HACK THIS ZINE

v. 11 summer...fall 2010

HACK THIS ZINE

v. 11

summer...fall 2010

EXPLOIT CODE NOT PEOPLE

EDITORIAL

DEAR READERS,

Lock up the kids,
and call the police ..

== HOMELAND SECURITY ALERT:
SUBVERSIVE MATERIALS
ENCLOSED ==

The government considers your very interest in this subject to be dangerous. Soon you will not even be able to create or distribute these files without being made into a criminal by the corporate media. You are not the criminal,
they are the criminal. You know this, now give them some fucking justice.

The texts enclosed contain stories, projects, and ideas from people who have found ways to unplug themselves and hack the system. We can give you the ammunition and a network of hacktivists to network with, but they alone will not be enough to set yourself free. Only you can break your chains. Turn off your television and take to the streets. Get involved!

... Lock up the cops,
and call the kids!

Thank yous:

Thanks to everyone who helps keep our bits flowing securely and to everyone who helped work on this issue of the zine: Ringo, Discordia, Anonymous, The Pirate Bay, 2600, the Bay Are Anarchist Bookfair, Bradley Manning, the Wikileaks Crew, alxciada, anders, flatline, evoltech, sally, sexy hexy, frenzy, AnarchistNews.org (good work with the /ban trolls), postmodern modulus III, RiseUp.net, March-Hare Collective and everyone else who we forgot that is working to protect and support the struggle. Thanks to all of those resisting police violence in their communities, all those facing state oppression, and those engaged in the struggle everywhere. Thank You!

Questions? Comments? Article Submissions? Get a hold of us at: email: staff [at] hackbloc [dot] org
our website: hackbloc.org/contact

Get Copies Of The Zine: Electronic copies of the zine are available for free online at the hackbloc website: https://hackbloc.org/zine

There are two versions of the zine: a full color graphical PDF version which is best for printing and also includes all sorts of extras, as well as a raw TXT version for a more readable and compatible format. Having the zine in your hands is still the best way to experience our zine. If you can't print your own(double sided 8.5x11) then you can order copies of this issue and all back issues online from Microcosm Publishing (microcosmpublishing.com) who are based out of Portland. If you are at the Portland, Oregon Anarchist Bookfair this year in you will be able to find us tabeling with the Matt and Maggi Support Committie (mattandmaggi.tumblr.com) and Cloacina (cloacina.org) . We are seeking translators to translate Hack This Zine into other languages, if you are interested send an email.

NEWS

Snitch Darren Thurston Offering Security Advice for Mac Users

If any of you have been getting Macintosh security advice from a person who goes by the name Hard_Mac, now would be a good time to cut ties. That person is actually Darren Thurston [1] [2], a known snitch from the green scare cases. Who needs good computer security when one of your friends will sell you down the river anyway? He also goes by Rad_Boy.

More references: Vancouver Anarchist Online Archive[3], crimethinc[4], Portland IMC[5]

1. https://twitter.com/hard_mac
2. http://social.implu.com/t/hard_mac
3. https://vanarchive.wordpress.com/2010/01/18/darren-thurston-a-history-of-vancouvers-most-notorious-activist-turned-police-informant/
4. http://www.crimethinc.com/blog/2007/12/22/on-darren-thurston%E2%80%99s-statement-%E2%80%9Cfired-back%E2%80%9D/
5. http://portland.indymedia.org/en/2007/05/360251.shtml

EDITORIAL

So, you thought this was just some boring hacking zine? The zine you hold in your hands has a long history, which may be surprising to you since you may have never read it. We have worked overtime to do outreach and make sure it gets in as many hands as possible. Like many small-time publications, our zine has gone through a lot of changes from our writers to what we emphasize to what we aim to do.

This is about hacking, revolution, activism, insurrection, social struggle, revolt, dissent, direct action, and where they all merge. We've got a little for everybody, and a lot for that special somebody. Hacking zines have been done to death an unquantifiable amount of times. Remember the "new" phrack? Remember the new "blacklisted 411!"? These hacker zines failed for several reasons but some of the main ones were the lack of interest and the lack of competent authors.

We don't need another zine about how you explored some pbx system and did nothing with it. We don't want to know about some new hack you discovered in a social networking site which was rendered totally useless when you told the overlords. We

EDITORIAL

don't want another how-to which doesn't actually work because the publisher was too scared to publish it accurately. We don't want to hear you whine about how hackers just don't have any ethics or professionalism or how we're always being portrayed wrongly in the media.

Hacking has a rich history and it won't be ruined by the whitewashing that the security industry has tried to put it through. We study and tinker with systems because we want to, not because somebody gave us the modem and said, "here, make it go faster". We find security holes in programs because we're curious and we told the world because it was important. We knew it would make the company look bad, but we did it anyways because without the spreading of that knowledge, thousands if not millions of users would be at risk. When they tell us not to research, we turn right around and find another vulnerability to smack in their face. When they tell us not to publish our findings, we get hundreds of our friends to mirror them on their sites. We'll leak it all, shut it all down, build it all back, sit in our chairs, and smile at the quickly-scrolling output which would be meaningless to anybody else.

This issue brings our zine back to the basics. The last few issues have been too focused on the technical, a little far from our politics, hard to get a hold of, and hard to read when printed in black and white, and overall plain and boring. Looking back

NEWS

FIRST SALE DOCTRINE DESTROYED BY FEDERAL APPEALS COURT

"A federal appeals court said Friday that software makers can use shrink-wrap and click-wrap licenses to forbid the transfer or resale of their wares, an apparent gutting of the so-called first-sale doctrine.

The first-sale doctrine is an affirmative defense to copyright infringement that allows legitimate owners of copies of copyrighted works to resell those copies. That defense, the court said, is "unavailable to those who are only licensed to use their copies of copyrighted works." (.pdf)

The 3-0 decision by the 9th U.S. Circuit Court of Appeal, if it stands, means copyright owners may prohibit the resale of their wares by inserting clauses in their sales agreements."

More at http://www.wired.com/threatlevel/2010/09/first-sale-doctrine/

NEWS

Facebook Adds Secret "Delete Account" Option

Facebook has added an account delete option but it wasn't well publicized until around a day ago on Slashdot[1]. Unlike the "de-activation" many users have been forced into when trying to close their account, the delete function actually deletes your account and all your personal information according to Facebook. If you're excited to hear the news, here's the link: http://www.facebook.com/help/contact.php?show_form=delete_account

1. http://www.slashdot.org

Courts Give Thumbs Up to Warrantless Cell Phone Tracking

Wired reports that an appeals court has given the green light for law enforcement to get cell phone location data without a warrant. For more information, see the article at: http://www.wired.com/threatlevel/2010/09/cell-site-data

EDITORIAL

in our archives we figured out what we were missing and one thing we're certainly lacking is hands-on stuff anybody working for social change can do. We were missing the bleeding-edge exciting politics and how-to articles we used to have. We've been focusing too much on keeping up with the news and too little on shaping the future.

We don't believe in length requirements, specific political platforms which you must obey, or an intimidating board of editors. If you feel compelled to write something, send it to us. If you mix up your regular technical writing with a well-earned dose of hard-hitting politics or inspiring stories, send it to us. We'll get back to you quickly and let you know if the article will be included or not. If you want to write anonymously, we love that. If you have photoshop skills and want to make images to put in our zine, send them to us and we'll put them in. If you have good layout skills or want to design a cover, get on our discussion list (http://lists.hackbloc.org/mailman/listinfo/hackthiszine) and we'll hook you up with what you need. We do work parties in IRC so anybody who is interested can join in.

If you find that the articles inspire you to get out there and do something, do it. Part of this zine serves as political analysis which exists to introduce hackers to radical ideas. You'll make mistakes, we all do, and we learn from them instead of letting them inevitably paralyze us with fear. This zine is how a lot of us got involved, off our asses, and into

EDITORIAL

the streets (and often got arrested because nobody clued us in on what to do!). We want to connect the two worlds that hackers live in so we can build strong bonds for strong movements. We want to connect each other, support our prisoners, and give you something you can take away.

We want you to get this zine out there which is why it's anti-copyright. Print it out, scam copies, and get this into people's hands whether they're radicals, hackers, or just everyday folks who are looking for something different to get excited about -- something that helps them empower themselves to get out of their boring fucking lives which up until now have been empty. They have been working for money, for status, feeling as if there was a void. Hackers perhaps know this better than many where we work frustrating jobs maintaining servers, keeping websites online, designing websites which have no useful place in society, and keeping up the infrastructure which is used to facilitate capitalist globalization and exploit us all. We control the internet, we control the wire, and through this we control the mechanisms of state control.

Set up a table at your hackerspace, convention, or any other public space and start handing these out. Hand out as many as you can. Talk to everybody and figure out why they like the zine or don't, why they think hacking and social change should forever be isolated. Link to us on your

NEWS

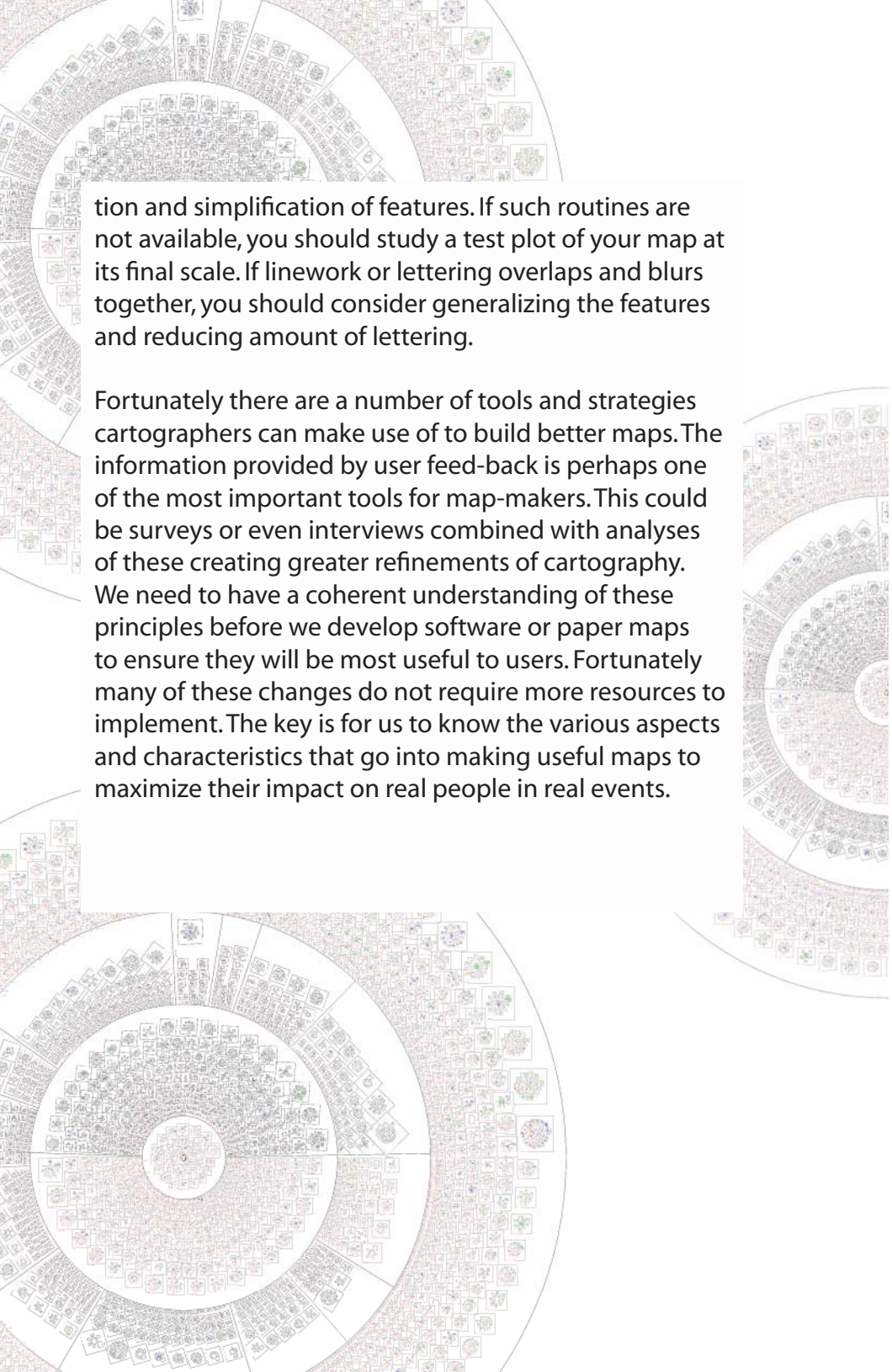
VERIZON*S ASS KICKED BY FCC, MUST PAY YOU MILLIONS

Verizon will refund between $30 and $90 million to customers for "mystery fees" charged to their wireless accounts. If you got a charge for data use on your cell phone bill that you didn't actually incur, you should have gotten a refund in Oct/Nov of this year. If you didn't get your refund, call Verizon and give them a piece of your mind.

http://www.theregister.co.uk/2010/10/04/verizon_payback/

UBEW Chapter Starting in Santa Cruz

A group in Santa Cruz flying under the banner of the "United Brotherhood of Electrical Workers" and "Santa Cruz Hackbloc" has started up. Though the group just started, they have already given workshops on electronic civil disobedience and circuit building. Find out at UBEW.org



tion and simplification of features. If such routines are not available, you should study a test plot of your map at its final scale. If linework or lettering overlaps and blurs together, you should consider generalizing the features and reducing amount of lettering.

Fortunately there are a number of tools and strategies cartographers can make use of to build better maps. The information provided by user feed-back is perhaps one of the most important tools for map-makers. This could be surveys or even interviews combined with analyses of these creating greater refinements of cartography. We need to have a coherent understanding of these principles before we develop software or paper maps to ensure they will be most useful to users. Fortunately many of these changes do not require more resources to implement. The key is for us to know the various aspects and characteristics that go into making useful maps to maximize their impact on real people in real events.

site, tweet us, promote us on your forum or hacker radio show, facebook us, whatever it is you do. If you found one article in here useful or interesting, that's enough reason to let that information be free. Want copies? Get in touch and we'll send you a batch for free (or extremely low cost). We've got thousands of these.

EDITORIAL

We can shut down the surveillance systems, corrupt the databases, hijack information routes, and bust through every firewall we'll ever encounter. As the upper classes continue to rely more and more on the digital realm for everything from basic communication to promotion, we find ourselves abound in opportunities for revolt. Abound in opportunities to explode and inspire others. Abound in opportunities to be something outside of ourselves. Abound in possibilities whose only horizon is our bandwidth and skills which we have honed over years of exploration, hard work, and information sharing.

If you need somebody to tell you what to do, you may as well just die because you clearly have nothing left to live for.

FUCKIN DO IT.

Got feedback? Thoughts? Suggestions? Want to help with distro?
hackthis_ine@lists.hackbloc.org

HACKERS AND THE LAW

June 17, 2010 Colorado Indymedia Asked to Identify Users by FBI

On June 17, Colorado Indymedia was contacted by Special Agent Adam Kowalski of the Federal Bureau of Investigation (FBI)/Department of Homeland Security (DHS). As part of an "ongoing investigation" by Federal Protective Services, they attempted to seize the Colorado Indymedia server, believing that we kept logs (such as IP address access logs) that could identity users on our site. Our servers are graciously hosted at Denver Open Media who was approached by Kowalski. Kowalski claimed he had a court order but refused to leave a copy at Denver Open Media. He was told to contact the system administrators in order to obtain the logs as Denver Open Media does not have the ability to consent to a seizure or search of our property.

As of this date, we do not have a copy of the court order if it even exists. It's likely that this was just a bluff as it's well-established that cops, the FBI, and other law enforcement can lie in order to illicit consent and lying about court orders is no exception.

We told the FBI that "Colorado Indymedia does not retain this [identifying] information because we strongly believe in the First Amendment right to free, anonymous speech. Frequently communities outside of our society's mainstream feel more comfortable expressing their views in an anonymous setting. Like all Independent Media Centers, Colorado Indymedia exists to serve these communities, and thus strives to maintain the anonymity of its users."

In particular, the FBI was looking for information that would

road closures; are there mobile obstacles; and so on. How does the map reflect this is important. Do users have time to comprehend the information being portrayed? Cartographers must try to best predict the real life conditions that could affect the use-ability of a type of map and the data points on it.

** How could maps avoid misinformation?*

Maps are created often in static environments at a particular time. Even dynamic maps have their parameters set to a specific time. How will time and changes be incorporated into a map, by the user or the cartographer or both. If users are expected to add to a map, that must be designed into the map.

** The issues of generalization, simplification, and abstraction*

Cartography is very much a process of abstraction in which features of the real world are generalized or simplified into symbols or key elements to meet the demands of the theme and audience. Not all elements or details have a bearing on the pattern or process being studied and so some need to be eliminated to draw the reader's attention to those facts that are relevant. Too much detail can hide or disguise the message of a map. The amount of detail that can be included is very much dependent on the scale at which the map will be produced, as the following examples demonstrate.

A small-scale map of a larger area must, out of necessity, be more generalized. Some automated systems now have the ability to provide assistance in the generaliza-

be highlighted should be a consideration of any cartographer. It may be useful to show the over all context of the area. Maybe socio-economic considerations are important for the users, maybe they want to do acts of solidarity or refrain from certain acts in certain unfamiliar neighborhoods based on politics, economics, culture or other considerations.

** Another question a careful map maker must ask is: Who will read the map?*

A cartographer must be able to identify the type of reader being addressed for two principal reasons. First, it is important to have an idea about what the audience is likely to know about the subject matter of the map. Second, it is useful to know how much background the readers have in using maps. Locals will need different information than strangers to the area. How comfortable are people with cartographic terms? What measurements if any are most useful to convey distance or scale, i.e. miles, kilometers or blocks?

** What conditions will the map be used in?*

This is an often overlooked consideration in developing maps. It is one thing to look at a map indoors in comfort, security, proper lighting and another outside, on the move, in poor weather, or in the dark. Weather can also effect a map's readability and ability to communicate. How does weather effect the act of moving around in space, does the map adequately reflect this? How about social factors: is public transportation running; are there

identify a user(s) who had used the "spamsucks" account. This account's username and password are posted on the main page of our site for users who would like to post and remain anonymous. Given the time period of the logs they were seeking, we believe they are looking to identify the individual(s) who posted the two communiques that claimed responsibility for the recent attacks on Immigrations and Custom Enforcement (ICE) offices. (See "ICE Facility Attacked in Loveland" http://colorado.indymedia.org/node/7733 and "ICE Office Attacked" http://colorado.indymedia.org/node/7721).

This request is part of an investigation by Federal Protective Services, the agency which is tasked with protecting the security of Federal property (such as buildings). Communiques posted by the same account claiming direct action attacks against other places such as a Wells Fargo branch (http://colorado.indymedia.org/node/7664) have not attracted similar reactions from the agency. It appears as if the ICE attacks prompted additional attention and heat due to their status as Federal buildings even though the attack on the Wells Fargo branch seems related to their funding of private ICE prisons through the GEO Group.

While this may look to many as a run-of-the-mill investigation, there are several things that bring this into question. Firstly, it is a well known and widely publicized policy of Colorado Indymedia that we do not retain logs that can identify individual users. For instance, our privacy policy (http://colorado.indymedia.org/node/550), which is linked to twice from our main page, notes that we do not log such information. The FBI is well aware of this policy but still decided to ask us for logs they know we do not keep. This could be a simple "fill in the box" task that has to be completed, but then why not approach DOM's Internet service provider, which almost certainly does retain logs of this nature (as all major Internet Service Providers and the NSA

do)? Additionally, the FBI seemed intent on seizing our server when they came to Denver Open Media, indicating their goal may have been the disruption of our service instead of simply identifying users.

Given this, it seems likely that the government is upset that we provide a venue for anonymous speech and is retaliating for this. We allow people who ordinarily cannot speak to tell their story to the world including those who took credit for smashing up the ICE offices. In any democratic society, it's important that all members of society can have as much available information in order to make informed decisions, including decisions about whether to support the actions that these communiques discuss. If places like COIMC did not exist, it could be that nobody would have heard why this office was attacked and people would be forced to make evaluations based on coverage from mainstream media outlets who act as a police mouthpiece. In retaliation for providing this service and working to give everybody a voice, we have been targeted.

This targeting is no surprise and something we expect from law enforcement. Police are a tool of those who are in power who use them to maintain that power through force. Behind every law is a charge, behind every badge is a gun, and behind every subpoena is the possibility of being kidnapped and held hostage for contempt. This type of targeting is done every day against those who assert their right to privacy, who do not have societal privilege, who lack the money to defend themselves in court or conform to society's norms, and who choose to defy and change those norms themselves or challenge the power structures that control society. We are not treated differently than anybody else and the targeting of Colorado Indymedia is

play a role in effective cartography, but it is the issue of communication that holds the central role in cartographic design. To ask "what is a good map?" is to ask how well it communicates with its intended audience. This means that one always begins a project by considering the message to be conveyed and the audience to be addressed. This raises a series of questions that must be addressed at the start of a project.

** The first is: What is the intent or goal of the map?*
In effect, the question asks what the reader should gain from the map or how the reader should respond. Motives vary greatly. Many maps are intended solely to convey accurate information about spatial relationships, others to sway public debate. For protests and disasters maps need a bit of both. A good map must convey spatial information. But this is not as simple as it may seem at first. The spatial information must include where something or somebody is and how best to get there. For example is the map mainly for people on foot, bike, public transportation or automobile types of transportation will not only effect the scale but what points of interest are more important. The political nature is also important.

For example in dynamic maps, how big should the icon for adversary forces be, what color, and what about the icon for friendlies. What are the political goals of the map's users? If it is an animal rights event what points of interest might be most important. How should these

Maps that Matter - Considerations for Successful Cartographic Communication

by the March Hare Communications Collective (march-hare.org)

This article seeks to identify the issues that make a map useful for users. There is a ton of well researched literature looking at the problem of cartographic communications. As radicals we are interested in designing mapping tools (whether paper or digital) that meet the unspoken needs of the users. Better maps create better opportunities for individuals to make decisions and explore the feasibility of various tactics. Mapping software (e.g. Ushahidi) or the paper maps copies that are made available at every mobilization or mass event have paid little attention to cartographic communication and available resources have often been used as-is. Here we seek to explore some basic ideas from the academic field of Cartographic Communication to allow radical map-makers to generate maps that matter. If cartography is a form of communication of a specific type of information, the measure of a good map is how well it conveys it to readers to enlighten, convince, or persuade.

Too often the pure aesthetic appeal of a map is equated with its informational value. Aesthetic issues certainly

business as usual. If the Department of Justice had their way (based on their actions and lobbying efforts), the right to anonymous speech would completely disappear. The services that we provide are a critical part of fostering social change and democratic discourse in this region. For this reason and many others we will not be intimidated into maintaining investigative records on our own users or shutting down our service. As far as we know, we are the only media outlet that has provided coverage on the attacks against ICE offices.

It's important when things like this happen we not internalize this repression and that we let people know we are being bullied. The majority of a bully's power is derived from their ability to keep their victim's silent. This is true whether those bullies are police, rapists, the bully who steals your lunch money, or an abusive parent. This enforced silence keeps the victim feeling powerless and alone. When we are silent, we cannot find others who have faced the same treatment and speak out about it or fight back. Police are a tool of those in power which they use to enforce their rules, laws, social codes, and ultimately maintain their place at the top of the hierarchy. They do not want to hear about people challenging their authority. Most of all, they want to make sure that nobody sees or hears about those actions and chooses to support those individuals or becomes inspired to challenge authority on their own.

You may view our privacy policy at http://colorado.indymedia.org/node/550 which contractually binds us to protect your information. We would like to thank Denver Open Media (http://denveropenmedia.org) for continuing to host our server and recognizing the importance of the service we provide. We continue to look for people who are

willing to help with website/server administration, moderation, legal problems, and other things. Please see http://colorado.indymedia.org/node/13 for more information. The original letter from the FBI can be found below including our response (with minor formatting changes for your viewing pleasure).

More information and original correspondence at http://colorado.indymedia.org/node/7781

July 30, 2010

Jacob Appelbaum of Wikileaks Detained By FBI, Equipment Seized

Jacob Appelbaum who works at the Tor Project and volunteers for Wikileaks was detained by federal officials upon re-entering the United States.

His phone was stolen by border guards and he was detained for over three hours. Unlike some not-so-smart students at MIT, who talked to the feds, Jacob refused to answer any questions. Like many of us, Jake appears to understand that there is a line in the sand and that the government is not our friend.

As hackers, we have to stop tolerating people who speak to federal authorities and help in their persecution of hackers and organizations like Wikileaks. They should be expelled from our events, mailing lists, and community.

as well. When fusion center bulletins are leaked, we get a glimpse at the depth of the results these fusion centers produce.

We need our own fusion centers and hacktivists are the best suited to make these happen. We need ways to share intelligence among regions, among people locally, and among our comrades in far away lands. In the age of Wikileaks, we need analysts pouring through leaked documents and notifying people and organizations who came up in them. With a strong combination of encryption, common-sense, offline communication systems, intelligence gathering, analysis and dissemination we can make it work.

So... hacktivists, get to it!

information used to keep citizens in line. They poured millions (if not billions) into a new system for sharing information known as the fusion center.

Fusion centers are a fairly basic concept. In essence, multiple law enforcement agencies, private interests, and emergency management agencies get together and share most all the information they have. Patterns in the data begin to emerge as fusion center analysts look at the intelligence gathered by all of these parties. The information is then turned into targeted analysis and sent to the parties who it's most interesting to. Information sharing between government agencies and corporations has always existed, but the level to which it has become formalized and distributed is something new.

While fusion centers are a huge infringement on civil liberties, are often outside the reach of measures usually used to reign in naughty police departments, and are a huge expense for taxpayers in general, they are reaching their goals. Coordination among law enforcement has increased to a level probably never imagined by those who came up with this idea and at the same time the corporations can get in on the fun

The FBI and the rest of the federal government is bringing down heat strong on the hacker movement due to the recent actions of Wikileaks. We must not budge, we must not talk, and we must let people know when we are targeted or harassed. Their greatest power is that of keeping us silent.

August 20, 2010
Perfect-Privacy.com Raided

The house of an administrator at Perfect-Privacy, a proxy/VPN service based in Germany was raided. According to the site:

"Today, Friday, August 20, 2010, between 7:00 and 8:00 a.m. CEST, the premises of one of Perfect Privacy's administrators were searched by the authorities. The administrator is listed as the contact person for Perfect Privacy's servers in Erfurt, Germany. The house search warrant is based on the suspicion that unknown suspects had routed illegal communications over the privacy servers in Erfurt. "

Services have been temporarily shut down so people with higher security needs are made aware of the raid. The hard drives with data pertaining to the services they offer were encrypted. It is also interesting to note that Perfect Privacy runs a Tor (link to https://www.torproject.org) Entry Guard Node as a public service.

See https://blog.perfect-privacy.com/2010/08/20/perfect-privacy-staff-member-gets-house-search/ for their blog post and official statement

August 2010

Julian Assange Charged with Rape Under Mysterious Circumstances

On August 20, 2010, Julian Assange, co-founder of Wikileaks, was charged with rape and molestation by the Swedish police. A warrant was issued for his arrest then strangely withdrawn two days later by a higher-up who said that there was "no evidence" that would arrange such a warrant. Normally in cases of such charges and warrants like this one, the suspect is not notified and neither is the media. Instead of following normal procedure, the prosecutor talked to the media immediately and is now being investigated for this activity. Fabricating charges is a common tactic of neutralizing (either through imprisonment or character assassination) political targets and this incident speaks to what kind of tricks we can expect to be played against Assange.

October 20, 2010

Court Finally Strikes Down Teen Internet Ban

A California appeals court has struck down as unconstitutional probation conditions that barred a 15-year-old convicted of possessing a stolen motorcycle from using a computer or the internet for any purpose other than school-related assignments.
Last week's decision from California's Court of Appeal for the Fourth Appellate District came in the case of a defendant identified only as J.J., who was convicted of receiving

would try and fill that same gap. Unfortunately, we are no longer on the bleeding edge in the world of technology or intelligence. Like many of the ways we operate as a movement, our intelligence apparatus hasn't been updated in the last several decades. Intelligence is still distributed in the same ways it was during the 60's. While the channels of communications may have changed (we now use blogs instead of underground newspapers) the way we collect, analyze, and disseminate intelligence remains the same.

The Bush administration made this exact same realization almost a decade ago. They realized that their intelligence apparatus was more than out-dated, that agencies couldn't communicate with each other effectively, and that this was especially true for domestic threats. As regular people jumped on myspace, shared information using sites like digg, and the internet's growth expanded by a factor almost too high to measure, state, local, and national law enforcement were using the same tired old techniques to gather

with them. Additionally, one needs to share the intelligence they have in case they leave or die suddenly. This intelligence needs to be distributed and passed onto newer members of the movement.

The CIA, the foreign intelligence agency for the United States Government, is often criticized by ex-agents for losing focus on human intelligence. Even with the spectacular advances in technology, thousand-fold increases in processing power and storage space, and new ways of storing relational data there's simply no replacement for the human mind. With all the wire-tapping, speech-to-text translation, and traffic analysis they can do there's no replacement for a person on the ground with specialized knowledge that is cultivated for a long period of time. While technology is sexy and often comes with promises of replacing us, intelligence is one place where we can't be completely replaced yet in the same way that we still need people to hold down jobs that robots can't. As long as the adversaries we fight are humans, we need humans analyzing the situation and coming up with useful information.

When the Indymedia system was first developed, there was no open publishing system out there. We were on the bleeding edge of technology, writing something that didn't exist before and taking our adversaries by surprise. Indymedia was a key part of the defeat of the WTO in 1999 and later, texting solutions

a stolen Honda 50cc off-road motorcycle. In addition to being required to complete a drug treatment program, the 15-year-old was ordered to delete any existing MySpace or Facebook pages, prohibited from using any instant messaging program and barred from using a computer for any purpose other than school-related assignment.

See http://www.theregister.co.uk/2010/10/20/facebook_limitations_unconstitutional/
http://tinyurl.com/2uvgvab

Canadian Teen Faces Serious Time for Revealing Security Flaws in School Grading System

"A 15-year-old who allegedly broke into a school board website before exposing the passwords of 27,000 fellow schoolchildren has been charged with computer hacking offences. The unnamed Ontario youngster from the Thames Valley area had earlier claimed that he had only carried out the hack to expose the board's weak security.

He said he had purposely chosen to break into the student portal, where marks and timetables were revealed but no changes could be made.

The teen faces four charges, including using a password to commit a computer offence and fraudulently obtaining computing services. Assuming the case proceeds, the youngster is likely to face trial in a juvenile court. "

Original article at http://www.theregister.co.uk/2010/11/02/teen_hack_suspect_charged/

Palin Email Hacker Gets 366 Days In Jail

"David Kernell smiled as the sentence was delivered in US District Court in Knoxville, according to news reports. He faced a maximum of 20 years in custody, and federal prosecutors had been seeking 18 months imprisonment. Defense attorneys had asked for probation with no time served in prison. He was also sentenced to three years of probation.

In April, Kernell was found guilty of one misdemeanor count of computer intrusion and a felony count of obstruction of justice. A jury acquitted him of a separate charge of wire fraud and deadlocked on a fourth charge for identity theft."

As many may remember, in 2008 Kernell guessed the password to Palin's private email account which she was using to conduct public business and hide those conversations from the public. The data was later hosted on Wikileaks after a successful takedown request. His house was raided by federal authorities during a house party.

More at http://www.theregister.co.uk/2010/11/12/palin_email_hacker_sentenced/

Matthew Crippen Faces Three Years for Allegedly Selling Modded XBoxes

Hacker Mathhew Crippen was charged with violating the DMCA in 2009 by modifying xboxes and selling them. After attempting to exclude his witnesses from testifying and obtaining evidence in violation of wiretap laws, the prosecution has now successfully removed his fair use defense. He faces a maximum of three years in prison for allegedly tinkering with these XBoxes.

every march, action, or mass demonstration. Without the correct intelligence, we cannot make educated decisions about the present or the future. This dooms us to repeat the mistakes of the past.

A common problem in social movements, particularly those in the United States, is the issue of memory permanence. Most people are not involved in the movement for more than 10 years and by 20 very few remain. Some of this is due to burn-out, being overburdened by repression, or internal drama which drives people away from each other and breaks bonds of solidarity. When these people leave, their memory leaves with them. All the knowledge they had about the local police department, its internal politics, how it conducted investigations and their strategies for repressing local action is gone. So is their knowledge of important faces, local history, who cause drama in our circles, and the tricks they play. Retaining intelligence (a larger executive-level view of the situation and adversary) and knowledge (specific facts and information) is more than a personal responsibility. It's not simply enough to learn your adversary on your own while swearing you'll always be as active as you are now. If you're an active member of the movement, you need to forge connections with those who are about to leave or have left for a number of reasons one of them being to make sure the intelligence they gathered isn't lost

Thoughts on Intelligence

by anonymous

Intelligence is a key part to social struggle. Intelligence tells us who our adversaries are, how they operate, and ultimately give us the ability to predict their actions. Intelligence (combined with security culture and effective organizing) allows us to smoke out informants and keep our movements safe from basic attacks. Intelligence is what makes or breaks

Oliver Drage Jailed for Not Handing Over Encryption Password

Under UK anti-terrorism laws, anybody can be jailed for refusing to hand over encryption passwords. Oliver has now become the third person to be jail for wisely refusing to hand over his encryption password. Det Sgt Neil Fowler, of Lancashire Police, said: "Drage was previously of good character so the immediate custodial sentence handed down by the judge in this case shows just how seriously the courts take this kind of offence." In other words, even the cops think he's a "good kid" but sent him to jail anyways. Police have still been unable to crack the password.

Court Order Shuts Down Limewire, Limewire Threatens Break-Away Project

A court ordered Limewire (due to an RIAA lawsuit) to cease distributing their software at which point the following notice appeared on their site:

"LimeWire is under a court order dated October 26, 2010 to stop distributing the LimeWire software. A copy of the injunction can be found here. LimeWire LLC, its directors and officers, are taking all steps to comply with the injunction. "

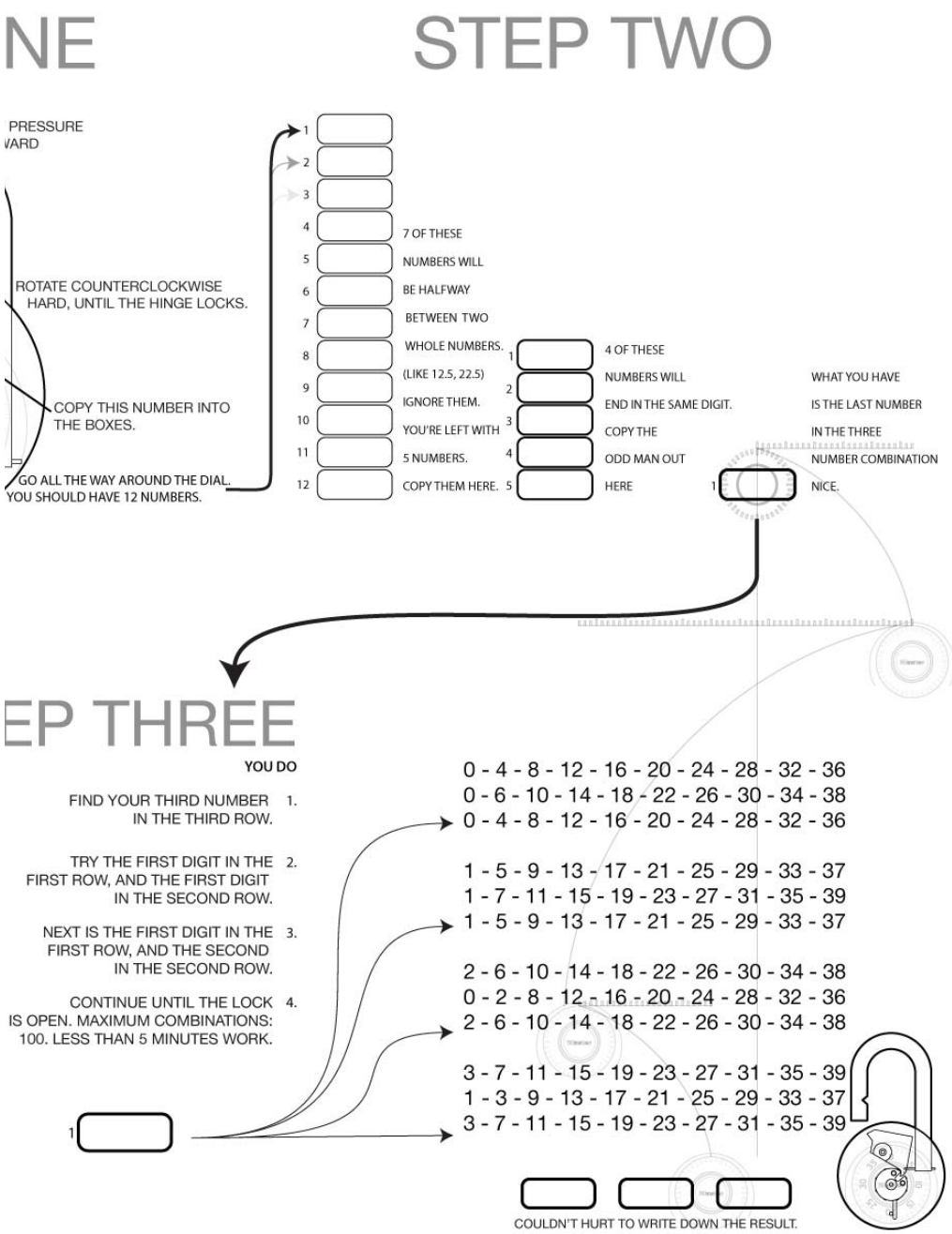
This is not the end of file-sharing, just the end of this particular program. As LimeWire was always open source software, crapware-free versions such as Frostwire have existed for some time. An un-official version called Limewire Pirate Edi-

tion was quickly resurrected only to have limewire turn on file-sharers and threaten them with a cease-and-desist for using their trademarked name. Like any company, they turned to save their asses and put their pocketbooks before their principles. Shame.

Bradley Manning Support Network Volunteer Fucked With at Border

David Maurice House was detained by US Customs Agents at the Chicago Airport (O'Hare). He was questioned for 90 minutes, had his property extensively searched, and had all of his digital devices confiscated. He refused to hand over his encryption keys. In the past few months, we've seen hackers getting detained at the border a lot. If this happens to you, remember that loose lips sink ships. Don't say anything, don't consent to search, don't sign anything, and demand to speak with an attorney. Don't give those fuckers an inch.

Official statement at http://www.bradleymanning.org/13410/bradley-manning-support-network-condemns-unjust-detainment-of-activist/ http://tinyurl.com/2v9cjec



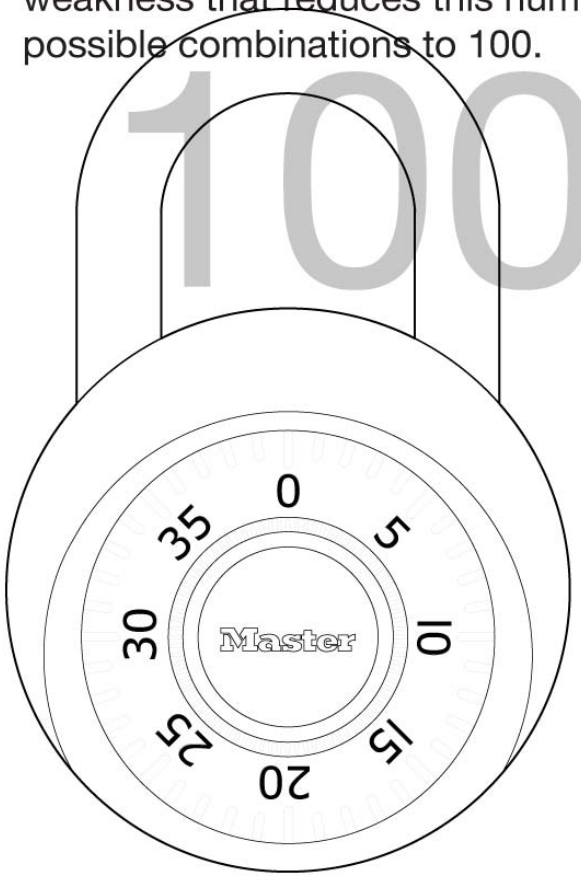
64,000

There are 64,000 perceived possible combinations to open a padlock. At first glance that's just more than 1 week of 24/7 manual attempts.

1 WEEK

There exists, though, a simple mechanical weakness that reduces this number of possible combinations to 100.

100



STEP O

STI

HERE'S AN EXAMPLE

1. LET'S SAY MY NUMBER'S 4. I'M IN THE FIRST SET OF NUMBERS
2. I'LL TRY 0 AS THE FIRST NUMBER, 0 AS THE SECOND NUMBER, THEN 4, THE NUMBER I KNOW.
3. MY NEXT NUMBER WOULD BE 0, THEN 6, THEN 4.
4. I CONTINUE TO 0, 10, 4. THEN 0, 14, 4. MAXIMUM AMOUNT OF TIME: ABOUT 5 MINUTES.

Programmer Faces Federal Investigation for Refusing TSA Full-body scan

John Tyner, a software programmer now faces a federal investigation after refusing a TSA full body scan. Here are a few snippets from his blog.

"I looked him straight in the eye and said, "if you touch my junk, I'll have you arrested.", "I stated that I would not allow myself to be subject to a molestation as a condition of getting on my flight. The supervisor informed me that it was a standard administrative security check and that they were authorized to do it. I repeated that I felt what they were doing was a sexual assault, and that if they were anyone but the government, the act would be illegal."

"At this point, I thought it was all over. I began to make my way to the stairs to exit the airport, when I was approached by another man in slacks and a sport coat. He was accompanied by the officer that had escorted me to the ticketing area and Mr. Silva. He informed me that I could not leave the airport. He said that once I start the screening in the secure area, I could not leave until it was completed. Having left the area, he stated, I would be subject to a civil suit and a $10,000 fine. "

His full blog post and description of the experience is available at http://johnnyedge.blogspot.com/2010/11/these-events-took-place-roughly-between.html http://tinyurl.com/2e47738. There is also a video posted there of the incident.

Hacker Moxie Marlinspike Detained at US Border

Moxie, who many of you may know as the security researcher behind SSLStrip among other projects, was detained at the US Border, searched, interrogated, and had his laptop seized.

“Some dude shows up with a picture of me on his cellphone,” Marlinspike said. “He’s going around looking at everyone and finally he finds me asleep with drool coming down my chin and he wakes me up.”, “The agent did not search his electronics, but after completing his questions told Marlinspike, “Now I have to call Washington.”” “Marlinspike says the forensic investigator told him at one point that he wouldn’t get his devices back unless he disclosed his passwords. His list of contacts and phone numbers weren’t secured, he says, but other data on his laptop and phones was encrypted.

A Firefox Extension That Blocks Advertiser Tracking

BeefTaco is a Firefox extension that automatically adds “opt-out” cookies for over 100 different online advertising networks. Many online advertising networks, such as Doubleclick, allow users to “opt out” of their online tracking by adding a cookie to their browser saying they don’t want to be tracked. The problem is that if you’re privacy conscious, you probably clear your private data on a regular basis including those cookies. This extension automatically re-adds those cookies while your browsing.

This extension hasn’t been tested for inter-operability among other privacy tools such as TorButton but can be another tool in one’s toolbox. It’s important to remember that customizing your browsing experience by blocking ads and installing certain extensions can differentiate you from other users and actually decrease your privacy depending on who you’re hiding from.

Check it out at https://addons.mozilla.org/en-US/firefox/addon/180650/ or tinyurl.com/beeftaco7

New Tool Released for Instant Easy Sidejacking Attacks

A new tool released on the weekend of Oct 22, 2010 allows pretty much any person to do sidejacking attacks against others on their local area network whether it be wired or wireless. Firesheep is a firefox extension that listens to network traffic and picks out account information for popular sites such as Facebook, Google, and Twitter. Simply click on the picture and you're logged into the vulnerable website as that user.

Picture taken from http://codebutler.com/firesheep

This tool could be used for lots of cool things, we'll leave that up to you. To prevent attacks like this, make sure your connection to the sites you visit is encrypted. A handy add-on for Firefox called HTTPS Everywhere can help you with this see https://www.eff.org/https-everywhere

"At first he was like, 'You have a choice you can give me your password and we can just do this all here, or we can send them to the lab and you're not going to have the equipment anyway and we're going to get all the data,'" Marlinspike said. "I said, 'It's encrypted and you're not going to get anything off of it.'""

Moxie (wisely) did not speculate to the media as to why he was detained. Remember kids: always encrypt your drives and get a good picture of what's in your devices in case they get tampered with! Never consent to a search!

Wired has a good article on this (where the quotes are from) at http://www.wired.com/threatlevel/2010/11/hacker-border-search/ http://tinyurl.com/25u5973

Solidarity Moxie!

OPERATION PAYBACK

Before I get into this report, I would like to note that almost all the information here was synthesized from mainstream media accounts of the situation. Some accounts from Anonymous and independent media sources were also used. In this cyber-attack, much like others, it is hard to get a scientific account of what happened and when after the fact. Therefore everything in this article, like every other article in this zine, should be taken with a grain of salt and a skeptic slant. Many in Anonymous have some things to work on in terms of their sexist and racist language, which people should keep in mind when reading this.

During September and October, Anonymous launched yet another successful attack on their enemies during "Operation Payback". Anonymous has become well known both inside and outside of hacker circles for launching spectacular short and long-term attacks against those who threaten freedom on the internet. Previous targets have included the Australian Government and members of their respective political parties for attempting to install a web filter for the entire country and the Government of Iran for repressing the "Green

Apple has proved again that security through obscurity doesn"t work.

They embedded a quick trick to unlock an iPhone when you lose your password. Hit "emergency call", dial ###, hit the call button, and then immediately hit the unlock button. Apple has released a patch for this but like many patches, a good portion of people won't install it. Now anybody who wants to can access an untold number of iPhones (or rather, the Phone app which contains contacts etc) which users think are secure.

TOOLS

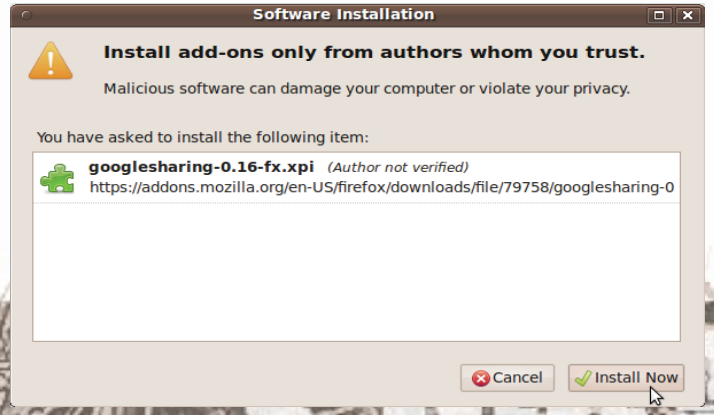
Institute for Disruptive Studies Releases a Google Condom of Sorts

The Institude for Disruptive Studies have released a tool to protect your privacy while you use Google. Riseup networks, the people behind riseup.net have said, “Googlesharing is an easy-to-use, free and open source plugin for firefox that anonymizes your google searches. When you do a google search, google collects information about your identity by recording the web address where you are searching from and the content of your searches. Google probably knows more about your web searches than you do!

Googlesharing works by sending all of your google-related traffic that does not require a login (i.e. not gmail) through a separate server, completely transparently (you don’t have to do anything). As a result, your online activity is aggregated with everyone else’s.”

Riseup, a radical online service provider known for their commitment to privacy currently run a Googlesharing proxy.

More info at http://www.googlesharing.net/ and https://we.riseup.net/riseuphelp/googlesharing.



OPERATION PAYBACK

Revolution” protests and censoring internet access to their citizens.

It all started September 17th, when Anonymous downed the website of Aiplex, an anti-piracy firm which had said publicly they engage in DDoSing torrent sites that don’t bow down to their demands. Later during the weekend of September 20, 2010 Anonymous took down the websites of the RIAA and MPAA. The primary tool of choice for Anonymous has been the

LOIC (low orbit ion cannon) which is a DDoS tool that enabled untold numbers of users to easily attack their targets[1]. While the tool is made for Windows, it can also be run in Linux using mono which supports .net. The tool works by flooding the target with HTTP and TCP requests, knocking offline all web services running on the server and making it difficult if not impossible for the administrator to login remotely. In LOIC (low orbit ion cannon) which is a DDoS tool that enabled untold numbers of users to easily attack their targets[1]. While the tool is made for Windows, it can also be run in Linux using mono which supports .net. The tool works by flooding the target with HTTP and TCP requests, knocking offline all web services running on the server and making it difficult if not impossible for the administrator to login remotely. In the past, some closed source tools have circulated in the circles of Anonymous that have actually been trojaned so it’s important to note that LOIC is open source. The communique for the initial attack is posted below:

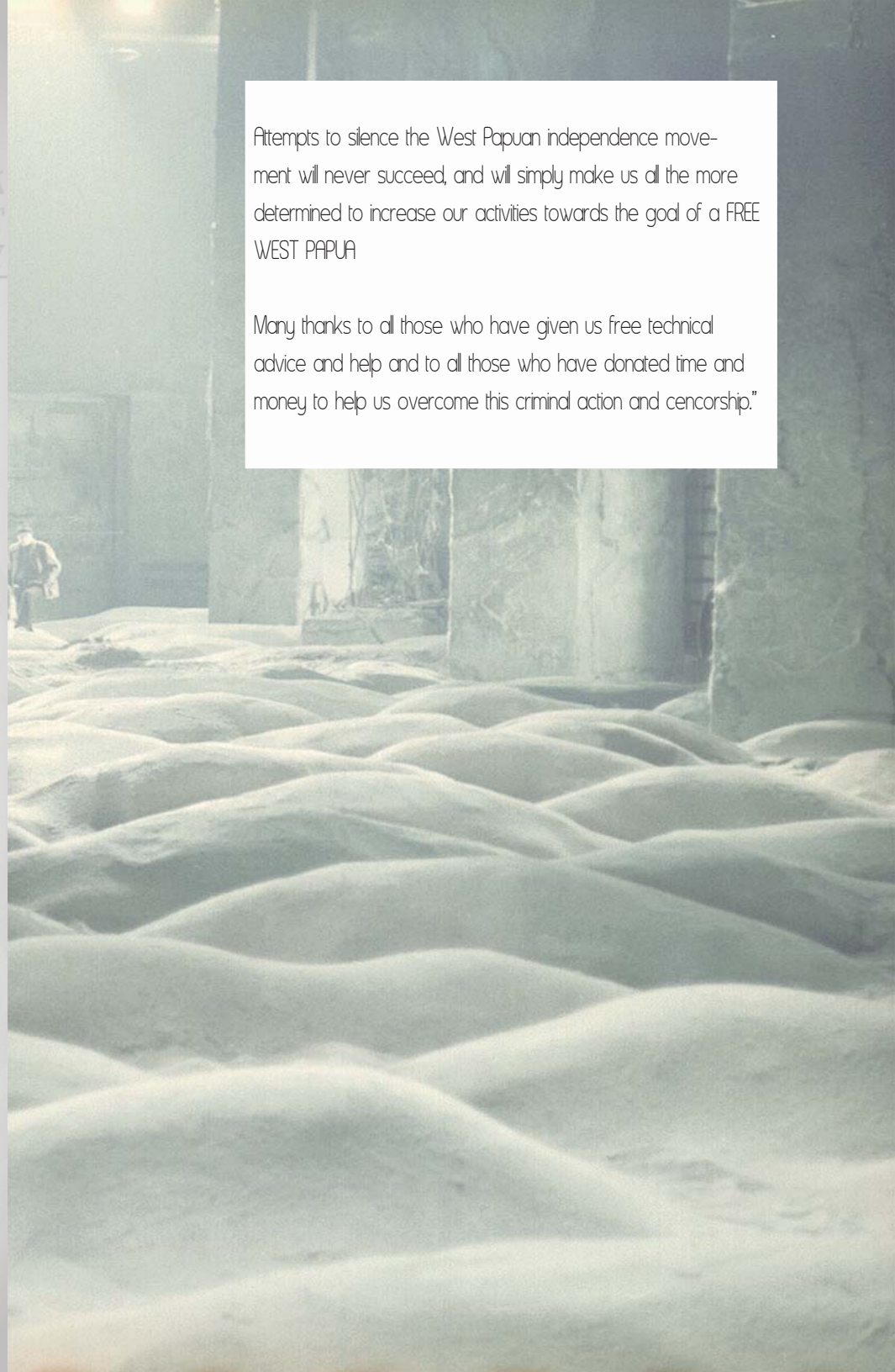
OPERATION PAYBACK IS A BITCH

DATE \SEPTEMBER 19, 2010\

TO WHOM IT MAY CONCERN,

THIS IS TO INFORM YOU THAT WE, ANONYMOUS, ARE ORGANIZING AN OPERATION CALLED "PAYBACK IS A BITCH". ANONYMOUS WILL BE ATTACKING THE RIAA (RECORDING INDUSTRY ASSOCIATION OF AMERICA), THE MPAA (MOTION PICTURES ASSOCIATION OF AMERICA), AND THEIR HIRED GUN AIPLEX FOR ATTACKS AGAINST THE POPULAR TORRENT AND FILE SHARING SITE, THE PIRATEBAY (WWW.THEPIRATEBAY.ORG). WE WILL PREVENT USERS TO ACCESS SAID ENEMY SITES AND WE WILL KEEP THEM DOWN FOR AS LONG AS WE CAN. BUT WHY, YOU ASK? ANONYMOUS IS TIRED OF CORPORATE INTERESTS CONTROLLING THE INTERNET AND SILENCING THE PEOPLE'S RIGHTS TO SPREAD INFORMATION, BUT MORE IMPORTANTLY, THE RIGHT TO SHARE WITH ONE ANOTHER. THE RIAA AND THE MPAA FEIGN TO AID THE ARTISTS AND THEIR CAUSE; YET THEY DO NO SUCH THING. IN THEIR EYES IS NOT HOPE, ONLY DOLLAR SIGNS. ANONYMOUS WILL NOT STAND THIS ANY LONGER. WE WISH YOU THE BEST OF LUCK.

SINCERELY,
ANONYMOUS,
WE ARE LEGION.



Attempts to silence the West Papuan independence movement will never succeed, and will simply make us all the more determined to increase our activities towards the goal of a FREE WEST PAPUA

Many thanks to all those who have given us free technical advice and help and to all those who have donated time and money to help us overcome this criminal action and cencorship."

Tribal Rights Groups Knocked Offline

A group hosting videos of Indonesian soldiers torturing and brutalizing native Papuans was taken offline by a DDoS attack as were several others who hosted the video. Targeted sites include but are not limited to West Papua Unite, Free West Papua, and a number of "human rights charities". Tactics like this coming from government and right-wing groups are becoming more common. From Free West Papua:

"Our Website is temporarily offline due to a DDoS cyber attack by those that want to hide the truth about Village Burnings and Torture in West Papua.

Wel suspect that the DDos cyber attack has been launched by the Indonesian Government and/or its allies.

We are re-enineering out site hope to be back online shortly. In the meantime please visit our official pages at:

Facebook
www.facebook.com/freewestpapua

Twitter
www.twitter.com/freewestpapua

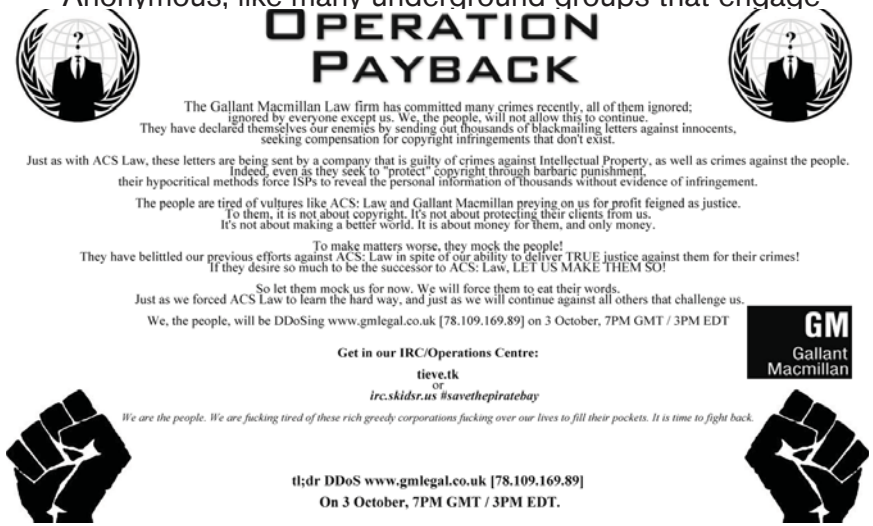
You can also Google "free west papua" or "papua merdeka" for many other news souces about West Papua

The beauty of these attacks is that because there are so many people participating, it is impossible to prosecute them all. Electronic Civil Disobedience has a rich history from its use by the Zapatistas[2] to its use against the World Trade Organization. In a few cases, US prosecutors have picked out one or two people who participated in these attacks and charged them but given the risk vs. reward ratio, participating in an ECD is much safer than going to a large demonstration in real life. As demonstrations are most useful as a form of propaganda, electronic civil disobedience can often be a suitable substitute due to the media coverage it generates.

On September 21st, Anonymous took the websites of ACS:LAW down[3]. ACS:LAW is a law firm in the UK which is in the business of suing and extorting money from alleged file sharers. Like their US counterparts, they rely on scant evidence and scare tactics. Of course, they also catch tons of innocent people in their nets and use illegal tactics to get money from their victims. The DDoS attack was so strong that it ultimately resulted in the death of ACS:LAW. In an attempt to recover their server, the administrator accidentally made their entire server a public directory and leaked every email they had ever sent or received. Not only did the emails contain sensitive business information such as reports showing

they were struggling to keep afloat, they also contained passwords which were likely further exploited by actors in Operation Payback. Like the MediaDefender leak, this leak plunged the company into bankruptcy[4]. Some Internet Service Providers stopped providing them with the IP addresses of alleged file sharers after that information was made public in the leak and these ISPs actually went to court to defend that position. If prosecuted, ACS:LAW could face 500,000 pounds in fines for such careless handling of victim information[5]. Later in the attacks, on October 1st, ACS:LAW was evacuated after bomb threats shut down the building[6].

Anonymous, like many underground groups that engage



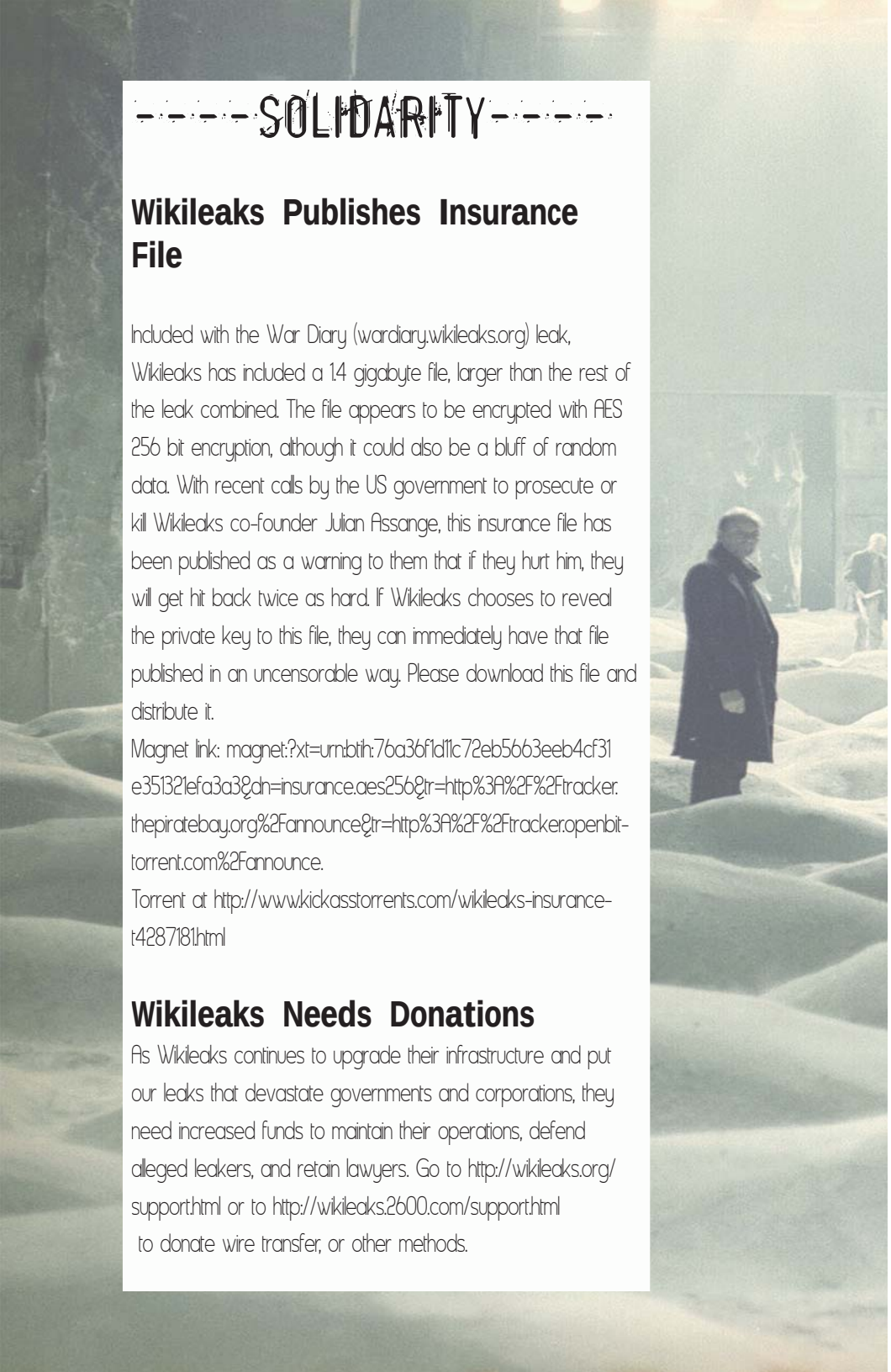
in illegal actions, doesn't have a formal structure or people who can speak for the entire group. Underground groups like this do often have common understandings which detail which action is acceptable and which is not (also called points of unity). They become extremely effective in their attacks by relying on a diversity of tactics: allowing everybody to do their own thing regardless of whether they agree with that particular tactic or not. Instead of having dozens of people maintaining an organizational struc-

New Website Launched for Bradley Manning, Support Needed

A new website, Free Bradley Manning (freebradley.org), has been launched to support alleged whistleblower Bradley Manning who is accused of leaking the Collateral Murder Video (collateralmurder.com), classified US State Department cables, and other information to Wikileaks. Unlike other support sites, this one is built by a group who has experience in prisoner support and suggests doing banner drops and other tactics instead of simply writing letters to congress. Stickers are available for free or a donation. All money donated goes directly to Bradley Manning, who is sitting in solitary confinement in a military prison. INCLUDE BRADLEY.GIF HERE.

As Bradley is in solitary confinement and can't currently receive letters except from people on a pre-approved list, all letters must go through a proxy. Mail postcards and letters of support to:

Bradley Manning, c/o Courage to Resist
484 Lake Park Ave #41
Oakland CA 94610



SOLIDARITY

Wikileaks Publishes Insurance File

Included with the War Diary (wardiary.wikileaks.org) leak, Wikileaks has included a 1.4 gigabyte file, larger than the rest of the leak combined. The file appears to be encrypted with AES 256 bit encryption, although it could also be a bluff of random data. With recent calls by the US government to prosecute or kill Wikileaks co-founder Julian Assange, this insurance file has been published as a warning to them that if they hurt him, they will get hit back twice as hard. If Wikileaks chooses to reveal the private key to this file, they can immediately have that file published in an uncensorable way. Please download this file and distribute it.

Magnet link: magnet:?xt=urn:btih:76a36f1d11c72eb5663eeb4cf31e351321efa3a3&dn=insurance.aes256&tr=http%3A%2F%2Ftracker.thepiratebay.org%2Fannounce&tr=http%3A%2F%2Ftracker.openbittorrent.com%2Fannounce.

Torrent at http://www.kickasstorrents.com/wikileaks-insurance-t4287181.html

Wikileaks Needs Donations

As Wikileaks continues to upgrade their infrastructure and put our leaks that devastate governments and corporations, they need increased funds to maintain their operations, defend alleged leakers, and retain lawyers. Go to http://wikileaks.org/support.html or to http://wikileaks.2600.com/support.html to donate wire transfer, or other methods.

ture and telling others what is and isn't acceptable protest behaviour, they are all instead focused on doing what they do best and coordinating with other sections of the movement based on who they wanted to work with. In this round of attacks, we saw DDoS attacks, defacements, in-real-life protests, black faxes, "mail bombs" (where a person is mailed free promotional materials, ordered pizzas, etc. by the thousands), and even bomb threats against their targets. While there was certainly internal discussion among different factions of Anonymous, this wasn't allowed to divide the group or stifle action.

In the past, the campaigns of Anonymous have been very effective at garnering large numbers to attack specific targets. The only commonality that held together the people doing these attacks together was that they didn't like the target and had some connection through which they could find out about the attacks ahead of time. This means that many of them were users of various imageboards such as 4chan. This time around, anarchist politics began slipping into their announcements and rhetoric.

Throughout the campaign there

Here's a quick timeline of the rest of the attacks with references for those who want to learn more:

- On September 27th, Anonymous took down the website of the Australian Federation Against Copyright Theft, the Aussie counterpart to the MPAA and RIAA. Because the website was not on a dedicated connection, over 8,000 other websites were also taken offline including several websites for parts of the Aussie government.[7]
- On October 3rd, the website of the Gallant Macmillan law firm which was attempting to extort the identities behind a few thousand alleged file sharers was taken offline. This was also conveniently the day before their most important court appearance. [8]
- On October 4th, after attacking Gallant Macmillan law, Anonymous attacked one of their largest clients: The Ministry of Sound.[9]

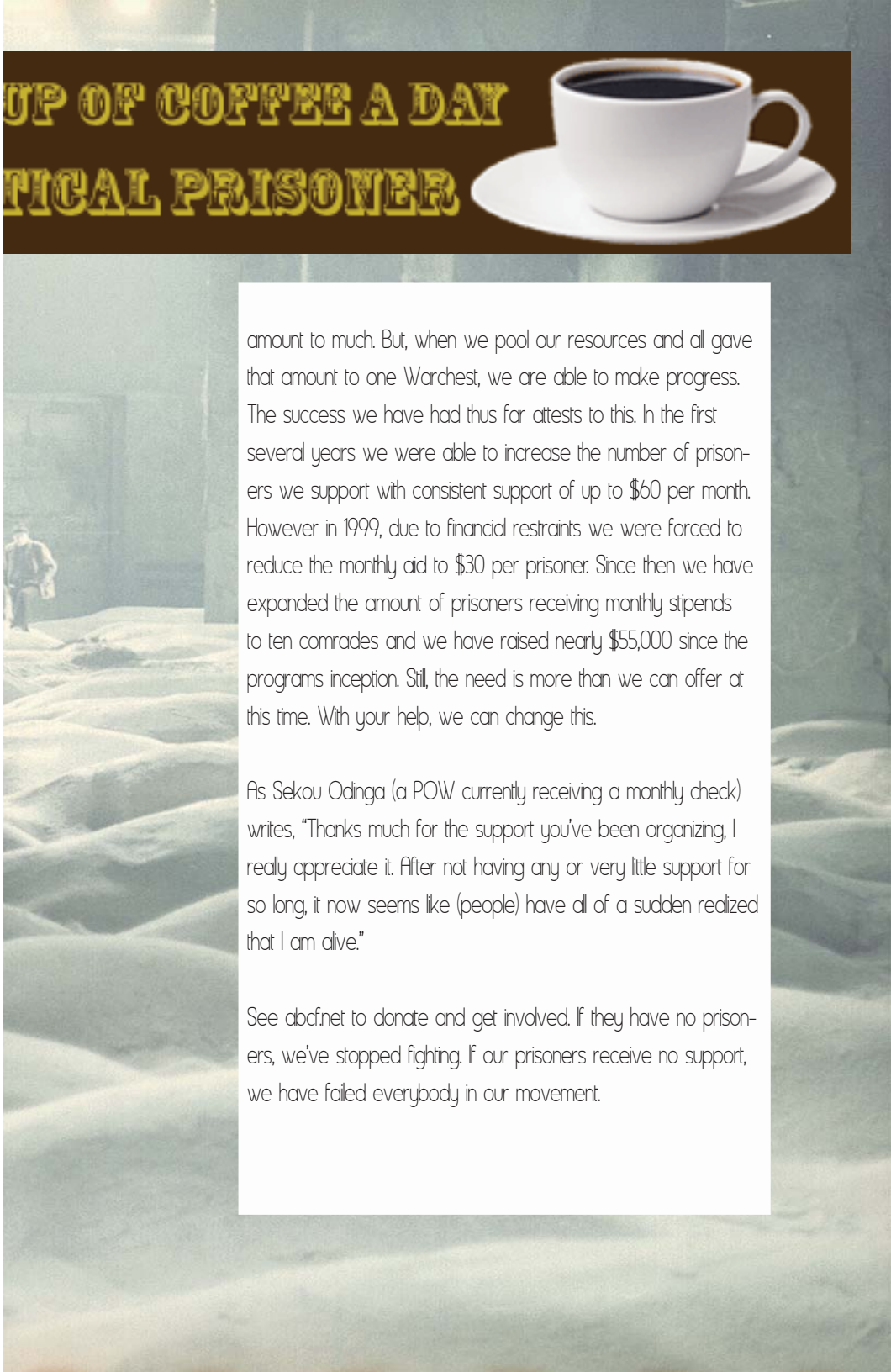
- On October 6th, the website for the Sociedad General de Autores y Editores was knocked offline which is another copyright lobbyist group similar to the RIAA/MPAA in Spain. [10]
- On October 13th, the websites of Gene Simmons (of KISS) were taken down. Gene Simmons has become notorious in the anti-copyright communities for his tirades against piracy such as the one which prompted this attack: "Make sure your brand is protected... Make sure there are no incursions. Be litigious. Sue everybody. Take their homes, their cars. Don't let anybody cross that line."[11]
- On Oct 15th, the website Copyprotected.com was defaced. The site was set up by the MPAA to promote the "benefits" of DRM on blu-ray discs and other media. [12] [13]
- On Oct 16th, the UK Intellectual Property

were interviews with a number of "key people" who helped set up IRC channels and plug new folks in. Here are a few questions which have particularly interesting answers. [18]

Q: Who is Anonymous?
A: I believe it is just a description of what we are. Anonymous is not an organization with hierarchy and leaders. We manifest as Anarchy. We are comprised of people from all walks of life. In short, we feel strongly motivated to do what we can to fight back against things which are morally questionable.

Q: Are you prepared to go to jail for your cause?
A: Yes, but we've taken every measure we can to make sure that our anonymity remains in tact. More importantly, why isn't this question asked to the very people who hired Aiplex to attack us in the first place?

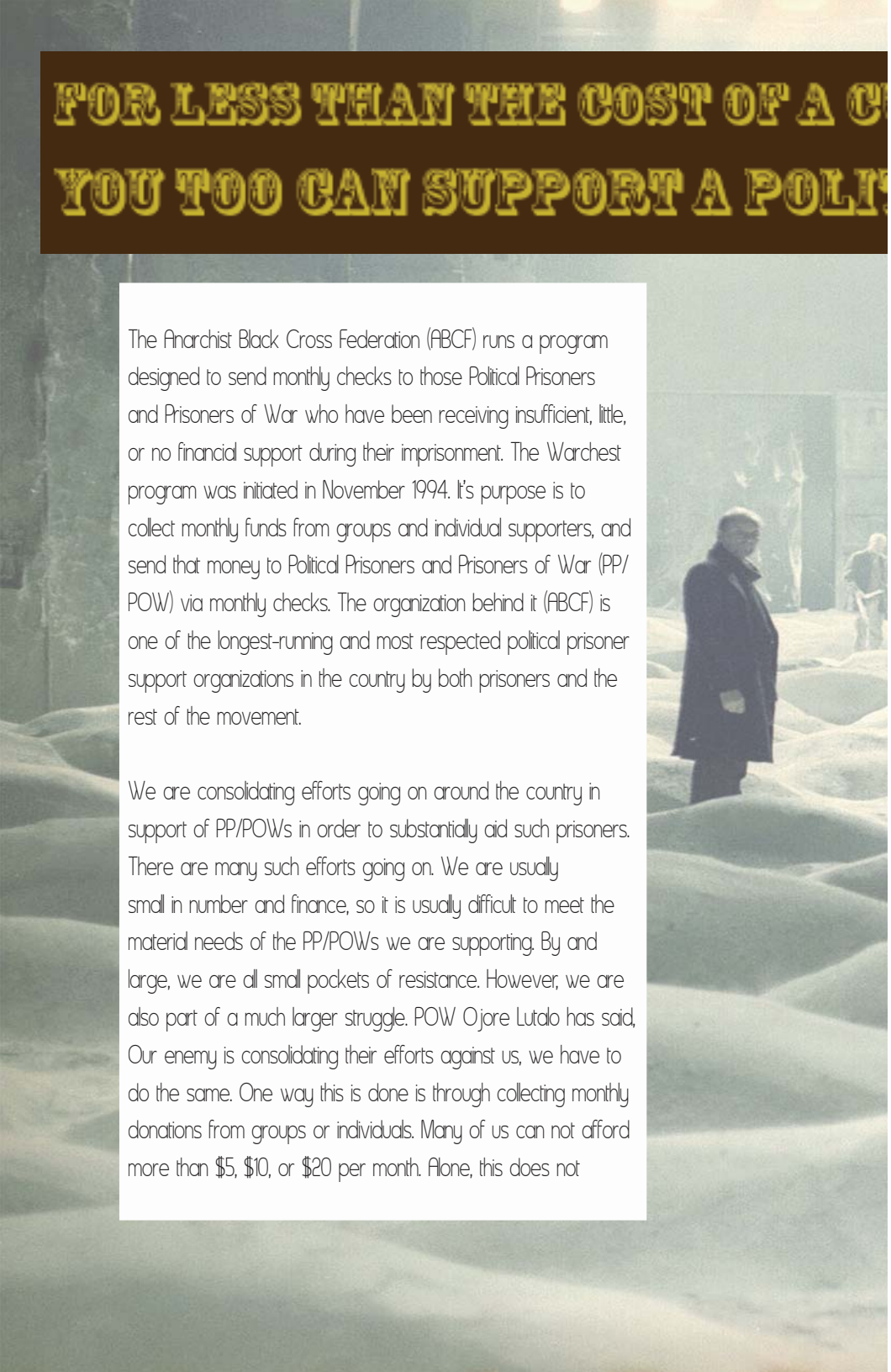
Q: Are you aware that this sort of attack is illegal in many countries and that your group can potentially put innocent people who support your cause under legal scrutiny?
A: I think that most people/participants are aware of that risk. In a



amount to much. But, when we pool our resources and all gave that amount to one Warchest, we are able to make progress. The success we have had thus far attests to this. In the first several years we were able to increase the number of prisoners we support with consistent support of up to $60 per month. However in 1999, due to financial restraints we were forced to reduce the monthly aid to $30 per prisoner. Since then we have expanded the amount of prisoners receiving monthly stipends to ten comrades and we have raised nearly $55,000 since the programs inception. Still, the need is more than we can offer at this time. With your help, we can change this.

As Sekou Odinga (a POW currently receiving a monthly check) writes, "Thanks much for the support you've been organizing, I really appreciate it. After not having any or very little support for so long, it now seems like (people) have all of a sudden realized that I am alive."

See abcf.net to donate and get involved. If they have no prisoners, we've stopped fighting. If our prisoners receive no support, we have failed everybody in our movement.



The Anarchist Black Cross Federation (ABCF) runs a program designed to send monthly checks to those Political Prisoners and Prisoners of War who have been receiving insufficient, little, or no financial support during their imprisonment. The Warchest program was initiated in November 1994. It's purpose is to collect monthly funds from groups and individual supporters, and send that money to Political Prisoners and Prisoners of War (PP/POW) via monthly checks. The organization behind it (ABCF) is one of the longest-running and most respected political prisoner support organizations in the country by both prisoners and the rest of the movement.

We are consolidating efforts going on around the country in support of PP/POWs in order to substantially aid such prisoners. There are many such efforts going on. We are usually small in number and finance, so it is usually difficult to meet the material needs of the PP/POWs we are supporting. By and large, we are all small pockets of resistance. However, we are also part of a much larger struggle. POW Ojore Lutalo has said, Our enemy is consolidating their efforts against us, we have to do the same. One way this is done is through collecting monthly donations from groups or individuals. Many of us can not afford more than $5, $10, or $20 per month. Alone, this does not

world where our voice is ignored we feel we have no choice but to revert to direct action.

Q: Some people view this as the future of protests. Do you foresee future protests like this for other causes in the future?

A: Certainly. As for the protests, I hope the future of protests is ACTION. Not walking in circles with useless signs that are ignored.

Like most campaigns, this campaign by Anonymous had to come to an end. They had sent a powerful message to their targets, successfully shut down a law firm practicing pay-up-or-else copyright extortion, almost shut down a second, gained media coverage that is pretty damn hard to measure, and once again showed that file sharers and internet citizens alike have a militant side to them. As this campaign was mainly an act of propaganda, its purposes had been fulfilled. As people realized this, the campaign fizzled out.

Many news outlets such as Torrentfreak[19] reported that the Pirate Party had written an open letter to Anonymous asking them to stop their campaign and "seek out a legal method to express your frus-

Office website was knocked offline. [14] [15]

- On Oct 17th, the website of Gene Simmons site taken down for the second time. After the first attack, Gene made the following statement which earned him a painful blow by the low orbit ion cannon:

"Some of you may have heard a few popcorn farts re: our sites being threatened by hackers. Our legal team and the FBI have been on the case and we have found a few, shall we say "adventurous" young people, who feel they are above the law. And, as stated in my MIPCOM speech, we will sue their pants off. First, they will be punished. Second, they might find their little butts in jail, right next to someone who's been there for years and is looking for a new girl friend. We will soon be printing their names and pictures. We will find you. You cannot hide."

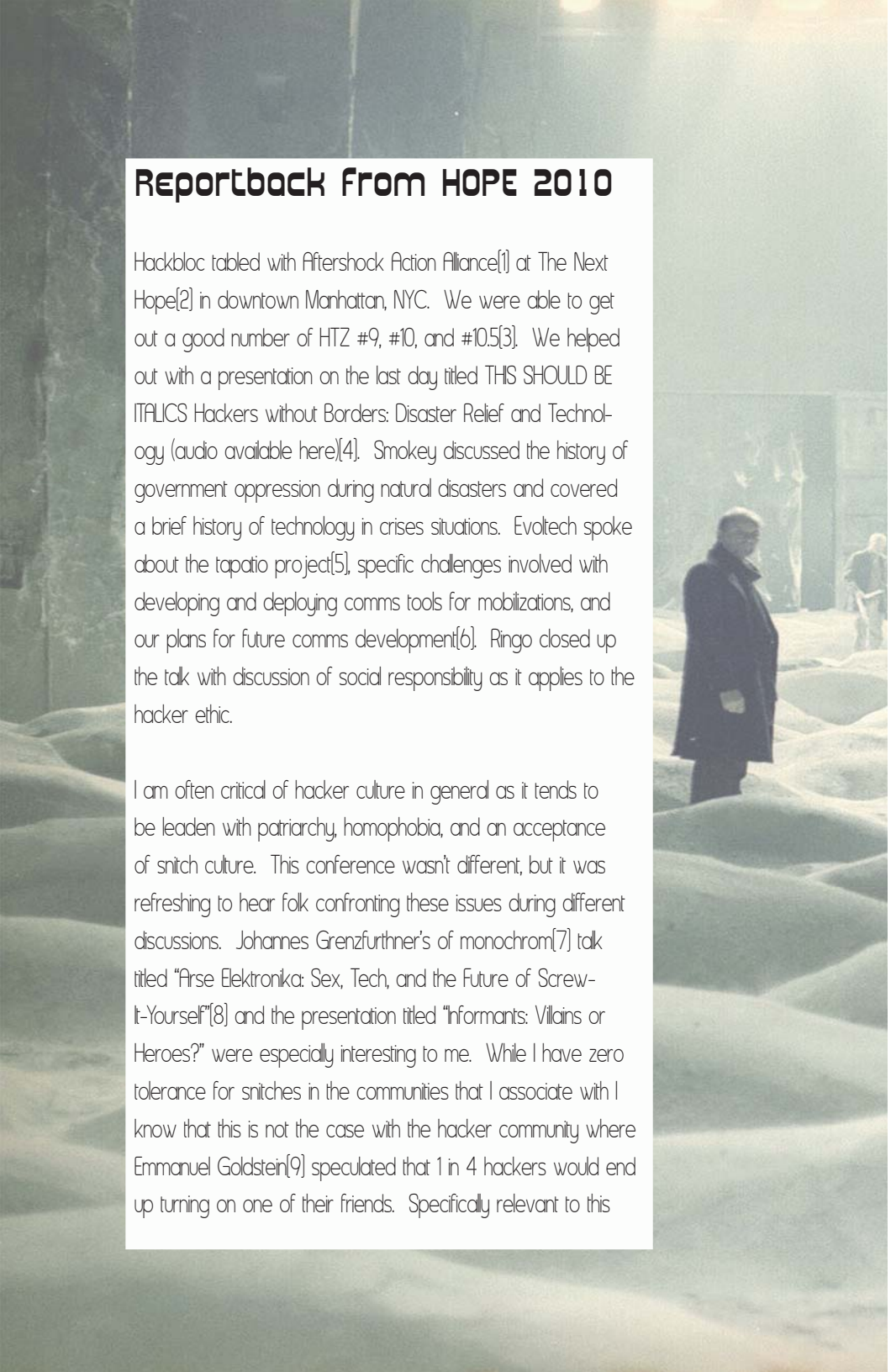
- On Oct 29th, the website of the RIAA was DDoSed again. According to PC Magazine, they were able to take down the site within five to seven minutes.[16]
- On Nov 3rd the website of the US Copyright Office was knocked offline by a DDoS attack.[17]

tration and disquiet with the copyright industry". Political parties and authoritarian groups have a long history of co-opting movements and this is no exception. They again make the argument that legal protest is the only way to make change when most social changes (such as the ones that will be required to get rid of copyright) have happened because movements did not compromise and took the action necessary to see through their goals. The Pirate Party saw their power slipping away as people moved to more direct forms of action and did what they had to in order to maintain it. Political parties and candidates are a way to absorb energy that would otherwise go into action that would directly and efficiently fix the problems society has. It is the court system for social change. If the pirate party had their way, they would be able to control the entire movement and keep actions only to what is legally and socially acceptable to them. Only then, they claim, can real change happen but we know that isn't how it works.
The claim that "Nobody would listen to us if we said piracy should be legal, but when we ask for copyright lifespan to be reduced to 'fair' lengths, that would sound a lot more reasonable." sounds exactly like the logic used by politi-

discussion was the outing of Adrian Lamo[10] as an informant who turned on alleged whistleblower Bradley Manning[11] for the alleged leak of the Collateral Murder video[12]. What I appreciated from the informant talk was that it provided a forum for dialogue about snitch culture and state oppression specifically as it relates to the individual lives of victims in the hacker community where otherwise I think this would have just gone ignored and would not be addressed publicly.

Ironically, we published an article proposing a stop snitching movement as it applies to hackers in issue 9, not knowing how timely and relevant it would quickly become. It was inspiring to hear the clapping and cheers every time we brought up expelling snitches from the movement both in our presentation and the one by Wikileaks.

1. http://aftershockaction.blogspot.com/
2. http://www.thenexthope.org
3. https://hackthiszine.org
4. http://thenexthope.org/schedule/sunday/
5. https://drupal.org/project/tapatio
6. http://www.march-hare.org/
7. http://www.monochrom.at/
8. http://www.monochrom.at/arse-elektronika/
9. https://secure.wikimedia.org/wikipedia/en/wiki/Eric_Corley
10. https://hackbloc.org/node/2123
11. http://www.freebradley.org/
12. http://www.collateralmurder.com/



Reportback from HOPE 2010

Hackbloc tabled with Aftershock Action Alliance[1] at The Next Hope[2] in downtown Manhattan, NYC. We were able to get out a good number of HTZ #9, #10, and #10.5[3]. We helped out with a presentation on the last day titled THIS SHOULD BE ITALICS Hackers without Borders: Disaster Relief and Technology (audio available here)[4]. Smokey discussed the history of government oppression during natural disasters and covered a brief history of technology in crises situations. Evoltech spoke about the tapatio project[5], specific challenges involved with developing and deploying comms tools for mobilizations, and our plans for future comms development[6]. Ringo closed up the talk with discussion of social responsibility as it applies to the hacker ethic.

I am often critical of hacker culture in general as it tends to be leaden with patriarchy, homophobia, and an acceptance of snitch culture. This conference wasn't different, but it was refreshing to hear folk confronting these issues during different discussions. Johannes Grenzfurthner's of monochrom[7] talk titled "Arse Elektronika: Sex, Tech, and the Future of Screw-It-Yourself"[8] and the presentation titled "Informants: Villains or Heroes?" were especially interesting to me. While I have zero tolerance for snitches in the communities that I associate with I know that this is not the case with the hacker community where Emmanuel Goldstein[9] speculated that 1 in 4 hackers would end up turning on one of their friends. Specifically relevant to this

cians during the civil rights movement that blacks and whites could be "separate but equal". As long as we keep walking around with signs, signing petitions, and writing letters, systemic change can never happen. It just doesn't make sense to ask somebody who is given terrifying amounts of money, power, or influence from doing something wrong to stop doing it, nor does it make sense to ask Mr. Burns to implement more safety measures when he disposes of nuclear waste. If you can make enough phone calls to make that person's life unlivable, maybe you might get somewhere but in that case, you might as well just blockade the damn plant. This is the same strategy we need to adapt when dealing with copyright.

Despite the fact that this "letter to Anonymous" came almost a month after the last action during the Operation Payback campaign, many news sites reported that this was the reason the campaign stopped. They claim that a few "leaders" of Anonymous made an agreement with the pirate party and pretty much convinced the rest of Anonymous to stop their attack. Nothing could be farther from the truth or more dangerous to spread as our narrative of what happened. As everybody knows, Anonymous has no leaders and nobody can control them. There is no formal organizational structure through which any agreement like this could ever be reached.

In the future, these types of attacks on Anonymous should be treated as severely as those by Gene Simmons if they wish to remain successful. They are more dangerous as they are not overtly against what Anonymous does nor are they as obvious to the untrained eye. Co-option is as much of a risk as neutralization by other more overt authoritarian forces.
We should not report this version of the story when we look back on this campaign. The intense level of

direct action that occurred during these months is something we should all be proud of. We should be inspired by previous success to build larger actions which bring larger longer-lasting change. We should be proud that there are groups like Anonymous that are willing to put it on the line to defend a free internet and promote creative action and fuck any apologist that says any different. This is our story, not theirs.

"We are Anonymous.

We are legion.
We cannot be stopped.
We do not forgive.
We do not forget.
Expect us."

As to what's the next step, perhaps Anonymous will start planning more long-term campaigns against certain law firms and other enemies who deserve their full wrath. Those within Anonymous will probably take this short respite to figure out what is to be done next and (hopefully) to be a little less sexist, racist, and exclusive.

Only those who comprise Anonymous can decide this and only those who label themselves as Anonymous can decide who comprises it.

Further Research:

Solidarity with all riots, seize the wires!"

"The telegraph is now asking for people to send in e-mails identifying student rioters at Millbank (http://www.telegraph.co.uk/news/picturegalleries/uknews/8125764/Do-you-recognise-these-student-rioters.html). The *Social War Protetection Agency * says 'hella fuck that'. We are asking anyone with free time to send an email, or ten emails, or hundreds of emails, or thousands of emails to ********** with the name of your favorite imaginary persons. Keep homies out of jail. Jam! Jam! Jam!

FORWARD FAR AND WIDE"

1. An interesting account is available at http://news.infoshop.org/article.php?story=20101111052301786

Send an Email Save a Rioter

The Telegraph (a UK publication) published pictures of alleged “rioters” at the demonstration against budget cuts that would cut school funding [1]. They asked the public in help identifying them. In response to this, calls were put up online for mass mailings to the Telegraph with false “identifications” of those in the pictures. Two of those calls are copied below.

“Every day we see media outlets being used to “identify” “rioters” involved in different struggles. The good news is that we can easily defeat this by flooding them with false identifications. Go ahead, send an email to ********** identifying various students whose pictures have been published at http://www.telegraph.co.uk/news/picturegalleries/uknews/8125764/Do-you-recognise-these-student-rioters.html. Be sure to include why you think it’s them (we used to go to school, I remember he loved fire extinguishers etc). Give full and false contact info so you can’t be separated from legitimate reports and for the love of god don’t use your riseup account.

Account of the campaign from closer to the source: http://encyclopediadramatica.com/Operation_Payback http://tinyurl.com/29hu93o
Interesting Article: http://blogs.computerworld.com/16995/collective_power_of_4chan_and_Anonymous_the_future_of_cyber_protests
http://tinyurl.com/35tx2qx
Interesting Article: http://alphavilleherald.com/2010/10/operation-payback-is-a-bitch-hactivism-at-the-dawn-of-copyright-controversies.html
http://tinyurl.com/2fstvqx
Explicitly Above-ground Group of Anons who Plan Protests Against Scientology http://www.whyweprotest.net
http://tinyurl.com/6ef27o
Indymedia for Anonymous - http://www.anonnewswire.org/
http://tinyurl.com/38blpxv
Wiki with lots of information about Anonymous and their previous campaigns: http://tinyurl.com/38blpxv
ACS:LAW
Leak Analysis: http://torrentfreak.com/acslaw-anti-piracy-law-firm-torn-apart-by-leaked-emails-100925/
http://tinyurl.com/25nrgbd

1.http://sourceforge.net/projects/loic/ http://tinyurl.com/y5z6df5
2.http://switch.sjsu.edu/web/v4n2/stefan/ http://tinyurl.com/3666zq2
3.http://torrentfreak.com/new-4chan-ddos-targets-hated-anti-piracy-law-firm-100922/ http://tinyurl.com/29z5sfm
4. http://torrentfreak.com/acslaw-boss-i-feel-defeated-and-could-go-bankrupt-101003/ http://tinyurl.com/2ablzwj
5.http://www.bbc.co.uk/news/technology-11418970 http://tinyurl.com/2deyt24
6.http://torrentfreak.com/anti-piracy-law-firm-evacuated-after-bomb-threat-101001/
http://tinyurl.com/2aqxtge
7.http://torrentfreak.com/ddos-takes-down-aussie-anti-pirates-and-8000-other-sites-100928/ http://tinyurl.com/25nrgbd
8.http://torrentfreak.com/anti-piracy-lawyers-face-ddos-before-pivotal-court-decision-101002/
http://tinyurl.com/2caumlw
9. http://torrentfreak.com/ministry-of-sound-silenced-by-huge-ddos-attack-101004/

http://tinyurl.com/335j7s2
10.http://www.slyck.com/story2076_SGAE_Next_Target_in_Anonymous_DDoS_Attack
http://tinyurl.com/26pus3j
11.http://www.slyck.com/story2085_Anonymous_Strikes_at_KISS_Frontman_Gene_Simmons_With_DDoS_Attack
http://tinyurl.com/39fbl59
12.http://torrentfreak.com/mpaa-copy-protected-drmsite-hacked-by-Anonymous-101015/ http://tinyurl.com/39fbl59
13.http://www.theregister.co.uk/2010/10/15/mpaa_site_dns_hack/
http://tinyurl.com/36q26hd
14.http://torrentfreak.com/Anonymous-takes-out-uks-intellectual-property-office-website-101017/ http://tinyurl.com/2etjpqm
15.http://www.theregister.co.uk/2010/10/18/anon_ipo_ddos/
http://tinyurl.com/34ypx2m
16.http://www.pcmag.com/article2/0,2817,2371784,00.asp http://tinyurl.com/2bo8jt8
17.http://www.slyck.com/news.php?story=2116
http://tinyurl.com/328hndj
18.http://pandalabs.pandasecurity.com/an-interview-with-Anonymous/
http://tinyurl.com/2wwymua
19.http://torrentfreak.com/pirate-parties-use-influence-to-halt-operation-payback-101120/ http://tinyurl.com/2cqoab8

Full Body Scan Images from Courthouse Leaked to the Media

“At the heart of the controversy over “body scanners” is a promise: The images of our naked bodies will never be public. U.S. Marshals in a Florida Federal courthouse saved 35,000 images on their scanner. These are those images.”

See the images and Wired’s coverage at http://www.wired.com/threatlevel/2010/11/giz-scans/

sity under the federal Morrill Act. When that bill was signed by Abraham Lincoln in 1862, education was recognized as a privilege, one that as Americans, we tend to forget. So if you have see nothing, if the crimes committed against us remain unknown to you, then I would suggest that you allow the fifth of November to pass unmarked. But if you see what I see, if you feel as I feel, and if you would seek as I seek then I ask you to stand beside me, and one year from today on lawns of this fine university we shall give the squirrels a fifth of November that shall never be forgot!

And really IT, get with the program and stop wasting exorbitant amounts of money on equipment that periodically freezes and allows unauthorized access. Consider stepping outside your personal areas of comfort and the safe purchases dictated by popular culture. This system which you took months and untold thousands of dollars to implement, I have re-designed in one hour.

Good luck.

ACTION REPORTS

July 23, 2010: European Carbon Trading Website Defaced

Hacktivists defaced the website of the European Climate Exchange, a “cap and trade” program. This greenwashing solution to climate change allows super-rich companies to sell “carbon credits” to other super-rich companies while appearing to care about the environment. The communique on the website read:

“ Heard of this wonderful system of Cap and Trade? Here’s basically how it works:

1. Set an overall limit on pollutant emissions (the cap). Make sure the cap isn’t too ambitious and is susceptible to corporate lobbying.
2. Grant the industries plenty of free licenses to pollute (carbon credits), so they can continue business-as-usual. Biggest polluters get rewarded with most credits.
3. Allow the cap to be raised by additional offset credits and other holes in the system.

4. Pollutant emissions are now made into tradable commodities; A new speculative market is born.
5. Make the whole system as obscure as possible, and assure the general public that the free market will take care of the climate crisis
6. ???
7. Profit!

The Cap and Trade system (as implemented in the EU Emissions Trading Scheme) has a whole range of issues:

* It's main purpose is not to reduce emissions, but to help polluters meet "reduction" targets in the cheapest way possible, in a business-as-usual scenario.
* Leaves room for unverifiable manipulation.
* Generates outrageous profits for big industry polluters, investors in fraudulent offset projects, opportunist traders and new 'marketplaces' such as the European Climate Exchange.
* It distracts attention from the wider, systemic changes and collective political action that needs to be taken to tackle climate change and it's fundamental root causes."

Source: Australia Indymedia http://indymedia.org.au/2010/07/24/european-climate-exchange-website-hacked

in some apparent state of perpetual inebriation. What has transpired in our culture that steadfast pursuit of dignity, purpose, and wisdom has yielded space for squirrels who enter without ambitions and with no outward enthusiasm for the fantastic academic culture that this University might otherwise have.

How did this happen? Who is to blame? Well certainly there are those more responsible than others. But again, truth be told... if you're looking for the guilty, you need only look in a mirror.
I know why you do it. I know you're afraid. Who wouldn't be? Squirrels are ferocious creatures. Weighing in at 5 pounds muscle and 1 ounce fur, these diurnal rodents may multiply 3 fold in the time of one semester. They can survive almost any habitat feeding on seeds, nuts, or the unsuspecting meaty prey. Fear got the best of you and in your panic, you let them into our city, your lawns, and your very lives.

And so I resolve to end this tyranny that has soaked into the very brick that holds our university together. More than one hundred years ago, WSU was founded as a land grant univer-

death or the end of some awful bloody struggle, are celebrated with a nice holiday - I thought we could mark this November the fifth, a day that is sadly no longer remembered, by taking some time out of our daily lives to sit down and have a little chat.

There are of course, those who do not want us to speak. I suspect even now that the phones are ringing at the the information technology office and functionaries -- which is rather ironic terminology given our upcoming topic -- will soon scurry from their lair to suppress our pleasant conversation. Why? Because while the strict social patterns of obedience may be used in lieu of conversation, soft spoken words will always retain their power. Words offer the means to meaning and for those who will listen, the enunciation of truth. And the truth is, that there is something quite troubling with our University, isn't there?

At some level, each one of you knows already of what I speak, or whom, rather. They, with their beady little eyes and mamillian faces, who have come to Pullman merely to eat, drink, and bread. Truly, it is the squirrels that have infiltrated our once astute university, who run rampant and wild through the lawns

The attack was carried out by the pseudonymous tech collective decocidio. They linked to our site and for the sake of being explicit, we would like to say we are not involved with this attack nor do we know anything about it. They also linked to Earth First! among other sites such as their wikipedia entry available via SSL at https://secure.wikimedia.org/wikipedia/en/wiki/Decocidio http://tinyurl.com/3axljqk. Original mirror of the defacement available at http://www.zone-h.org/mirror/id/11201786 http://tinyurl.com/327h7bk.

Decocidio logo

July 25, 2010: Wikileaks Releases the "War Diaries"

The whistleblowing website Wikileaks releases a set of classified documents entitled the "Afghan War Diary". The set encompasses a whopping 91,000 reports. Alleged whistleblower Bradley Manning (see bradleymanning.org) has been named as a "person of interest" in the search for who leaked these documents however he has not been charged with or accused of leaking them. The War Diary details almost every action taken by the US Army in Afghanistan during 2004-2010 from bombings to pulling over cars to investigations. The reports are written by the soldiers involved and reveal (as if it was a surpise) indiscriminate killing of civillians and possible war crimes. This is the most complete picture of a war humankind has ever had during it. The War Diary may be accessed at wardiary.wikileaks.org. Numerous torrents are available for those who want the raw data and don't want to overload Wikileaks servers.

Some of them know what they're talking about. And students, stop being so apathetic. When you hear or see something that troubles you make your opinion known. Do something about it. Don't just sit around and play video games or check your Facebook status.

Previously there was a list of complaints posted on this website. This campaign is not about complaining, but instead promoting responsible student activism and involvement. What was done to the classroom computers was bad, the apathy within the student body is far worse. "
V's facebook gained almost 2,000 friends. The full communique which was read to every student taking classes that day (video on the site)

Good day, WSU. Allow me first to apologize for this interruption. It will be brief such that you may quietly, or otherwise, continue with your various obligations. I do, like many of you, appreciate the comforts of everyday routine, the security of the familiar, the tranquility of repetition. I enjoy them as much as any chap. But in the spirit of commemoration - whereby those important events of the past, usually associated with someone's

V for Vendetta Hacker Hits Washington State University, Calls for Uprising

A hacker wearing a Guy Fawkes mask hijacked school computers and projectors to send a message to the students: get up and do something, let your voice be heard, and give the school a 5th of November to remember next year. The hack, which they say only took one hour, threw the school into a panic as they contacted the police. From the website wsu1812.com: "We, the students of WSU, have grown tired of this university's disregard for the opinion of it's students. While this attitude of disrespect is not common, it seems to be present in some of the highest ranking university officials. It is time the university regarded students as customers, not source of income.

But students, you are just as at fault as anyone. The ASWSU "student government" is a prime culprit in this problem. Really it stems from student apathy. We just don't care.

So, here is your call to action. University officials, it's time to clean up your act. Listen to your students once in a while.

July 30, 2010: Vatican Googlebombed over Weekend

Anonymous hackers googlebomb the Vatican, causing searches for the organization's website to link to pedofilo.com (pedophile in Italian) ahead of their official website. While no communique or claim of responsibility was posted, it's clear that this action was done to bring attention to the church's culpability in the rape of an unknown but high number of children. The googlebomb happens some time during the weekend and is quickly corrected by Google.

Aug 25, 2010: Wikileaks Slaps US Government in the Face, Releasing Leaked CIA Document

Shortly after the Department of Defense demanded that Wikileaks return all the classified documents in their posession and take them off their site, they released a new leak from the CIA Red Cell, which provides internal analysis for the CIA. While the leak is interesting in and of itself, it is also a well-deserved slap in the face to the Department of Defense which

believes it has the right to make demands of Wikileaks or censor material that is already in the public domain. See the leak at http://wikileaks.org/wiki/CIA_Red_Cell_Memorandum_on_United_States_%22exporting_terrorism%22,_2_Feb_2010. Magnet link: magnet:?xt=urn:btih:7SYWLUJ44TQKGMOS572NYX5PGXXLNELE&dn=us-cia-redcell-exporter-of-terrorism-2010.pdf

August 2010: EFF Asks Verizon to Remove Unreliable Certificate Authority

The Electronic Frontier Foundation has asked Verizon[1], a certificate authority, to stop trusting the certificate issued to Etisalat.

Etisalat was caught using its authority to sign an update for blackberries in the United Arab Emirates which caused malicious code to be downloaded onto blackberry user's devices without their consent. This code (better called surveillance software) was used by the government of the UAE to spy on blackberry users.

Because browsers and other software trust Etisalat's authority, this means that any users SSL connection with any site could be hijacked completely transparently. This leaves their personal information vulnerable as well as their computers if they download executable code which is signed by Etisalat.

Hopefully Verizon revokes this certificate and the SSL trust system will be made slightly more secure. As long as trust for this system is not distributed and resides in a hierarchy, problems like this will continue to occur.

1. https://www.eff.org/deeplinks/2010/08/open-letter-verizon