and pseudonymous hacking is discussed in greater detail in Chapter 5.

or a very large number of participants who leverage the work of a smaller core group. The possibility of solo action seems to be one of the attractions of hacking in general, and hacktivism in particular.

The final characteristic that differentiates the transgressive and outlaw orientations is in the propensity for hacktivism across borders. While transnational activism has received some attention in recent years, it is still the exception rather than the rule in political participation. In the case of hacktivism, the reverse is true: hacktivism across borders is at least as common as hacktivism within borders, and it is often difficult to distinguish between the two.

I have found it useful to distinguish between national, multinational, and international hacktivism. National hacktivism occurs when a hacktivist targets a government, business or organization within his or her own country. Multinational hacktivism occurs when hacktivists band together across borders to attack a common target at the subnational, national, or multinational level. And international hacktivism consists of hacktivists in one country targeting a government, business, organization in another country, most often as part of a reciprocal "cyberwar" that parallels an offline international conflict.

We can best understand how these orientations translate into specific practices by looking at each type of hacktivism in greater detail. I begin with an account of political cracking (which comes from an outlaw orientation) before proceeding to performative hacktivism and political coding (which share a transgressive orientation).

*Political cracking: an introduction*

Political cracking consists of hacktions that are clearly illegal, undertaken by hacker-programmers. This encompasses the largest number of hacktivist incidents to date (though probably not the largest number of participants), and spans a wide range of issues and nations. It also encompasses a wide range of tactics, including site defacements, redirects, denial of service attacks, information theft, and sabotage.

Calling these activities "political cracking" draws on a distinction that is maintained by many members of the hacker community. Among early computer enthusiasts, a "hack" was a technical "feat…imbued with innovation, style, and technical virtuosity" and people "called themselves 'hackers' with great pride."(Levy 1984) Hackers from that generation "prefer to call their progeny 'crackers' in order to differentiate themselves from what they perceive as their younger criminal counterparts."(Thomas 2002). Within the hacker community, hackers who engage in clearly illegal and destructive activity – like web site defacements or information theft – are thus often referred to as "crackers," in order to differentiate this activity from the "leave no footprints" hacking condoned by the hacker ethic. It is in this tradition that I use the term "political cracking" to refer the type of hacktivism that encompasses illegal activities – such as site defacements, redirects, DoS attacks and sabotage – harnessed to political ends.

It should not be surprising that political crackers therefore remain anonymous. The 1996 defacement of the U.S. Department of Justice, for example, left no explicit clue

as to the cracker's identity; the person or people behind the 2000 Nike site redirect likewise remained anonymous.

Political crackers tend to work alone, or in very small groups. A single cracker can experience a high degree of political efficacy by defacing or redirecting a web site, potentially attracting a great deal of media attention. There are none of the coordination or free rider problems of collective action, but the actor is nonetheless able to achieve much of the public recognition that adheres to collective political action.

Small group action is also common. Many political crackers apparently belong to groups that include anywhere from two to perhaps a dozen members; hacktions may be executed by a lone hacker, a couple of hackers, or a larger number of group members. It can be difficult to distinguish solo from small group hacks, since hacktions are so often anonymous or pseudonymous. Where a hack is credited to a specific group, such as the World's Fantabulous Defacers, it may not be clear whether it was executed by one group member or by several hackers working together.

Some ongoing defacement campaigns, like those seen in the transnational conflicts between Israel and Palestine, or India and Pakistan, might also be considered collective action; but in these instances the individual hacks are still conducted by solo or small-group hackers, with little or no apparent coordination of the overall campaign.

Political cracking encompasses national, multinational and international hacktivism, but it is most common in international form. International hacktivism, sometimes called "infowar" or "cyberwar", refers to instances where citizens of one country hack targets in another, usually in a reciprocal conflict between two countries. Examples include the long-running battles between Palestinian and Israeli crackers,

between Chinese and American crackers, and between Pakistani and Indian crackers. We do see some instances of multinational cracking, however, as when milw0rm, a multinational group of hackers, targeted the Indian government to protest its nuclear tests. And particularly in the early days of political cracking, when hacking was just shading into hacktivism, national hacktivism was quite common: the cracker campaigns on behalf of Kevin Mitnick, or against the US Communications Decency Act, both consisted primarily of national cracking.

While the distinction between these three types of hacktivism is theoretically significant, in practice it is often hard to recognize. Because so many hacktivists work anonymously or pseudonymously, their national origin may be impossible to ascertain. Nonetheless there are many instances in which we can distinguish national, transnational and international hacktivism, and in which the distinction usefully informs our understanding of the hacktivists and their actions.

The first quasi-political cracking was focused on hacker-specific issues like the regulation of the Internet or the prosecution of individual crackers. But cracking has since broadened to encompass a much broader range of causes, from gun control (pro and con) to globalization and corporate power. Today the greatest concentration of political cracking incidents occurs in the context of international cyberwars: between Israelis and Palestinians, Indians and Pakistanis, Chinese and Americans. Each of these cyberwars has seen hundreds or even thousands of web sites defaced in a campaign that pits political cracker against political cracker.

While it has been credibly argued that governments have sponsored some of this cyberwar cracking (Borger 1999; Kalathil and Boas 2003; La Canna 2001), the majority

of political cracking activities are illegal in the jurisdiction of the target, the cracker, or both. As a result, political cracking is almost always anonymous, or more often, pseudonymous. Precisely because hacker culture puts so much value on technical prowess, crackers like to build their reputations by taking credit for their hacktions under handles.

The fact that the activities of political crackers are generally illegal does not mean they are necessarily destructive. Indeed, the "hacker ethic" is widely seen as precluding destructive activity:

> It is against hacker ethics to alter any data aside from the logs that are needed to clean their tracks. They have no need or desire to destroy data as the malicious crackers. They are there to explore the system and learn more. The hacker has a constant yearning and thirst for knowledge that increases in intensity as their journey progresses.(Mizrach)

Web site defacements, DoS attacks, and information thefts can adhere to this standard by leaving the sites they deface fundamentally intact.

Unlike other forms of hacktivism, engaging in any form of political cracking requires at least a minimal knowledge of code and/or hacking techniques, which is still almost unheard of outside the hacker community. Political cracking is thus almost entirely confined to hacktivists who come from hacker backgrounds, or who have spent enough time on hacker sites to acquire the necessary skills. These crackers can work alone or in small groups (sometimes called hacker gangs or crews) in undertaking their various hacktions.

Like their non-political counterparts, most political crackers seem to be quite young – if not teenagers, then not far into their twenties. While there are some women involved in political cracking, most of these teenagers are boys. As Douglas Thomas points out, hacking is very much a "boy culture" in its emphasis on notions of mastery,

competition, and subordination. (Thomas 2002) That carries over to the world of political cracking, in which political site defacements will bear comments like "all those wannabe unicode kiddies who are defacing thinking they have joined us can DREAM ON cuz all they are doing is making themselves more GAY"("http://listserv.gao.gov COMPROMISED" 2001).

Comments like this reflect more than adolescent narcissism. The stunt mentality that pervades cracker culture, whereby site defacements and redirects are a way of demonstrating technical prowess and establishing a reputation as a hacker[12], takes on a somewhat different meaning in the hacktivist context. When cracking is politicized, the attention-seeking character of site defacements, etc. is reframed (at least nominally) as the pursuit of attention for worthy and perhaps neglected issues. The implicit logic is that by drawing attention to these issues, political crackers can affect public opinion, and perhaps even public policy.

That logic is the logic of policy change, not policy circumvention. For all that political cracking uses the language of lawlessness, its impact ultimately depends on the rule of law – or at least on some kind of relationship between public opinion and public policy. Political crackers are, in their own way, conscious of maintaining this distinction between rhetoric and direct action; in the words of one cracker group, "[i]t's just a machine we use to do what we do, not a gun or missile or something"("AIC (Anti India Crew) interview").

---

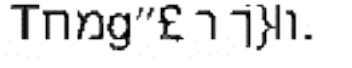
[12] Of course, site defacements, redirects and other forms of cracking only build reputation in the (generally young) segment of the hacker scene that regards cracking as a legitimate or admirable form of hacking. The hacker-programmer "establishment" is not impressed by these kinds of activities – on the contrary, a reputation as a cracker can preclude acceptance into the established hacker-programmer community.

*Political cracking: the case of the WFD*

The WFD – also known as the World's Fantabulous Defacers – emerged in November 2000, and racked up an extraordinary series of anti-Indian and anti-Israeli defacements over the next two years. The group numbered about a dozen members from five countries ("Interview with World's Fantabulous Defacers"), though reportedly most were from Pakistan (Khan 2001). One defacement lists these members as Nightman, M0r0n, sub-0, Noogie, module, ApocalypseDow and B_Real (B_Real 2001); another lists m0r0n, nightman, Sub-0, Cyberpunk, B_real, laughing3y3s, Sofh, h3ll rais3r, Brake^Off, hid03ous, B1n4ry C0d3 and one additional member whose handle can not be typographically rendered (m0r0n and nightman 2000b)[13].

Estimates of the WFD's total number of attacks vary significantly. The Zone-H defacement mirror lists only 349 defacements (including 26 mass defacements of multiple sites) from November 20 2000 to November 21 2002.("Digital Attacks Archive for WFD" 2004) But Internet security experts mi2g estimated in September 2002 that the WFD had conducted over 400 attacks just in the November 2001-September 2002 period. Since not all WFD attacks are necessarily represented in the Zone-H mirror, this higher estimate is easy to believe. Indeed, the WFD itself claimed that only about 20% of their attacks have been mirrored, since the mirrors are too slow in capturing reported defacements("Interview with World's Fantabulous Defacers").

---

[13] This member's name appears as  .

The majority of these hacks were used to promote "global awareness" (to use the WFD's favorite term) of human rights abuses of Muslim populations in either Palestine or Kashmir, with occasional defacements on other human rights issues affecting Muslims (such as the situations in Chechnya and the former Yugoslavia). WFD members m0r0n and nightman pointed out that the group has a broader agenda:

> We have defaced FOR many issues, if you look at our defacements it says "FREE KASHMIR, PALESTINE, LIFT THE SANCTIONS ON IRAQ, FREE CHECHNIA." So you see we are FOR all those people suffering in the world against atrocities! (m0r0n and nightman 2002)

By the group's own assessment ("Interview with World's Fantabulous Defacers"), its most important hacks have been those against the Bollywood Stock Exchange and Cricketbulls.com, "a site which trades imaginary shares on the popularity of leading Indian players" ("Hackers stump site" 2001). One of the elements that came to distinguish the WFD's defacements was the placement of Flash (Internet-viewable) movies on its web sites. These Flash movies used a sophisticated combination of text, image and sound to create effective messages about human rights issues.

A very typical WFD defacement is the group's February 2001 defacement of an inter-university library network in India, which featured a Flash movie embedded in a very long page of text and images. To illustrate the group's style I am reproducing a series of screen captures from the Flash movie, and a set of screen captures that encompass the complete web page[14] in which it was embedded (see next three pages).

As a group of political crackers, the WFD is both the most transparent and the most opaque of my case studies. On the one hand, everything they have done is online

---

[14] The defacement is archived at http://www.attrition.org/mirror/attrition/2001/02/24/www.inflibnet.ac.in/

and visible: their defacements are archived in the Zone-H and Attrition mirrors, and there is no other WFD activity to be accounted for. On the other hand, because its activities are illegal, the WFD is more elusive than my other subjects. The only source of information about the WFD is the WFD itself. Its web site defacements and online interviews are the ultimate sources of everything that has been written about the group. But m0r0n and nightman's consistent e-mail addresses[15] and ready availability for e-mail interviews makes them one of the few defacement crews for which some (admittedly unverified) biographical details are available. While other WFD members have also conducted interviews, m0r0n and nightman are by far the most frequent and visible interview subjects.

My own e-mail interview with the WFD's m0r0n and nightman has significant overlap with other published e-mail interviews the pair have conducted, since they tend to recycle their answers from one interview to the next. They insisted on being interviewed together, claiming that "[w]e cannot give separate interviews because we don't consider ourselves separate, a team is a team." While that is certainly one credible explanation for their decision to answer collectively, I cannot discount the possibility that this "pair" are actually one person, since I could only find two web pages on which the name of one appears without the name of the other.

Because all information about the WFD flows from the WFD, specifics about the group and its members are very limited – and limited to the areas that group members believe are relevant or desirable to make public. In their e-mailed response to my

[15] When I tried to contact other defacers who had (somewhat unusually) included their e-mail addresses in their defacements, the e-mails bounced, suggesting the accounts had been closed.

questions, m0r0n and nightman declined to share their day-to-day work ("We're all studying. The level does not matter!"); their country of residence[16] ("Dividing people according to country is not our style, as mentioned earlier ``DIVISION`` is not a word in

[16] I later discovered that the pair had identified themselves as Pakistani in some of their pre-WFD hacks.


**Figure 2. Stills from WFD Flash Movie "truth9.swf", as seen in a February 2001 defacement**

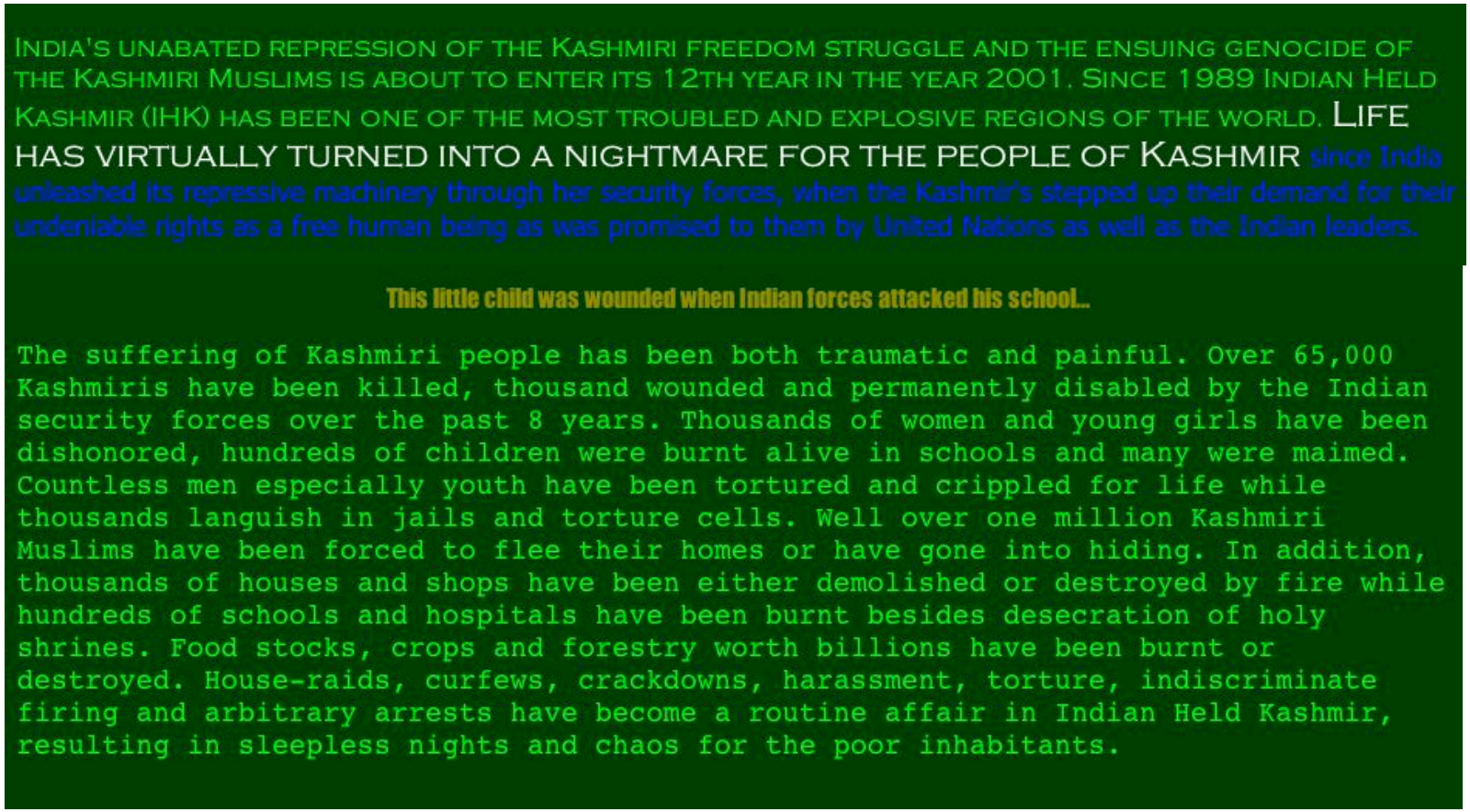



**Figure 3. Screen capture of February 2001 web site defacement by WFD (part 1)**

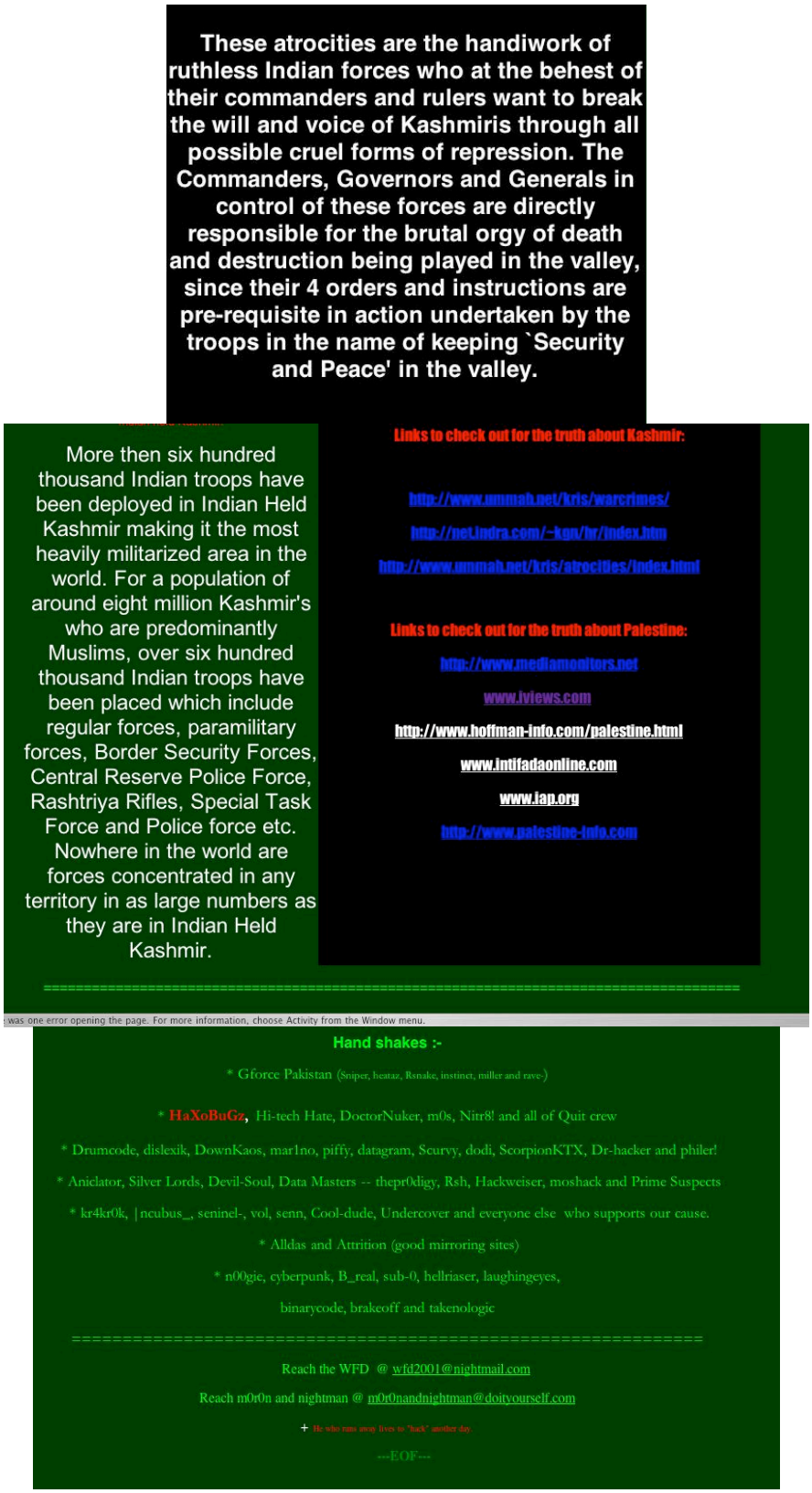



**Figure 4. Screen capture of February 2001 web site defacement by WFD (part 2)**

our lexicon") and their age ("Old enough to know about the issue we're dealing with inside out.") – although they did state that "We're not old enough to vote yet". And the tone of their answers was further suggestion that they were still teenagers, such as their response to my question, "What hacks do you wish you'd done yourself?": "We'd leave OTHERS to wish they had done what we had done. We do what we wish for!"

Working within these limitations, it is nonetheless possible to construct a basic outline of the WFD's genesis and activities. "We used to hack into systems but for the matter of proving ourselves that we could," m0r0n wrote. "Then one day Nightman & I decided we should do it for a reason!"(m0r0n and nightman 2002)

The pair's initial hacks defaced web sites that seem to have been randomly targeted:

> You are owned by nightman and m0r0n (Pakistan!) We just want to create global awareness so that people might now what Indians are doing to Kashmiris. The members;): m0r0n, NightMan, ftp, code0, laughingeyes, iniquity! (my pal hehe ;), cooldude, pollution, iNfra and Undercover and oh my Computer to ;) Greets: tushay, king, Stargazer, sofh, obi_wan_Kenobi, kitten, pyari, anushah, AlexenderTG, b000m, xpert, Bss (bittersweetsymphony – I did not miss you this time!(m0r0n and nightman 2000c)

The short, plaintext[17] black-on-white defacement was visually different from the rather busy style the pair would later adopt as part of the WFD, and much shorter, but the core message – hacking to promote "global awareness" of Muslim human rights – would remain consistent. The Zone-H archive records 62 hacks under the m0r0n and nightman's handle over the next three months. It is no accident that this defacement was written in English. For the WFD, as with other Islamic hacker groups, "English is currently the lingua franca" and all defacements are posted in English.(Taggart 2001)

---

[17] The term "plaintext" refers to messages constructed strictly in the standard ASCII character set, without the use of images or formatting.

Not long after m0r0n and nightman's hacks first appear in mirror archives, the WFD makes its first appearance. According to the group, its various members came together "sort of haphazardly" ("India Cracked interview with WFD" 2001):

> There is nothing official about the formation of WFD. The first defacement as mirrored by hacking mirror alldas.de is 20th November 2000. At the peak of the Middle East cyberwar that had broken out in late October, m0r0n and nightman were already defacing Israeli websites to spread the truth. CyberPunk & B_Real approached them and joined hands with them on the "global awareness" issue. Then other cyber-warriors like Sub-0 and n00gie shook hands with the truth. We are a team! (m0r0n and nightman 2002)

The first WFD-credited hacks, in November 2000, had no political content – though they bore a closer visual resemblance to the WFD's eventual style. The first WFD defacement that is preserved in the Attrition mirror was an attack on www.oem.com.mx, in which the site was defaced with a simple Flash movie that read, over several screens:

WFD Crew own this
Owned by World Fuck Defacers
members: l^cyBeRpUnK^l, B1n4ry C0d3, Brake^Off,
hid30us, phel0n, Philer, DELAY, Scan_disk&YZT, Module.
wfd@mail.com
weak security means stupidity
(WFD 2000a)

The only elements of this hack that lived on in the style of the hacktivist WFD were the use of Flash, the use of the WFD acronym, and a handful of members: CyberPunk, B1n4ry C0d3, Brake Off, and Module.

m0r0n and nightman were meanwhile continuing their plaintext defacements, expanding the length of their messages as well as the scope of their politics. For example, a November 28 defacement took on human rights in the former Yugoslavia:

> m0r0n and nightman own you. Yugoslavia, which Serbia is a part of started their movement against Kosovah in 1998 in which they conducted a scorched earth policy in Kosova, raising villages to the ground, creating an exodus of over one million refugees and internally displaced persons and committed horrific atrocities against unarmed civilians , including women and children. STOP KILLING INNOCENT CIVILIANS is our message to these people. Stop the violence in Kashmir and Palestine too. The human life is precious and you people donot give a damn about it !!! STOP IT!!! We wish every Muslim a happy Ramadan(or Ramzan). Please remember us in your prayers. All ifs and

> buts to .... m0r0nandnightman@hushmail.com . Greetz to GFORCE Pakistan, DoctorNuker , CyberPunk, B Real and company and all those who support us. Peace @ Kosova , Peace @ Kashmir , Peace @ Palestine and finally Peace @ EARTH! Long Live Pakistan ( Pakistan ZIndabad!!!)(m0r0n and nightman 2000c)

We find the WFD's first quasi-political hack on November 28, 2000, in m0r0n and nightman's plaintext style:

> 0wn3d by WFD now were defacing for Global Awareness, .....CyBeRpUnK strikes again(WFD 2000b)

By early December, the group had found its combination of political message and visual style. A December 3 defacement of a a regional government web site in Italy combined images from the Palestinian-Israeli conflict with a lengthy message about Israeli human rights violations in Palestine:


**Figure 5. WFD site defacement, December 2000.**

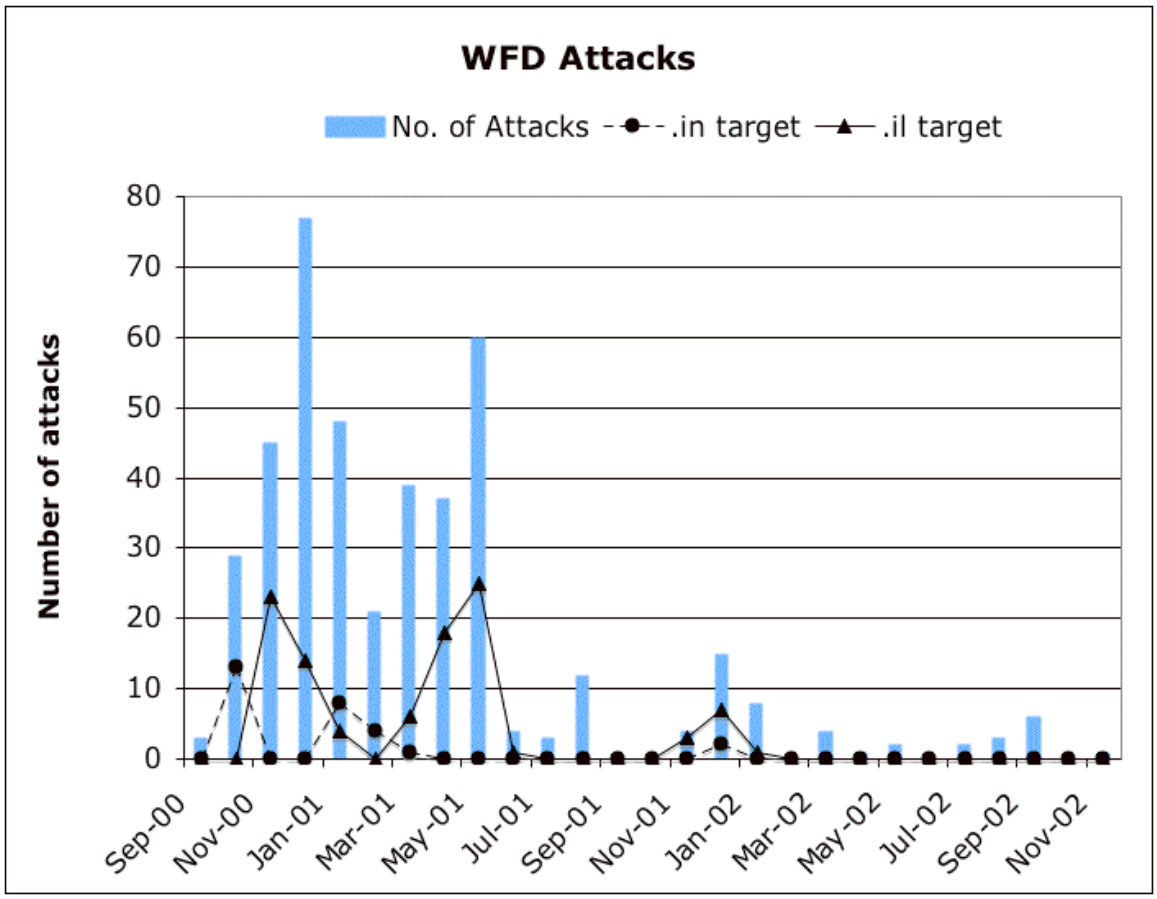



**Figure 6. WFD attacks by month and top level domain**

An analysis[18] of the defacement statistics archived on http://www.zone-h.org show that December 2000 was the WFD's most active month: Zone-H records 76 defacements that month, out of 424 from September 2000 to September 2002. This analysis further shows that while the group initially focused on Indian web sites in its late 2000 attacks, it quickly shifted to primarily attacking Israeli or Israel-linked sites.

[18] The analysis is based on a list of 424 attacks in the Zone-H archive, including those credited to WFD members m0r0n, CyberPunk and n00gie as well as those credited WFD itself. I used the top level domain of each target (e.g. .com, .il, .in) to indicate the country of target, though this was really only useful in establishing the relative focus on Indian versus Israeli targets, since many targets with other TLDs nonetheless corresponded to Israeli or Indian web sites.

The top level domain (TLD) is only an imperfect measure of the targeted site's nationality, but the peaks in .il (Israel) and .in (Indian) targets do provide a rough indicator of the group's shifts in focus. But .il and .in targets only make up a total of 24% and 6.6% of the WFD's targets, respectively; the group also targeted many.com and .net sites, as well as some .mx (Mexican), .yu (Yugoslavian), .tw (Taiwanese), .au (Australian), .edu, .gov, and assorted other TLDs. Some of these other TLDs still corresponded to Indian and Israeli sites, such as www.semiotica.net (an Israeli site hit in April 2001), www.natyavihar.com and www.bonafidesurgicals.com[19] (two Indian sites hit in January 2001).

Some TLDs correspond to non-Indian, non-Israeli sites that were nonetheless strategic targets, such as the web site of a US Veterans Affairs clinic that was defaced with a message that began, "m0r0n and nightman of WFD (World's fantabulous defacers) own a Government site to spread their message."(m0r0n and nightman 2000a) A similar example was the Navy Marine Corps relief site defaced with the message:

> Site defaced by WFD (World's fantabulous defacers) Free Kashmir and stop the violence in Palestine!! The U.S. Military is giving a helping hand to the corrupt Indians and the Israelis. But they don't know that the truth always previals!! Contact us @ wfd2001@nightmail.com(WFD 2001)

And the web site of the Newspaper Association of America was attacked in January 2001 with a message about US complicity in Israeli actions against Palestinians:

---

[19] As with a number of sites that the WFD targeted, Bona Fide Surgicals is no longer online at this address. Because site identification was often crucial to assessing whether a target was randomly or strategically chosen, I used the waybackmachine to visit web sites that are no longer online. A project of the Internet Archive, the waybackmachine regularly archives cross-sections of the Internet such that at least some pages were archived for each of the sites I needed to identify.


**Figure 7. WFD site defacement, January 2001.**

The defacement contained a long multi-part message that included discussion of Palestinian feelings about Israeli occupation, details on specific incidents of anti-Palestinian violence, and a description of US assistance for Israel. Its opening words made the choice of target clear:

> The newspapers of America are full everyday with flagrant lies about the events happening in the Middle East. In fact, the entire American media distorts the truth and twists it as to manipulate the minds of the American people. Suffering Palestinian children are portrayed as "terrorists", simply because they fight for their freedom from an oppressor that seeks to destroy their hopes and dreams.

The defacement concluded in similar terms:

> Our message to the newspapers of America
> STOP BLINDLY SUPPORTING ISRAEL WHICH IS, UNDOUBTEDLY, THE LAST THEOCRACY/FASCIST STATE LEFT IN THE WORLD. START TELLING THE TRUTH ABOUT WHAT HAPPENED AND IS HAPPENING IN PALESTINE, as well as the truth about Kashmir and Chechnya.(WFD 2001)

Still other sites, such as trendmicro.com.cn (a Chinese computer company hit in December 2000) and www.vwtrendsweb.com (an automotive magazine) seem to have been randomly chosen. Another apparently random target, a now-defunct US-based

"Midwest Source for Hip-Hop Info and Gear", was defaced with a message that described the attack as retribution for a hack against an English language Muslim web site:

> This is a reply to the Israeli hackers who hacked www.iviews.com. Just to show them that we are not as yet caught or dead! We will always rise when we are needed! -- wfd!

In their interviews –- with me and with others – m0r0n and nightman are less interested in exploring the details of their hacktivism than in recapping the same issues they spotlight in their defacements. In response to the question "what effects do you think your hacktivism has had?" the pair offered a very long history of the Kashmir conflict, detailing Indian human rights violations in the region, before briefly addressing the original question with the comment that "[u]s defacing sites may not bring peace, but it will certainly create global awareness about the suffering of the Muslims of Kashmir, and the righteousness of their cause."

m0r0n and nightman appear to see their hacktivism as a world away from offline political action. When asked "what other kinds of political activity have you been involved with, on or offline?" they responded:

> Haha ... we've helped Osama Bin Laden in doing some stunts & stuffs! Man, we're hacktivists. It's not PHYSICAL WAR! [20]This is the only thing we do. We do what we're best at!(m0r0n and nightman 2002)

---

[20] This argument seems to do justice to the experience of at least one of the WFD's targets. The webmaster of HelpingIsrael.com, an online crisis center that the WFD defaced, wrote of her ultimate reaction to the defacement:

> These digital demons were getting the best of me, and my husband was giving me that "You're a bit touched, aren't you?" look. So I blurted out: "You have no idea what it's like to be a victim of cyberterrorism!"
> I said this to a man who had spent 27 years in the IDF, who had buried comrades, friends and real terror victims.
> Then it dawned on me... it's "virtual," stupid! I'm letting my real world get swept away by some "virtual" goons.
> They can't undo the good that's already been done or break-up the supply lines and connections that have already been established between the donors and the communities (those transactions take place by "snail mail").

This was the only reference I found that provided any thread of connection between the WFD and the events following 9/11. The small spike in WFD activity that is apparent in September 2001 makes eminent sense in the context of the upsurge in both pro- and anti-Islamic web hacking after the September 11 attacks. But it is impossible to evaluate the WFD's response or position in regard to the 9/11 attacks because there are no mirrors available for the period in question.

The group's defacement streak came to a sudden and unexplained end in November 2002. My efforts at contacting m0r0n and nightman for an explanation have gone unanswered. One possibility is that the WFD has been absorbed into a new or different hacker group. Security analysts mi2g reported in June 2002 that the WFD had become part of a larger alliance of Islamic hackers, but their report seems to be at least partially based on the fact that "[I]n a recent anti-Israeli overt digital attack, WFD acknowledged 32 other hacker groups and individuals, many of them with anti-US/UK and anti-India agendas." ("Pro-Islamic Hacker Groups Joining Forces Globally" 2002) As the above examples of WFD hacks should make clear, it is a common hacking practice to send "greetz" to like-minded hackers, and not necessarily a sign of some more organized collaboration. My own research has found no evidence to suggest that WFD members are

---

> Let them waste their time, money and energy on virtual destruction, while I devote my energies to my real family and productive endeavors.
> Real anxiety is when you send your husband and children off in seven different directions in the morning not knowing if Hamas, those only-too-real masterminds of evil, are serious about their top-10 terror countdown.(Horowitz 2001)

now part of another organization; it seems equally likely that they have simply outgrown their hacking phase.

*Performative hacktivism: an introduction*

Performative hacktivism consists of legally ambiguous hacktions, undertaken by hacktivists with artist-activist backgrounds. It draws heavily on the tradition of political theater in its adaptation of hacking for political purposes. The term "performative" not only captures the broad notion of hacktivism as performance – which these hacktions most certainly are – but also the more particular idea of political protest as a "speech act". The notion of politics as spectacle that has informed performative hacktivism also characterizes a wider array of "carnivalesque" protest tactics popularized by the anti-globalization movement (Boje 2001).

Many performative hacktivists come from theater or art backgrounds, and see hacktivism as a new form of political art. Some of these hacktivists produce other forms of Internet or digital art, in addition to their hacktivism. And even those performative activists who are not artists per se share the aesthetic and theoretical baggage of the postmodern left.

Some examples of art from members of the hacktivist community:
Carnivore (Alex Galloway)
Virtual Quilt (Carmin Karasic)
FadeForward (Ricardo Dominguez)

Since performative hacktivism emerges out of a left political culture, we should not be surprised that it usually focuses on left-wing issues such as globalization, liberation struggles (especially that of Mexico's Zapatistas), and corporate power. Many performative hacktions have been coordinated, or at least timed to coincide, with simultaneous street protests.

The most visible groups of performative hacktivists are the Electronic Disturbance Theater, ®™ark, and the electrohippies. The Electronic Disturbance Theater is a group of four U.S.-based activists who banded together in 1998 to create a digital protest in solidarity with the Zapatistas. ®™ark is a U.S.-based activist "mutual fund" that sponsors acts of "anti-corporate sabotage"—including a number of hacktions. ("®™ark Website", "Bringing it to You" page) It uses its status as a legal corporation to both spoof and (potentially) benefit from limitations on corporate liability(Sebok 2001). The UK-based electrohippies collective was created in July 1999 with the intention of using the Internet to challenge the commercialization of cyberspace; until it disbanded in July 2002, it focused its activities on anti-corporate hacktions like its virtual sit-in against the WTO.

Performative hacktions have encompassed a wide range of issues, but usually focus on offline issues like globalization and human rights. They almost always engage a transnational coalition of activists, even if the sites are assembled by hacktivists in one country who then solicit sit-in participation from a broader cross-national population.

Performative hacktivism mostly takes the form of virtual sit-ins or site parodies – forms of hacktivism with clear precedents in the traditions of street protest and political theater. This area of hacktivism has also made some moves into the field of software development, but only as a way of facilitating the primary tactics of sit-ins and site parodies. The EDT developed an open source version of its sit-in tools, and a group called the Yes Men have created software that automates the creation of web site parodies.

While performative hacktivist tactics are carefully constructed to avoid clear legal jeopardy, they are not without legal risk. The virtual sit-in tactic is essentially a less illegal version of the denial-of-service attack; since actual people are loading the pages that overload a server, it is not clearly illegal. But at least one virtual sit-in (conducted by the EDT in 1998) was counter-attacked by the U.S. military (Schwartau 2000), and a site parody (of the WTO's web site) faced the threat of legal challenge (Ramasastry 2002).

The intensity of the reaction that these hacktivists have provoked attests to the success of their hacktions as performance. Performative hacktivists are very much oriented to the public eye, and see their activities as a way of challenging corporate and media domination of public discourse. Their hacktions are aimed at shifting that discourse by raising awareness and creating public pressure – not at directly affecting outcomes.

As this may suggest, performative hacktivism is more theory-driven than other forms of hacktivism. Performative hacktivists often cite European critical theorists as sources of intellectual inspiration in their efforts to comprehend the political or performative dimensions of cyberspace: Ricardo Dominguez offers a typical voice when he writes that "[r]ecombinant culture, the implosion of genetics and speed, creates a spasm of hypermorphic delusion wherein Sandborn-understands-Virilio-as-Hegel-understands-Napoleon."(Dominguez 1996) Different performative hacktivists offer different theoretical takes on the nature of hacktivism, but a common theme is the way the Internet has changed the relationship between the human body and human identity. Performative hacktivists use the Internet as a way of exploring the new virtual body, and its relationship to the corporeal world; they sometimes argue that power has shifted

altogether into the virtual world, and thus needs to be challenged within cyberspace itself. In the opening words of *The Electronic Disturbance*, a theoretical work that has informed the activities of the EDT in particular:

> The rules of cultural and political resistance have dramatically changed. The revolution in technology brought about by the rapid development of the computer and video has created a new geography of power relations in the first world that could only be imagined as little as twenty years ago: people are reduced to data, surveillance occurs on a global scale, minds are melded to screenal [sic] reality, and an authoritarian power emerges that thrives on absence. The new geography is a virtual geography, and the core of political and cultural resistance must assert itself in this electronic space. (Critical Art Ensemble. 1994, p.3)

*Performative hacktivism: The case of the Electronic Disturbance Theater*

The Electronic Disturbance Theater was the first performative hacktivist group, and remains an influential leader. The group has four members, all American, although they are geographically scattered and mostly collaborate remotely. Best-known for its invention of the virtual sit-in technique, the group works on a variety of offline progressive issues – most notably, the human rights record of the Mexican government – with projects that are as much art as politics. If performative hacktivism owes a big debt to political theater and digital art, that is partly the influence of the EDT.

The EDT, in turn, owes a debt to the Critical Art Ensemble (CAE), a group that included EDT founder Ricardo Dominguez. A handsome Mexican-American with funky horn-rimmed glasses, Dominguez talks just like he writes: heavy on the critical theory, more like a performance than a conversation. The artists of CAE collectively wrote several books that lay the theoretical foundations for performative hacktivism, including *(Critical Art Ensemble 2001; Critical Art Ensemble. 1994; Critical Art Ensemble. 1996).* In an interview, Dominguez said he left the CAE because he was frustrated that the group was unwilling to put its theories of "electronic civil disobedience" into practice.

Dominguez later made that translation himself, as the founder of the Electronic Disturbance Theater. The EDT was initially geared towards action in solidarity with Mexicon's Zapatista rebels. At the time of the 1994 rebellion, Dominguez was an aspiring digital artist, supporting himself as a network administrator for a progressive computer network in New York City. He was particularly impressed by the Zapatistas' creative use of the Internet, and by their innovative ways of engaging the broader Chiapas community. Take their concept of organizing topical roundtables: setting up discussions around different topics, like music or literature, so that regular people could talk about their ideas and help the Zapatistas brainstorm.

Dominguez decided to adapt the Zapatatistas' tables to an international network setting. He elicited an invitation from MIT as a sort of artist-in-residence, while remaining primarily in New York. But MIT still gave him the resources he needed for his own creation of Digital Zapatismo: a virtual network table, an extension of the Zapatistas' own network table.

He used free audio and video software to run a virtual network table three times a week, for four months. The "table" consisted of inviting various people to talk to him, either by phone or in person; he then broadcast the whole thing over the Internet, and projected it at MIT. Discussions covered a range of issues the Zapatistas had raised, from the future of neoliberalism to the rights of indigenous peoples. These conversations lasted anywhere from two to six hours at a time.

Through his network table, Dominguez came into contact with the other three future members of the EDT. Carmin Karasic was the MIT lab assistant assigned as his technical support. Stefan Wray was living in Austin, Texas when Dominguez

interviewed him about his writings on the US military's role in Mexican drug wars. And Brett Stalbaum was a fellow Internet artist, based in California, who joined Domiguez's mailing list.

The four formed a partnership when the Mexican government returned to Chiapas in full force in December 1997, leaving forty-five unarmed peasants dead in the village of Acteal. The "Acteal Massacre" galvanized the members of Domiguez's incipient network, beginning with Karasic, who e-mailed Dominguez with a request for the names of the Acteal dead. Her intention was to create an electronic monument herself.

Meanwhile Dominguez had been contacted by the Anonymous Digital Coalition, a group of activists based in Italy. The ADC had developed a plan for encouraging people to simultaneously visit a given Mexican government website, constantly reloading a given web site until the server slowed or crashed. Dominguez forwarded the ADC e-mail to his own e-mail list, and immediately heard back from Stalbaum. Stalbaum offered to write a simple program that would make web browsers reload the targeted web page automatically, greatly increasing the effectiveness of the attack. But he was only interested in writing the program, and not in designing its appearance.

Dominguez's solution was to enlist Karasic to design the interface, integrating the net attack into her plan for an Acteal monument. Wray was brought in as a fourth collaborator, to give theoretical depth to their work. Within two weeks, the team had created the first "virtual sit-in" tool, which they named the Zapatista FloodNet. The FloodNet could be used to orchestrate a coordinated attack in which sympathetic computer users could cheaply and easily participate in a protest, from the comfort of their own homes or offices. The EDT would announce a given target and a protest date and

time. All a would-be participant needed to do was download the FloodNet code sometime before the protest was to take place. At the appointed hour, all those participants would activate the code –- itself just a simple script that sent a command to the participant's web browser – and all of their browsers would simultaneously point to the target's web site. The FloodNet code would automate the "refresh" function on the browser, constantly loading and reloading the target's web page on the computers of each and every participant. The flood of simultaneous, constantly re-issued page requests would overload the server. And while the effectiveness of the attack did not depend on the participants having any particular visual experience, the EDT designed the FloodNet code to incorporate a protest message.

The FloodNet sat halfway between a distributed denial of service (DDoS) attack (a longstanding hacker technique) and the kind of manual sit-in envisioned by the Anonymous Digital Coalition. In a DdoS attack, computer hackers infiltrate thousands of private computers in order to direct them to simultaneously target given web sites, so that the targets shut down in the face of overwhelming traffic. The tactic is effective, but lacks public credibility because it can be conducted by a lone hacker, appropriates the computers of innocent bystanders, and is unambiguously illegal. But the ADC's proposed tactic had the opposite problem: its reliance on individual users to target and reload web pages made it inefficient, and unlikely to yield any tangible results without millions of simultaneous participants.

The EDT's FloodNet, in contrast, could hope for some effectiveness – in slowing or even crashing servers – even if participants numbered only in the thousands. But the need for some critical mass allowed it to lay claim to the tradition of "mass" protest, as

did the fact that its effects would be proportional to the number of participants (because more participation translates into more traffic, and more traffic translates into slower and slower servers). The EDT also tried to shore up its legitimacy by departing from usual hacking practices, according to Dominguez:

> I decided that we would become the Electronic Disturbance Theater, and then we made a decision that was very very strange but that seemed on a gut level what we needed to do, but it went against all the usual elements. We decided not to be anonymous. Not to be secret – to be transparent. And this went against hacker culture, which is about anonymity, which is about secrecy. We also pushed open source. That is, all our code had to be very simple, you know, anybody can use it. We would also let people know what we were doing, when we were going to do it, how we were doing it. And I felt this would create a much better drama.(Dominguez 2002a)

EDT's first action was on April 10, 1998: a virtual sit-in targeting the web site of Mexican President Ernesto Zedillo. Stefan Wray later noted that:

> We had 8,141 separate hits on the Zapatista FloodNet browser aimed at Zedillo's web site. We are fairly certain we did not shut down this web site, although we did receive a message that read, 'I think the Mex server just crashed.' We think this message reflects the fact there were sporadic moments when access to the site was slowed down or even blocked.(Wray 1999b)

In what would become characteristic of both the EDT and the larger world of performative hacktivism, the group focused as much on media coverage of their hacktion, as on the hacktion itself. From the beginning, the group measured its success more in terms of press coverage (which drew attention to the Zapatista plight) than in terms of the actual slowing or crashing of servers. By that standard, the EDT could be thrilled with its first FloodNet, which was covered on the web site of the New York Times:

> Don't call them hackers. Ricardo Dominguez and Stefan Wray consider themselves theorists and practitioners of "electronic civil disobedience." …In an early test of their system, Dominguez and Wray posted messages in the Zapatista networks in early April, calling for colleagues to link to FloodNet on April 10. The target that day was the Web site of President Ernesto Zedillo of Mexico. According to Dominguez, 8,141 surfers around the world connected to Flood Net that day, which resulted in some slowing down and interruption of the Zedillo site. Dominguez added that a computer from Mexico tried to hack into Flood Net and disable its program, but was unsuccessful.(Kaplan 1998)

The encouragement came at a crucial time, when the EDT was escalating its FloodNet campaign. Throughout the spring, they kept their sights trained on the Mexican government, organizing actions, giving talks, and publishing articles. In a later speech, Wray described this period as one in which:

> our greatest admirers were among digital artists, while our harshest critics were within the left. Most digital artists were able to see immediately, almost intuitively, the value of our work. But leftists raised age-old questions about effectiveness and responsibility, while hackers thought that we were too soft. Through quite a number of email listservs, we provoked discussion among a range of people. Conversations about what we did and said rippled out way beyond our small group of four.(Wray 1999b)

Thanks to their rising status in the digital art scene, the group received an invitation to the Ars Electronica festival in Linz, Austria, which describes its mandate as

> tracking and nurturing the digital revolution, analyzing the social and cultural effects of digital media and communications technologies from critical as well as utopian, artistic and scientific perspectives, thinking them through and inferring potential developments.("Timeshift: The World in Twenty-Five Years" 2004)

The festival was scheduled for September, 1998. The EDT called its proposal for the festival the SWARM:

> Think of a swarm as an array of Flood Net-like devices, arising, acting, and dispersing simultaneously against an array of cyberspacial political targets. If the electronic pulses generated by our Flood Net actions are represented by a small mountain stream, the electronic pulses generated by a swarm of convergent ECD actions are a raging torrent.(Wray 1998)

The project was described in greater detail in the group's August 25 press release, announcing its planned action during the festival:

> NETSTRIKE AGAINST GOVERNMENT, MILITARY, AND FINANCIAL WEB SITES IN MEXICO, THE UNITED STATES, AND GERMANY: CALL FOR FLOODNET ACTIONS (SWARM) ON SEPTEMBER 9 -- AGAINST PRESIDENT ZEDILLO, PENTAGON, AND FRANKFURT STOCK EXCHANGE
>
> In solidarity with the Zapatistas, indigenous peoples in Chiapas, others resisting the Mexican government, the global pro-Zapatista movement, and people everywhere struggling against neoliberalism and the global economy, the Electronic Disturbance Theater urges SWARM actions, multiple acts of Electronic Civil Disobedience, on Wednesday, September 9, 1998.

To demonstrate our capacity for simultaneous global electronic actions and to emphasize the multiple nature of our opponents, FloodNet will target three web sites in Mexico, the United States, and Europe representing three important sectors: government, military, and financial.

In Mexico, FloodNet will target President Zedillo's web site, (http://www.presidencia.gob.mx/) an obvious choice and one we have made before. In the United States, FloodNet will target the Pentagon, (http://www.defenselink.mil/) also an obvious choice given the level of U.S. military and intelligence involvement in Mexico. And in Germany, FloodNet will target the Frankfurt Stock Exchange, (http://www.exchange.de/) a less obvious choice, but one that makes sense as it is a key European financial site with high symbolic value and as Germany is a major player in the global neoliberal economy.(Electronic Disturbance Theater 1998)

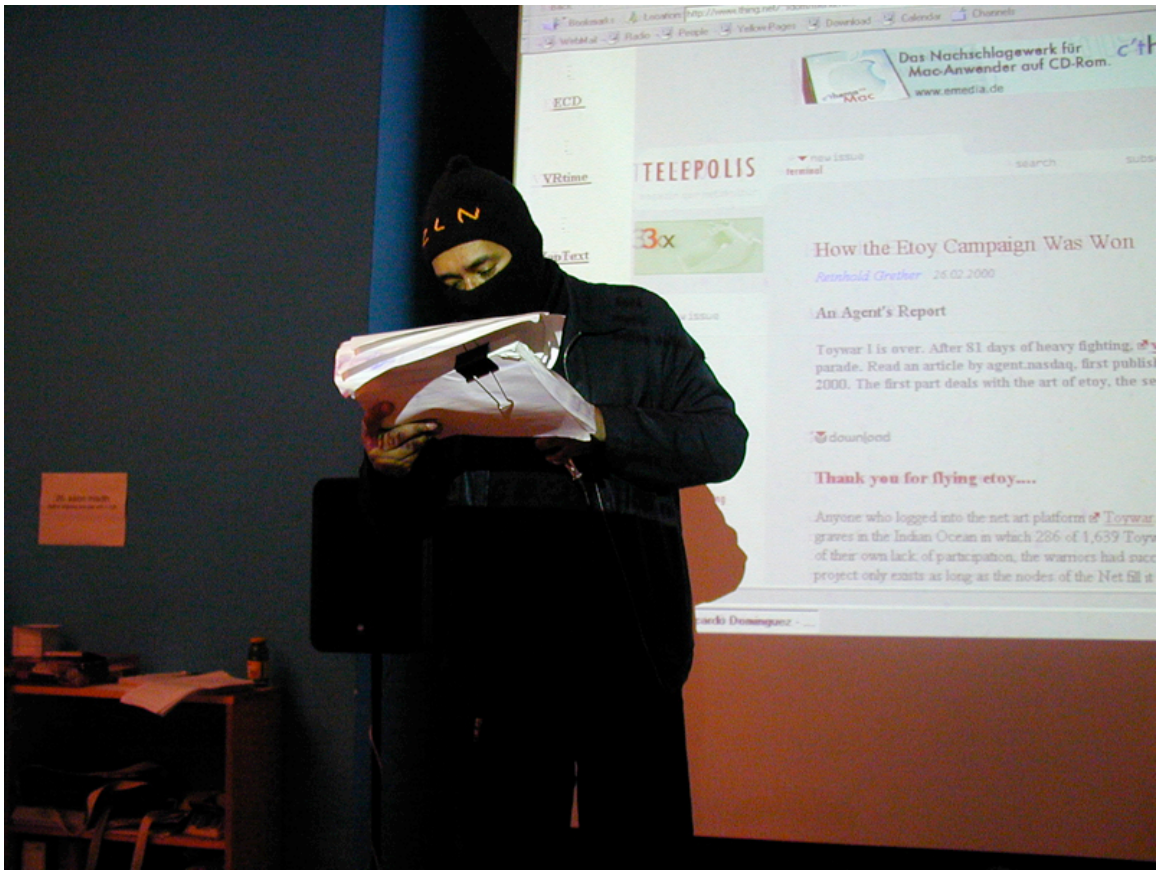



**Figure 8. Ricardo Dominguez in performance (occasion unknown).**
(Image available at **http://boo.mi2.hr/~zblace/mi2_4promo/**)

At the festival itself, EDT members found fresh fodder for their view that the FloodNet put them on the front line of a battle between digital art and computer hacking.

Festival organizers had convened a hacker gathering in conjunction with the festival, and according to Dominguez, the hackers took a hostile stand towards the EDT's planned installation. "They said, 'Ricardo, Stefan, what you're about to do will destroy infrastructure. And if you guys do it, we will take you down.' It was our first encounter with what I call the 'digitally correct' community. Those who believe that bandwidth is above human lives."(Dominguez 2002a) Also according to Dominguez, the group received its first threat:

> I was getting a lot of calls from the press. So at 7:30 in the morning I wake up haphazardly and they go, is this Ricardo Dominguez? I said, yes. Electronic Disturbance? Yes, yes. Then in very clear, Mexican Spanish, they said, we know who you are, we know where you're at, we know where your family is, do not go downstairs, do not do this performance. You know that this is not a game. You know what will happen to you.(Dominguez 2002a)

The group's immediate reaction was to put out a press release, announcing the threat. But the phone call was quickly eclipsed by the news that the installation itself had crashed.

> According to highly placed Pentagon sources, the Floodnet assault was pre-announced by the EDT so the Pentagon was able to prepare for it. Its response was orchestrated by the Defense Information Systems Agency (DISA), which has experience with both defensive and offensive cyber-tools. Once the attack began, the Pentagon launched a denial of service attack of its own. Requests from the EDT browsers were redirected to a Java applet called 'hostileapplet,' which Dominguez says crashed the browsers. The applet fired a "series of rapidly appearing Java coffee cups across the bottom of the browser screen coupled with the phrase 'ACK.' FloodNet froze," he says. (Schwartau 1999)

The Pentagon's counter-attack had implications that were larger than the EDT could have hoped for. An 1878 law, Posse Comitatus, prohibits the US military from engaging in domestic law enforcement; observers raised the question of whether the response to SWARM was a violation of that law.(Schwartau 1999) The group used the

issue to raise the possibility of a lawsuit – another publicity-generator – but did not pursue it.

A further encounter with the defense community came one year later, in the form of an invitation to speak – or "perform" – for a meeting of National Security Agency. Arranged by Schwartau, the meeting was intended to give NSA officials a chance to assess the EDT for themselves, and to consider whether the group's tactics – which were quickly spreading to a broader community – should be considered cyber-terrorism. While no public verdict was issued, the EDT has not recorded any subsequent counter-attacks from the Pentagon. Dominguez was nonetheless frustrated with what he perceived as his audience's failure to understand the EDT's performance:

> I don't know if you've ever read the very first play written here in the United States, "My Country Cousin," which is kind of a Daniel Boone type character from Kentucky being invited by his city cousins in Philadelphia – remember Philadelphia was the city of cities at that particular time – and they invite him to go to the theater. Well, halfway through the play he gets up, runs onstage, and hits the bad guy. And of course everybody's wondering what's going on. And they have to explain to the country bumpkin that it's a simulation, that the evil guy is not really evil, that he's only pretending. And so basically what the NSA and these information agencies, and hackers, in looking at EDT, are kind of like country bumpkins. They actually believe that Hamlet is killing Claudius. Instead of thinking hey, this is a really good performance, it actually seems real, it's moving, it's bringing me to really think out certain questions. And this is where they haven't read their Baudrillard. And perhaps they did read it, but misunderstood it.

The EDT has retained not only its high-minded theoretical approach, but also its specific dual foci on indigenous rights in Mexico, and distributed denial of service attacks. The group helped to organize a 2002 virtual sit-in against the Mexican supreme court, as well as a 2003 "Operacion Digna" protest against the Mexican government, and the Supreme Court of Chihuahua(fusco 2003)**.** But they have also broadened their activism to encompass issues like globalization and corporate power, collaborating in the

1999 “toywar” protest against the eToys corporation[21] and the 2002 protest against the World Economic Forum (Dominguez 2002b). The individual members of the EDT have also continued to pursue their respective careers as Internet artists and theorists by writing, performing, teaching, and exhibiting their work. The separate accomplishments of each EDT member and the collective reputation of the EDT as a hacktivist leader seem to be mutually reinforcing.

The EDT’s activities have been crucial in defining the activities and culture of the performative hacktivist scene. The group’s November 1998 release of its FloodNet code has allowed other groups to conduct virtual sit-ins for their own purposes: examples include a 1999 protest over arms control issues("Call for Electronic Civil Disobedience" 1999); an October 2000 Italian virtual sit-in over a censorship incident("The Axe of Censorship Falls on the Roman Civic Network" 2000); and a 2001 “living wage” virtual sit-in organized by the EDT on behalf of Harvard’s Progressive Student Labor Movement (Costanza-Chock 2001).

The EDT’s cross-pollination of political theater, digital art, and progressive politics has also been influential. It has extended networks among theater, art, and activist circles, and encouraged members of those circles to upgrade their technical skills. And its application of political hacking to offline issues has helped make hacktivist techniques – especially the virtual sit-in – part of the political repertoire for activists on a number of progressive issues, such as globalization, indigenous rights, and corporate power.

---

[21] See Chapter 4 for details on this case.

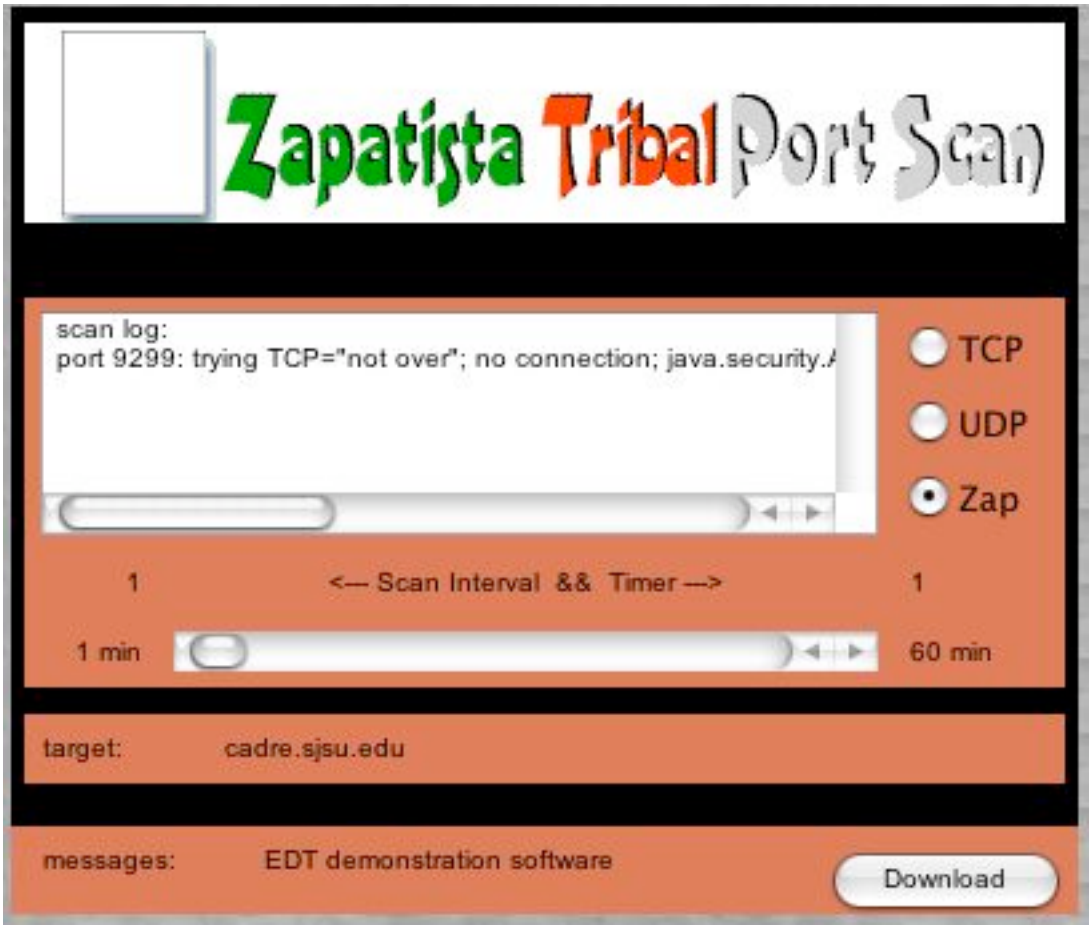



**Figure 9. The FloodNet Interface**

The EDT members seem to have benefited personally from their involvement in performative hacktivism. The two members I interviewed – Dominguez and Karasic – were basically unknown to the digital art world when they formed the EDT. But in the intervening years, they – along with Stalbaum and Wray – developed a significant profile in the worlds of digital art and progressive activism. Three EDT members (Dominguez, Karasic, and Stalbaum) have been frequent contributors to digital art shows, which have further exposed digital artists to the tactics and potential of performative hacktivism, Two members (Wray and Dominguez) have written and spoken widely on the theory and application of electronic civil disobedience, often drawing linkages to contemporary

critical theorists (such as Baudrillard and Virilio) that have currency with some artists and left-wing activists. Their personal profiles as artists and theorists have been boosted by the notoriety of the EDT, and the EDT's credibility has benefited from the increasing visibility of its members.

*Political coding: an introduction*

Political coding consists of hackers turning their technical skills into transgressive politics. These hackers are, metaphorically at least, the older brothers of political crackers. Many of the hackers who participate in political coding started out as non-political hackers, programmers or crackers, and came to political coding as an outgrowth of that activity. They typically adhere to the hacker convention of using handles (or pseudonyms), though the real names that correspond to most of these handles are relatively easy to ascertain.

Political coding so far reflects the cyber-libertarian worldview described by Barbrook and Cameron (1995), Katz (1997), Norris (2001) and others in their description of Internet political culture. This cyber-libertarian ideology emphasizes individual rights, especially online rights, as the most important political good. This viewpoint explains why political coding has focused entirely on issues that are directly related to the hacker community. Some hacktivists argue that this focus on Internet-oriented issues is core to the notion of hacktivism – that hacktivism is, by definition, activism related to the Internet. (Ruffin 2002)

Several political coding projects have facilitated the distribution of DeCSS, a piece of software that decrypts DVDs for playback on Linux machines. The software has been banned at the behest of the Motion Picture Association of America (MPAA) which

objected to the cracking of its CSS encryption, meant to prevent copying of DVDs. The DeCSS coding projects have been undertaken by solo or small-group actors, working anonymously or pseudonymously.

Another strand of political coding focuses on Internet censorship, particularly as it affects democracy activists in authoritarian regimes. Internet censorship has been the chief target of the Hacktivismo project, sponsored by the Cult of the Dead Cow (cDc). The Hacktivismo project has rapidly become the center of the political coding scene, and has received a great deal of media attention.

Both of these projects aim not at influence, but at policy circumvention. The various programs aimed at disseminating DeCSS are not trying to change the legal rulings on DeCSS decryption; they are trying to make those rulings unenforceable and meaningless. Hacktivismo doesn't try to directly change the Chinese government's Internet censorship policy; it develops ways of evading that censorship, regardless of the government's policy.

In the process of circumventing policy, these projects may also have some policy impact by raising awareness of the issues they focus on. The Hacktivismo team, in particular, takes care to publicize its activities in order to increase media coverage of the censorship issue. But awareness and influence are useful byproducts, not the primary goal.

The ability to circumvent policy depends on hacktivists committing the time to develop and complete a software product. The software that political coders develop is virtually always open source, which means it can be freely distributed, modified, and improved by other coders. The open source model lessens the burden on any one

developer or team, but software development is still a time-intensive form of hacktivism, compared with defacing a web site.

It is also skill-intensive, since it demands a core team of coders. But not all political coders are programmers: a number of people involved in the Hacktivismo project contribute other kinds of skills, like writing or web design. While this suggests that political coding does not necessarily require a high level of programming knowledge, even non-programmers tend to have some background in Internet-oriented activities. Although they may not be hackers per se, they are certainly conversant in hacker culture.

The legal risks associated with political coding vary from project to project. Jon Johansen, the Norwegian teenager who created the original DeCSS software, was indicted in Norway, and cannot travel to the United States for fear of prosecution there. Hacktivismo's Board of Directors includes Cindy Cohn, the lawyer for the Electronic Frontier Foundation, specifically to guard against the potential legal ramifications of Hacktivismo's various activities. Oxblood Ruffin, the founder of Hacktivismo, regards travel to China as an impossibility in light of his activities (Ruffin 2002).

Ultimately the success of political coding seems to lie in the high perceptions of efficacy among its practitioners. Hacktivists who have started out in other forms of hacktivism may be drawn in by the promise of direct effect. metac0m, creator of thehacktivist.com, comes from an activist background; but he has moved his energies into political coding because it "produces something tangible, rather than just protest" and is "something people can use." (metac0m 2002)

*Political coding: the case of Hacktivismo*

> Recently members of Legions Of the Underground "attacked" China yet again on their "human rights" condition. China setup firewalls in an effort to detour the people of the Chinese Republic from viewing sites which were found objectional by the Communist rule of China. These firewalls were paralyzed, and reconfigured. The group stands behind these actions 100% although the actions taken were that alone of the of the members who decided to impose action in an conformed fashion towards China. …All in all remember the information is out there, and it belongs to us. Join us in the fight to keep all data free. Keep the government(s) from impertinently tampering with rules, and regulations that go against our rights as inhabitants of this nation, as a society as a PUBLIC of the U.S.A (or whatever other country)... Ban together, and speak out in numbers before your right to speak is contraband entirely.(Optiklenz 1998)

When the Legions of the Underground (LoU) published this item in its December 1998 newsletter, hacker forays into anti-censorship activism were just a footnote in the hacker scene. But the LoU's hacks, led by notorious hacker Bronc Buster, were just the beginning. Anti-censorship hacking – using the tools of political crackers – soon gave birth to the more sophisticated tactic of anti-censorship coding. And at the forefront of this new field of activity was the Cult of the Dead Cow and its offshoot, Hacktivismo.

Hacktivismo initially emerged as a project of the Cult of the Dead Cow, a Texas-based hacker group that has used media savvy to solidify a reputation as a field leader, and "expanded the domain of hacking into the realm of the political" (Thomas 2002). The cDc was the elite of the hacker world, a US-based hacker group that dated back to 1984 (the Internet's equivalent of the Paleolithic era).

The group's founder, who uses the handle Grandmaster Ratte, started the cDc as a fourteen-year-old kid in Lubbock, Texas; eighteen years later he still reigns over the cDc from New York City, where he spends his non-work hours recording hip hop music in his apartment. When we met for an interview his references to his boogie board and his BMX bike reinforced the impression of talking with a teenager; but his aspirations include very middle-aged dreams of an RV, kids, and work as a day trader. His approach

to the cDc was an equal mix of the adolescent and the adult: he talked about making the group "big and popular", but says that goal is driven by the fact that he "wants kids to do something with their skills"(Grandmaster Ratte 2002). Until Hacktivismo, cDc was best known for its "Back Orifice" software program, which revealed some major security problems with the Windows operating system.


**Figure 10. An example of the cDc's distinctive visual identity**
(designed by Sir Dystic; online at http://www.cultdeadcow.com/large_image.php3?image_id=5)

In 1996, the cDc hacker Omega first used the phrase "hacktivism", inspiring cDc members to start registering domains like hacktivism.net and hacktivism.org (Ruffin 2004b). But nobody was more taken with the concept than the cDc's "Foreign Minister", who uses the handle Oxblood Ruffin. A fifty-two-year-old white man whose buzz-cut and casual clothes are the only mildly offbeat elements of his appearance, he is one of the oldest hacktivists in the sample. His personal demeanor hints at his background in public relations; charming and expansive, he kept up a lively conversation about hacktivism for five hours (my longest interview).

Ruffin's PR background includes ten years' work in the United Nations community in New York, primarily doing media work for UN-related publications. Originally from southern Ontario, Ruffin was living in Toronto at the time of our September 2002 interview. At the time he was working full-time on Hacktivismo; that brief stint of full-time Hacktivsmo work was preceded several months of public relations consulting, which in turn was preceded by a job at Open Cola, a Toronto software company that had some cachet in hacker circles.

Ruffin, by his own admission, is "not in the least technical" (Ruffin 2002)—though his notion of "technical" is clearly influenced by the hacker circles in which he moves. While he is not a full-fledged programmer, he is well-versed in web technologies, able to write computer scripts, and can even claim a youthful career as a "phreaker" – someone who hacks into telephone systems. Ruffin described his relationship to technology in colorful terms: "Did you ever see *Pretty Woman*? There's a scene where Richard Gere is driving a Lotus, but doesn't really know how to drive it. That's how I am with a really sweet computer."(Ruffin 2002)

Despite his technical limitations, Ruffin was invited to join the cDc in 1996. According to Ruffin, cDc membership is by invitation only: "if you ask to join, they'll never let you in." (Ruffin 2002) But Ruffin's online explorations led him into a regular correspondence with Deth Veggie, who forwarded their correspondence to the cDc members' e-mail list; soon, Ruffin received an invitation to join. Six and a half years later, Ruffin was clearly still thrilled by his membership in such a selective group; in the course of our interview, he described the cDc as "like Skull and Bones, but more

exclusive" and "the Beastie Boys of hacking", and noted that when he first saw the cDc web site, he thought it was "insane and brilliant".

When the cDc began playing with the concept of hacktivism, Ruffin had an opportunity to make a major contribution to the group's self-mythologizing. More than any of the cDc members, Ruffin was immediately taken with the concept of hacktivism:

> I always liked hacktivism as a word but thought the definition needed to be tightened up. Cyberwar had a fairly similar connotation; two big brains from RAND Corporation coined that in 1993. No, we needed something unique, something that had never quite existed in quite the same way before. It was Reid Fleming who brought in the hook. Reid set up hacktivism.org that featured a quote from the United Nations Universal Declaration of Human Rights (UNDHR). It was Article 19 and it read, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." The first time I read that I felt like my head had gone to heaven. That was it. We would link technology with human rights. (Ruffin 2004b)

Ruffin's efforts at putting meat on the bones of hacktivism started to take shape at the 1999 Defcon hacker convention in Vegas. In conversation with his fellow cDc members, Ruffin arrived at the idea of developing a tool that would take on the large state-sponsored firewalls that limited access to the Internet in countries like Saudi Arabia, Cuba, Tunisia, and China. Firewalls

> act as intermediaries between users and the rest of the Internet. In countries where the Web is censored, the only way to access the Internet is through the firewalls. A user enters a URL - the address of a Web page - into his or her browser. This URL gets passed to the firewall, which checks to see if it is one of those banned by the government. If the URL is not on the list, the firewall forwards the request for the Web page and the contents of the page are relayed back to the user, who can then read it. If the URL is on the banned list the firewall refuses to forward the request and sends a page back to user indicating that the page he or she requested cannot be viewed by order of the government. ("About the Peekabooty Project")

Ruffin began to recruit hackers for his new project, reaching beyond the membership of the cDc itself.

> Bronc Buster and The Pull from the United States, and The Mixter from Germany - who was then working as a security consultant in Israel - jumped on board. All brought different skills to the table and each was highly motivated. What is quite interesting is that we all knew each other by reputation but had never met in person. And over time ideas and code started to flow from one to the other to the point where we had our first

> prototype: a distributed network application called Peekabooty. It would allow users to bypass firewalls, national or corporate, and access the free side of the Web from a host computer. Part of our plan was to publicize state-sponsored censorship of the Internet and raise as much awareness as possible. (Ruffin 2004b)

The project's name was deliberately provocative. Grandmaster Ratte advised Ruffin to make hacktivism

**Figure 11. The Hacktivismo logo**


> sexy, sweaty, and dangerous. That's what would get hackers interested. They were the ones who were going to sit down and hack the code together for long hours and at no pay; not, with all due respect, the human rights establishment. They were just getting used to Web browsers. I decided to stick hacktivism in everyone's face with a product name that was impossible to ignore. (Ruffin 2004b)

The name might have been playful, but Peekabooty's intentions were serious. As the project's mission statement explains,

> Peekabooty is software that enables people inside countries where the Web is censored to bypass those censorship measures. The theory behind it is simple: bypass the firewalls by providing an alternate intermediary to the World Wide Web. …A user in a country that censors the Internet connects to the ad hoc network of computers running Peekabooty. A small number of randomly selected computers in the network retrieves the Web pages and relays them back to the user. As far the censoring firewall is concerned, the user is simply accessing some computer not on its "banned" list. The retrieved Web pages are encrypted using the de facto standard for secure transactions in order to prevent the firewall from examining the Web pages' contents. Since the encryption used is a secure transaction standard, it will look like an ordinary e-business transaction to the firewall. ("About the Peekabooty Project")

As detailed in Chapter 4, Peekabooty became mired in internal conflicts; its chief developer, Drunken Master, left the Hacktivismo team, and took the Peekabooty project with him. In response, Ruffin envisaged a new generation of anti-censorship tools, and recruited a new generation of programmers to complement his existing team. Today, the group claims forty-odd members "from the Americas, Europe, Russia, Israel, Iran, India, Australia, Taiwan, and the Peoples Republic of China." (Ruffin 2004b)

From this diverse group I interviewed a total of seven Hacktivismo members, in addition to cDc guru Grandmaster Ratte and ex-member Drunken Master (now going by his real name, Paul Baranowski). From Hacktivismo's Toronto contingent I interviewed Ruffin, and two members he recruited from Open Cola: Mr. Happy, a 29-year-old programmer; and Ca$h Money, a 32-year-old webmaster. I also interviewed metac0m, who started out as a hacktivist for traditional left-wing causes, got into anti-censorship hacktivism, and was then recruited by Ruffin; he still runs the biggest web site for tracking hacktivist activities world-wide. In Germany I interviewed Mixter, a 23-year-old Arab-German programmer, who remained one of the group's stars: he first popped into international headlines in 2000, when one of his software tools was rumored to be the engine behind a series of high-profile Internet attacks. I also interviewed two of Mixter's recruits: Lisa Thalheim, a nineteen-year-old university student in Berlin whom Mixter knew from the Germany's Chaos Computer Club (CCC), and Jules, another CCC member.

In their physical self-presentation, Hacktivismo members ranged from urban hipsters to stereotypical computer geeks. In their verbal presentation, they were almost universally sophisticated and polished[22], offering clear and often quite original political analyses of hacktivism, computer hacking, and larger social issues. Their idiosyncratic comments included:

---

[22] In view of Hacktivismo's internal struggles it was noteworthy that the one exception was Paul Baronowski, the programmer who split off from Hacktivismo by turning Peekabooty into an independent project. Baranowski lacked the ease that other Hacktivismo members displayed in their discussion of political issues, although he seemed comfortable discussing technical issues around programming Peekabooty. This suggested that the dispute over the relative importance of programming and p.r. contributions may have reflected underlying personality differences.

> "I don't entirely rule out defacements, but the people who do them pick targets that have nothing to do with what they're protesting. I've been tempted, but it's not worth it. I wanted to write an article called 'Why I didn't deface this site.'" (metac0m)
>
> "Everyone here (in Germany) was against the war that Bush wants. No everyone is in favor. It makes me angry that opinions changed without any new argumentation around it." (Jules)
>
> "I'm hoping to get into the question of 'can representative democracy work?'…Everyone is talking about direct democracy, but the problem with direct democracy is that you never get all the facts. Especially in the current system of advertising." (Ca$h Money)
>
> "Politics used to be determined by protests. Before that, guns. Now it's about who controls the technology. A technologically superior force can overcome one that's militarily or financially superior." (Mr. Happy)
>
> "I believe in thinking properly and using the scientific approach. But with such a complex problem (tackling censorship) -- if it doesn't work properly, someone might be killed. You can't just write code. They (Hacktivismo members) are all great coders. But they don't tend to be patient." (Lisa Thalheim)
>
> "Most of the poverty in the third world is not economic or exploitation but due to lack of freedom. In every third world country you have a totalitarian government or overregulation." (Mixter)

Baranowski was a clear outlier in his difficulty in articulating or conceptualizing the social, political and communications aspects of anti-censorship hacktivism; his interest and expertise is in the technical challenges. A former member of the Young Democrats, his most articulate case for Peekabooty was that "censorship rubs me the wrong way". (Baranowski 2002) In our conversation about the Hacktivismo rupture it was clear that he regarded coding as the "real" work of the project, and public relations as irrelevant; speaking of Ruffin, Baranowski said he was "just a PR guy." (Baranowski 2002)

The post-Peekbooty Hacktivismo has launched several projects of its own. Camera/Shy is a steganography program that "enables users to share censored information with their friends by hiding it in plain view as ordinary gif images"(Hacktivismo 2002); according to Ruffin, Hacktivismo "heard from a lot of

expat hackers from Iran, China, and the United Arab Emirates living in the West who were using it with their friends back home." (Ruffin 2004b)

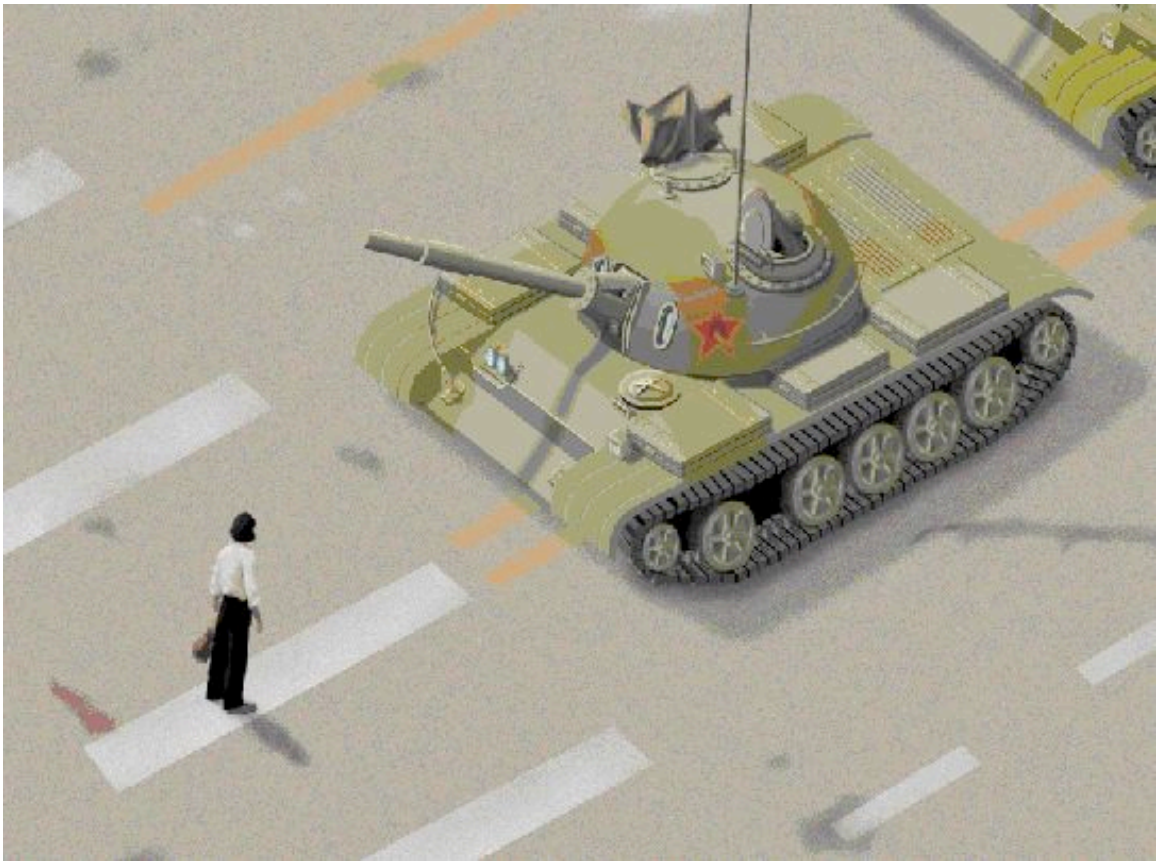


**Figure 12. A demonstration of Camera/Shy.**
This image hides the text of an article, "Dalai Lama Calls Wang Ruowang a freedom fighter" (stonefisk 2002)**.**

Hacktivismo's other major release was Six/Four, a peer-to-peer protocol for enabling censorship-free Internet traffic that was named for the date of the Tiananmen Square massacre. Six/Four is the closest thing to a new version of Peekabooty, in that it aims at circumventing firewalls. One of the project's biggest hurdles was obtaining US government approval: because the US government regulates cryptographic tools, and Six/Four uses cryptography, Ruffin worried that international distribution of Six/Four

could put US Hacktivismo members in legal jeopardy. So the group went through the US government's formal process for approving cryptography exports, and delayed Six/Four's release for the four months it took to get formal approval.

Arising out of Six/Four was a side project that may prove as significant as Six/Four itself: HESSLA ("The Hacktivismo Enhanced-Source Software License Agreement"), a legal framework that allows software developers to impose political terms of use on their users. HESSLA was inspired by the General Public License (GPL), a software license used by developers who want to make their software freely available and open to modification; but Hacktivismo was concerned that the GPL would allow human rights violators to use its tools, too. Their solution was a legal framework that would make the software available on the condition of human rights compliance:

> The HESSLA explicitly prohibits anybody from introducing spy-ware, surveillance technology, or other undesirable code into modified versions of HESSLA-licensed programs. Additionally, the license prohibits any use of the software by any government that has any policy or practice of violating human rights. The most novel innovation in the license distributes enforcement power instead of concentrating it in Hacktivismo's hands. If it is discovered that any government has violated the terms of the license, the HESSLA then empowers end-users to act as enforcers too. (Ruffin 2004b)

While Ruffin acknowledges that it is unlikely that anyone will use HESSLA as the basis for a human rights lawsuit, he says that Hacktivismo will be satisfied if they "deter at least some of the 'evil-doers' from using our software." (Ruffin 2004b) It is harder to gauge the direct impact of the software itself, for reasons that are intrinsic to the nature of the project. According to Ruffin,

> We've gotten email from people in the PRC and Iran saying that they'd been using Camera/Shy and thanking us, but they didn't say what kind of content they were trading in. We probably got fifty pieces of email when the software was originally released; still get the odd piece here and there. I met a guy [American] at HOPE who said he'd been using Camera/Shy and posting content for some friends in the UAE, but again, just a very quick hello, then he ran away.(Ruffin 2004a)

The Hacktivismo story highlights the extent to which political coding is going mainstream – thanks in no small part to Ruffin and his collaborators. After years of covert hacker wars between the US and China, the US government has now openly embraced Hacktivismo-style activism as a tool of its foreign policy. The Voice of America has launched its own anti-firewall tool, modeled on Peekabooty and Six/Four. And the US Congress recently approved the creation of an "Office of Global Internet Freedom," charged with combating Internet censorship through the use of hacktivist tools; Hacktivismo was consulted during the legislative process.

Hacktivismo's marriage of hacking and activism has helped bring not only hacker tools, but also the hacker agenda, into the political mainstream. While media pundits exclaimed over modest innovations like online petitions and virtual primaries, Hacktivismo insinuated far more confrontational tactics into the political toolbox. Thanks to Hacktivismo, governments are now adopting hacktivist tactics as their own, and Hacktivismo has thrust the Internet itself to the center of the policy stage. Their success makes a compelling case for hacktivism's growing influence on both the means and ends of twenty-first century politics.

*Transgressive hacktivism: the commonalities of political coders and performative hacktivists*

Reflecting on the three types of hacktivism, we see that it is not merely hacktivist origins that define, unite, or divide different hacktivists. The orientations of different hacktivists – whether outlaw or transgressive – form a second crucial dimension, dividing coders from crackers, and aligning coders and performative hacktivists. A brief review of

the commonalities among political coders and performative hacktivists helps to flesh out the notion of a transgressive orientation, and confirms the line between transgressive and outlaw orientations as a crucial element in modeling hacktivists types.

Both political coders and performative hacktivists try to skirt the boundaries of the law by refraining from activity that is unambiguously illegal, like cracking, instead staging hacktions that may or may not be illegal, but for which they are unlikely to be prosecuted. The virtual sit-in technique, for example, was deliberately designed to circumvent restrictions on denial-of-service attacks; because virtual sit-ins rely on actual human beings rather than "zombie"[23] computers to attack their targets, they are probably legal – or at least, less illegal than distributed denial-of-service attacks. Some hacktivists draw the line at their own national borders; they confine their work to activities that are legal in their own country, but recognize that their hacktivism may preclude traveling to the countries they have targeted.

Political coders and performative hacktivists also share norms of accountability to the liberal democratic legal order. Political coders often use handles, but these pseudonyms are almost always traceable to a real-world identity – more like nicknames than like shields. Performative hacktivists likewise either use traceable pseudonyms, or operate under their everyday legal names.

Political coders and performative hacktivists have the same propensity for collective action. They typically work in medium-size groups, but often aim at mobilizing much larger numbers of participants. Hacktivismo members and DeCSS distributors may

---

[23] When computer hackers surreptitiously take command of other people's personal computers during distributed denial of service attacks, the remotely controlled computers are called "zombies".

number in the dozens – but the impact of their hacktions depends on hundreds or even thousands of people putting the software to use.

Finally, political coders and performative hacktivists share a tendency for multinational engagement, working with hacktivists across national borders. For political coders this fits with the hacker-programmer tradition of discarding superficial or irrelevant information like gender, race, or nationality; for performative hacktivists it fits with postmodern notions about the transcendance of "meatspace"[24].

There are two major ways in which the orientations (as opposed to the origins) of political coders and performative hacktivists diverge. First – as noted in my discussion of hacktivist origins – political coders tend to focus on online issues, while performative hacktivists focus on offline issues. Second, performative hacktivists (like political crackers) tend to focus on policy change, while political coders focus on policy circumvention[25].

Performative hacktivism, like most forms of political participation, is directly or indirectly aimed at influencing the decisions of policymakers – whether those policymakers are businesspeople, government officials, or members of international organizations. Even efforts that seem to focus on galvanizing public support – like creating web site parodies – are pursuing public support as a means of effecting policy change by indirectly influencing policymakers.

The fact that performative hacktivism is aimed at policy or public influence can be obscured by the directly transgressive nature of many performative hacktions.

---

[24] Hacker jargon for real life, as opposed to cyberspace.

[25] This distinction is explored at greater length in Chapter 4, which focuses on the phenomenon of policy circumvention.

Hacktivists may use virtual sit-ins or parodies to directly target the objects of their wrath, but the political significance of those hacktions lies in their ability to command media or public attention. However direct the transgression, it ultimately relies on a policy decision (often, a decision by the hacktion's target or victim) in order to effect any change in political outcomes. Creating a fake WTO web site does not turn the WTO into an anti-globalization organization; it can only hope to embarrass or pressure the WTO into considering the larger issues around trade integration.

Political coding, in contrast, tries to circumvent policymakers by producing software that renders policy ineffective or irrelevant. Software that decodes DVDs circumvents copyright laws; software that reroutes web traffic circumvents censorship laws in authoritarian countries. The kind of hacktions thus present a far more fundamental challenge to our notion of politics and political participation. As long as participation is geared towards policy influence, it corresponds roughly to models of participation as voice; when it is geared towards policy circumvention, it looks more like exit.

**Conclusion**

The three types of hacktivism not only reflect variation in the political origins and orientations of hacktivists. Each type of hacktivism also has a distinct profile with regard to the other hacktivist and hacktion characteristics I identify earlier in this chapter. The profile of each type of hacktivism can be summarized by those characteristics (see Table 7, below).

These types are more than useful intellectual constructs: they represent meaningful divisions between political crackers, performative hackers, and political

coders. These divisions manifest in tensions and sometimes open conflicts between various groups of hackers. When the political crackers of the Legion of the Underground declared a cyberwar on Iraq and China in 1998, the cDc and other hacker groups issued a joint condemnation of the declaration of war("LoU STRIKE OUT WITH INTERNATIONAL COALITION OF HACKERS: A JOINT STATEMENT BY 2600, THE CHAOS COMPUTER CLUB, THE CULT OF THE DEADCOW, !HISPAHACK, L0PHT HEAVY INDUSTRIES, PHRACK AND PULHA" 1999). Oxblood Ruffin has likewise criticized the virtual sit-in technique of the electrohippies, and EDT member Ricardo Dominguez describes hackers as caring more about computers than about people.

The distinctions between political crackers, performative hackers, and political coders illuminate each of the theoretical problems posed by hacktivism. As the following chapters turn to questions about collective action, policy circumvention, and democratic deliberation, we will see how the differences among hacktivists translate into significant divisions in each of these arenas.

**Table 7: Types of hacktivism, summarized by characteristics**

| | Forms | Origins | Orientation | Issues | When |
|---|---|---|---|---|---|
| **Political cracking** | Defacements<br>Redirects<br>Denial of Service Attacks<br>Sabotage<br>Information Theft | Hacker-programmers | Outlaw | Online issues, gradually encompassing offline issues | Since early 1990s (with earlier antecedents); starts to encompass general issues only since 1997/98 |
| **Performative hacktivism** | Parodies<br>Sit--ins | Artist-activists | Transgressive | Offline issues | Since 1997 |
| **Political coding** | Software development | Hacker-programmers | Transgressive | Online issues | Since 1999 |