```
                  _
                  |\
                  | \
                  ||\
             __   ||\\      __
 ___________   _/_/  ||\\     _/_/   ___________
| _________   _/_/   || \\   _/_/    _________ |
||      _/_/_____  || >>  _/_/_____        ||
||      /_______/  || //  /_______/        ||
||             ||//             ||
||             ||//             ||
||             ||/              ||
||             | /              ||
||             |_/               ||
||                              ||
||   c o m m u n i c a t i o n s  ||
||________________________________________||
|__________________________________________|
 ...presents...
```

Hacktivism, From Here to There by Oxblood Ruffin

```
      __/////\   -cDc- CULT OF THE DEAD COW -cDc-   /\\\\\__
 Est. 1984   \\\\\/  cDc paramedia: text #384-06/03/2004 \/////   Est. 1984
  ___   _  _   ___    _  _   ___     _  _     ___   _  _    __
 |___heal_the_sick___raise_the_dead___cleanse_the_lepers___cast_out_demons__|
```

[The following paper was presented March 28, 2004 at Yale Law School as part of the CyberCrime and Digital Law Enforcement Conference.]

"cDc. Show and prove."

I've never thought there was a lot of debate about the meaning of hacktivism. It's a word that was coined by Omega - a longstanding member of the CULT OF THE DEAD COW (cDc) - in 1996. He used hacktivism to describe hacking for political purposes. Originally it was more of a quip or a joke. But from the first moment I heard Omega use it I knew that it would have profound meaning, not just for the cDc, but for millions of people across the Internet.

Almost immediately "hacktivism" spread like wildfire. The word sounded so cool everyone wanted to use it - the trendier-than-thou digerati, on-line news editors, and especially washed-up activists who had just discovered email. Suddenly, everyone became a "hacktivist." No one had a clue what it meant, but it sounded cool.

Soon thereafter cDc members started registering hacktivism top-level domains. Reid Fleming set up hacktivism.org and ran it for a few years, Count Zero grabbed hacktivism.net, and I reserved - but never ended up taking - hacktivism.com. It is currently available from a domain name broker for $2000. You can also pick up terminatorseeds.com from the same place for a grand. Buy both and you'll probably get a deal.

The people in the CULT OF THE DEAD COW who were most interested in hacktivism were Omega, Reid Fleming, Count Zero, Nightstalker, Tweety Fish and myself. We discussed it on our listserv, in private emails and at hacker conventions, one of the few places we would ever physically meet. I always liked hacktivism as a word but thought the definition needed to be tightened up. Cyberwar had a fairly similar connotation; two big brains from RAND Corporation coined that in 1993. No, we needed something unique, something that had never quite existed in quite the same way before. It was Reid Fleming who brought in the hook.

Reid set up hacktivism.org that featured a quote from the United Nations Universal Declaration of Human Rights (UNDHR). It was Article 19 and it read, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." The first time I read that I felt like my head had gone to heaven. That was it. We would link technology with human rights. But it took some more time to get there. In the meantime I had been corresponding with Cindy Cohn, then in private practice but now Legal Director of the Electronic Frontier Foundation (EFF).

Cindy explained that the UNDHR was a declaration. Although inspirational and a very important document in its own right, it had no binding power. It was not a law. The International Covenant on Civil and Political Rights (ICCPR) was another matter. It was intended to have binding power and had at least a few teeth. And coincidentally, Article 19 of the ICCPR - another United Nations document - said essentially the same thing as Article 19 of the UNDHR. It reads, in part, "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."

The more time I spent with these two documents the closer I got to hacktivism, at least as a noun. And in fairly short order I defined hacktivism to mean "using technology to improve human rights across electronic media." I also came up with the cDc tagline, "We put the hack into hacktivism." But that was mostly as a response to the leftovers that stuck an "h" in front of activism and thought they could transpose the same ball game they'd been playing since the industrial revolution onto the Internet. One thing they didn't understand was that it doesn't take a lot of people to change anything. It only takes one good programmer.

The Internet was beginning to percolate with a new kind of activism, much of it as a result of an interview I did with Blondie Wong in July 1998. It was published as a cDc textfile and recycled across the Net. Blondie was a truly inspirational fellow. Chinese dissident, charismatic, movie star looks, monk-like tendencies, and loads of money. He ran a group of hackers called the Hong Kong Blondes. They grew to about forty members and did a lot of hacking into Chinese networks. The interview got a lot of Western hackers thinking about politically motivated hacking. Then one group got too inspired and went past the mark.

There was an American hacker group called Legions of the Underground (LoU) that had been around for seven years. They had twenty or so members, some kind of flakey, but others with truly superior skills. One in particular had been trained with the US military and knew network security backwards. So LoU made a public announcement that they had declared Cyberwar against Iraq and China, mostly for human rights abuses. At first insiders thought it was a publicity stunt. Then we found out the action was for real. LoU was probing primitive inter-networks in Iraq and getting ready to throw the switch. That's when the international hacker hierarchy decided that enough was too much. Hacking for human rights was one thing. But we had to establish some ground rules for engagement.

A coalition of hacker groups issued a statement within a few days of LoU's declaration of war. Included were (from America) the CULT OF THE DEAD COW, the L0pht, Phrack, and (from Europe) the Chaos Computer Club, Hispahack, Pulhas, Toxyn and several Dutch hackers including the cryptography expert Rop Gonggrijp. While identifying with LoU's anger towards Iraq and China we pointed out that, "One cannot legitimately hope to improve a nation's free access to information by working to disable its data networks." LoU's members took our criticism to heart and wisely called off their campaign. And just to make a further point. LoU could easily have done significant damage, especially in China, had they followed through. The fact that an international coalition of hackers appealed to LoU's reason and managed to avert what could easily have blown into an international incident is commendable, even if I do say so myself.

It was largely as a result of this experience and some email exchanges with Frank Rieger of Germany's Chaos Computer Club, and chats with Reid Fleming, that I began to formulate some hard and fast rules for hacktivist tactics. First, no Web defacements. If groups or individuals are lawfully entitled to publish content on the Web, any violation of their right to distribute information is an abridgement of their First Amendment [freedom of expression] rights. The same goes for Denial of Service (DoS) attacks. There isn't a whole lot of difference between disabling a Web server's ability to provide information - even if that information is distasteful - and shouting down someone in a town hall meeting. Although this example is more uncivil than unlawful, DoSing is clearly a computer crime. Still, civility is not a bad virtue to practice.

Increasingly I spent time speaking with reporters and academics about hacktivism, commenting on a series of Web defacements and DoS attacks. The press was awash with articles about "hacktivists" who weren't much more than low-rent computer criminals. It just smelled like the same cheap hacks were being elevated to political protest when, in my opinion, they weren't any more than script kiddy antics in drag. It became increasingly important for me to define hacktivism, mostly because I believed, and continue to believe, that there were very definite tactics that were acceptable for hacktivists. If someone wanted to call his or her actions digital disobedience, or cyber sit-ins, or anything else, that was fine with me. But invoking the term hacktivism was not OK.

At the same time I was acting as the cDc's chief evangelist for hacktivism I began to joke that we had a noun longing to become a verb. It was one thing to talk about hacktivism. It was another to put it into practice. In the summer of 1999 the CULT OF THE DEAD COW descended upon Las Vegas like the well-heeled plague of locusts we are. Our mission was to launch BO2K – a network administration tool - at Defcon. Defcon is The World's Biggest Hacker Convention(tm). It used to have some grassroots legitimacy but now it's a job fair for entry-level computer security professionals. Gripes notwithstanding, I drafted the framework for Hacktivismo at this fifth rate Sodom and Gomorrah.

For some time the CULT OF THE DEAD COW had been aware of what has become known as "the Great Firewall of China." This is a system of DNS and desktop filtering used to control its citizens. American companies like Cisco and Websense had made the firewall available to the dot Commies. When you run a business from the beacon of freedom, exporting censorship is allowed especially if it feeds quarterly earnings. Since the cDc reasoned that access to information was a basic human right we started bouncing ideas around for piercing China's digital defenses. The first conversations I had were with Reid Fleming and AJ Effin Reznor in the Suite of the Elite, the cDc's high-roller digs at the Alexis Park, Defcon's hotel site. With a few possible development solutions in hand I began looking for the right mix of people to execute them. The first three hackers I approached agreed immediately.

Bronc Buster and The Pull from the United States, and The Mixter from Germany - who was then working as a security consultant in Israel - jumped on board. All brought different skills to the table and each was highly motivated. What is quite interesting is that we all knew each other by reputation but had never met in person. And over time ideas and code started to flow from one to the other to the point where we had our first prototype: a distributed network application called Peekabooty. It would allow users to bypass firewalls, national or corporate, and access the free side of the Web from a host computer. Part of our plan was to publicize state-sponsored censorship of the Internet and raise as much awareness as possible.

Some of the best advice I got in marketing hacktivism as an issue and a brand came from Grandmaster Ratte', the founder and resident communications guru of the cDc. He continually upbraided me for attempting to make hacktivism too respectable, too much of, as he put it, "a wine and cheese party." G. Ratte' advised me to make it sexy, sweaty, and dangerous. That's what would get hackers interested. They were the ones who were going to sit down and hack the code together for long hours and at no pay; not, with all due respect, the human rights establishment. They were just gettingused to Web browsers.

I decided to stick hacktivism in everyone's face with a product name that was impossible to ignore. Peekabooty came, innocently enough; from an experience I had in Harlem. I was standing in front of Grandmaster Ratte's apartment building waiting for him. I spied a little girl sneaking a peek at me from behind her mother's enormous, spandex-encased backside. And the name Peekabooty jumped into my mind. It seemed so perfect and so playful, no matter how sassy most people thought it was. And from that moment Peekabooty became synonymous with Internet censorship. It worked even better as a meme than a technology. Everyone started talking about it, from journalists to policy makers to Congressional leaders. Finally people were starting to wake up to Internet censorship because hackers with blue hair and funny sounding handles said it was important.

Hacktivismo grew into a truly international organization. Most people were technical; others were lawyers, human rights workers, and artists. Our team came from the Americas, Europe, Russia, Israel, Iran, India, Australia, Taiwan, and the Peoples Republic of China. As the group started to grow I thought it was important for us to publish something like a mission statement. Having spent so much time poring through United Nations documentation it seemed appropriate to publish a declaration. In June 2000 I was staying at Grandmaster Ratte's place in Harlem and drafted what was to become the Hacktivismo Declaration in one sitting. It took ten more months of painstaking revisions, but finally I posted it to the cDc listserv for extensive critiquing. Eventually it made its way to Fred von Lohmann at the EFF who made it tighter. Cindy Cohn also was helpful in many ways. The Hacktivismo Declaration was published on July 4th, 2001. It has since been translated into ten languages.

The declaration reads in part, "That full respect for human rights and fundamental freedoms includes the liberty of fair and reasonable access to information, whether by shortwave radio, air mail, simple telephony, the global Internet, or other media," and, "That state sponsored censorship of the Internet erodes peaceful and civilized coexistence, affects the exercise of democracy, and endangers the socioeconomic development of nations." Hackers may wear different clothes and have odd interests, but we know what important values are.

At the same time we were trying to get the message "out," we were also trying to get it "in." The cDc invited the distinguished human rights activist Dr. Patrick Ball to speak at Defcon to a room full of hackers. The place was packed and Patrick made a huge impression. His presence at Defcon did not go unnoticed by Slobodan Milosevic when Patrick was brought in to testify against him at Milosevic's war crimes trial in The Hague. When Milosevic cross-examined Patrick, one of the first questions he asked him was, "So, Dr. Ball. Vaht can you tell me about these Dead Cow Cult?" I have no idea how Patrick managed to keep a straight face.

Hacktivismo progressed as a group but encountered a serious hiccup when the lead developer for Peekabooty rewrote the entire code base and decided to hijack the project and leave the group. It's amazing what some people will do when they figure they aren't getting enough press. When it was first announced on our listserv there were several days of chaos and rage. Some members wanted to crucify our little fame seeker, but it seemed best to let him go. He had been a disruptive force in Hacktivismo for months and things weren't getting any better. Plus when his code was reviewed it left our security experts dumbfounded. Peekabooty had been rewritten to conform to design specs that been rejected a year before as grossly insecure. You could hear the baby Jesus crying in Shanghai.

Within weeks Hacktivismo bounced back and the ideas started to fly again. The Pull came up with a really sweet hack that made a lot of sense. Since most Web censorship is based on DNS filtering, why not play against expectations? The Pull reasoned that we could have people post content that would be censored in China, and other fire-walled countries, right in plain view. DNS and desktop filtering scans for Web requests related to human rights, critical political commentary, women's issues, and a range of other topics that dictators feel uncomfortable with. But this filtering does not look for, "pictures of Disneyland, my trip to the grocery store," and other banal topics. So we would hide censored content in palatable Web sites through the process of steganography.

Steganography is a kind of encryption that allows one to bury digital content in a digital content base. Think of a Web page displaying a picture of the Mona Lisa. Steganography would allow you to hide a copy of the Declaration of Independence, an MP3, or any other piece of content digitally rendered in Da Vinci's masterpiece. No wonder the old girl's smiling. Within the space of a weekend The Pull had hacked together a working copy of the program. He then spent the next few months tightening it up. Hacktivismo released the steganography app at H2K2, a biannual hacker con in New York City. It was widely deployed. We heard from a lot of expat hackers from Iran, China, and the United Arab Emirates living in the West who were using it with their friends back home. The application was called Camera/Shy.

Our next project was called The Six/Four System. It is a complex and intuitive work of genius invented by The Mixter. Six/Four (a reference to June 4th, or the Tiananmen Square massacre) is an inaugural technology. It enables hackers to cobble together applications and drop them on top of any Internet protocol. It's not what you'd call a "user friendly" technology. The code is a bit ugly but it does enable extraordinary possibilities. Beyond the compelling achievement of this work in progress, two extraordinary things happened. The first lovechild is both significant and amusing.

I was concerned about Six/Four's firepower. Although Hacktivismo is an international organization, we are mindful of American law. Given that the United States Department of Commerce (DOC) regulates cryptography as an export and that Six/Four includes cryptographic components, I didn't want to place American members of Hacktivismo at risk. Better to have the American government on board than working against us. So we had our attorney, Eric Grimm, apply to the DOC for a ruling on the exportability of our technology. What is normally a one-month process took nearly four months. I'm not sure that the DOC has ever had a request from a Canadian, me, and a German, The Mixter. And I'm almost positive they've never had a request emanating from an organization that included Cult, Dead, and Cow in its corporate identity. But come it did, and the Six/Four System was finally approved and became synonymous with American policy. It was a relief to have the U.S., especially the Bush administration, act as a facilitator of greater freedom rather than as an oppressor and regulator.

And now for lovechild number two. A few months before releasing Six/Four, The Mixter mentioned that he'd like to license his work under anything other than the General Public License (GPL). My ears pricked up. The GPL is a tergiversation in intellectual property (IP) law, conceived by the extraordinary Richard Stallman and codified by the eminent Eben Moglen. It postulates that code is "transparent," available for peer-review, customizable, and can be shared without charge, given that certain other requirements are adhered to. The GPL is widely considered as the Holy Grail of IP law in the digital age. It creates tumescence in the Electronic Frontier Foundation, the god-like Lawrence Lessig, and a host of lesser luminaries. It's a huge deal. But is it all that?

As important as the GPL is, it only seeks to do certain things. Namely, to create "freedom" to invent and to share. It assumes, as most hippy philosophies do - and I use that term with affection - that we live in a world of ideals; where all it takes is the "right" idea to find its way to the top and prevail in a marketplace of intellectual substance. And that the "idea" will be protected. That's a great worldview if you live in America or any of the other liberal democracies. But we don't. At least those of us in Hacktivismo don't. We live in a brutish and uncompromising world of thugs, Internet censors and life forms beyond the borders of civilized discourse. Hacktivismo stares down, just for starters, the government of China. They could win a prize for Most Inconscient Life Form In A Political Body(tm). This is a government that would not have put Ghandi or Martin Luther King in jail for the weekend. Beijing would have blasted a bullet into the backs of their heads and charged their next of kin for the cartridges the morning after.

No. Hacktivismo wanted to release its software under something a little less free than the GPL. The greater girdle we could put on the Internet's worst oppressors, the better. And so it was with this modest ambition that Eric Grimm, The Mixter, and myself began drafting what came to be called the Hacktivismo Enhanced Source Software License Agreement (HESSLA). The license enables both Hacktivismo and its end-users to go to court if someone tries to use the software in a malicious manner, or to introduce harmful changes in the software. It also contains more robust language than has previously been used to maximize enforcement against governments around the world.

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

This, we think, is a pretty novel "legal hack," and we are optimistic that it just might work when our "code" is finally "executed" in the U.S. legal system. So far, this part of the HESSLA has received little attention, but since we are here at Yale, perhaps it is worth discussing the origins of the idea of end-user enforcement, and what we are trying to accomplish.

Most of the provisions of the HESSLA (which build on the idea of "copyleft") explicitly credit the Yochai Benklers, Eben Moglens, and Lawrence Lessigs of the world for their inspiration. The end-user enforcement provisions, in contrast, draw more inspiration from the work of Harold Koh, James Silk, and the Lowenstein International Human Rights Clinic, here at Yale.

As many of you know, for well over a decade, the Yale Law School and some of its distinguished faculty have been at the forefront of developments in international human rights law - especially the implementation of human rights norms through civil lawsuits in U.S. courts, against (to borrow a phrase from George W. Bush) human rights "evil-doers." A little over two decades ago, the Second Circuit, in a case called Filartiga v. Pena-Irala, revived a 1789 statute called the Alien Tort Claims Act, and said that some victims of human rights abuses could sue some abusers, in U.S. courts, for certain violations of international law.

Remember -- some, not all, victims can sue; some, not all evil-doers, can be sued; and not all human rights abuses trigger legal remedies. In the intervening time, the ATCA (and additional legislation such as the Torture Victim Protection Act), have been used to great effect in civil litigation in the U.S. courts to bring some abusers of human rights to justice, as well as to compensate certain victims. Yale faculty have been directly involved in some of the key developments -- such as Professor Koh's role in the landmark Kadic v. Karadzic case, which was brought by one or more victims of sexual abuse against Bosnian Serb leader Radovan Karadzic.

While the human rights community has enjoyed many victories over the years, using various strategies to secure U.S. jurisdiction against foreign bad actors, legislative and court-established limitations still remain as obstacles to enforcement activity by the human rights community. Depending on the party occupying the Presidency, the Executive Branch of the United States government on occasion during the past two decades has often been openly hostile to the idea of vindicating human rights in U.S. courts, while, at other times, the Executive has been open to some limited progress in this field.

The jurisdiction, immunity, and end-user enforcement provisions of the HESSLA cannot compare, in importance, with the legal victories won over the past two decades in the human rights field. But we have sought to make a very modest contribution -- in the sense of adding one more arrow to the quiver of legal strategies that Professor Koh and other pioneers in the field of human rights law may be able to use to seek justice for victims of human rights abuses.

The more tools that human rights workers and plaintiffs can employ in these cases, we believe, the better. And, in light of continued restrictions on statutory causes of action (as well as the current administration's hostility to many aspects of the limited human rights laws we have), we believe that the HESSLA may yet prove useful.

Of course, in order for these provisions of the HESSLA to be invoked, a human rights defendant has to have used or modified the software. But this threshold issue is important, too, because we are quite happy if governmental and other abusers of human rights voluntarily decline to use our software on account of the in terrorem effect of the possibility of triggering a lawsuit. Even if it turns out that all the "bad guys" in the world are avoiding the software, and cannot be sued using this provisions of the license, that also means they are actively depriving themselves of the tools that we have created, while the "good guys" can use these tools.

Whether or not the HESSLA ever makes its way to court, we think that the mere existence of the HESSLA can have important, beneficial effects. The GPL still hasn't been tested in court, yet, regardless of the many claims made for it. But the positive social impact from the GPL certainly is not measured solely in terms of the frequency and nature of lawsuits involving the GPL.

We do know that many developers around the world are starting to use the HESSLA to license their works. Regardless of the occasional sniping from some free software fanatics, we are optimistic that the HESSLA, including the most critical parts of it, at the end of the day, are quite likely to be found to be enforceable against all or most defendants, including non-U.S. governments, in the U.S. court system. So long as the U.S. courts follow the letter of the Foreign Sovereign Immunities Act, the HESSLA has been drafted to maximize enforceability when the time comes to invoke it in court. Then again, we certainly do not have a monopoly on clever and novel legal or licensing ideas, so anyone in the audience (or at this law school), who has ideas on how to make the HESSLA even more effective, or more enforceable, is certainly welcome to communicate those suggestions to us or to our lawyer.

Returning to the critics of the license, we note that the primary criticism is simply that the HESSLA is not the GPL. Quite right. It isn't. Then again, many of these same skeptics also have, from time to time, voiced concern (typically prefaced with the disclaimer "IANAL") about whether the GPL itself is enforceable. Some day, those tests may arise. But until that time, we think it is worth asking whether the uncertainty of a license not previously tested in court nevertheless remains a factor that benefits or helps Hacktivismo's objectives. Among our objectives is to deter at least some of the "evil-doers" from using our software.

This room is full of lawyers and future lawyers. Ask yourselves: If you were advising some person or entity that viewed itself as a likely defendant in some future HESSLA enforcement action by Hacktivismo or by some end-user -- would you be so confident of your client's chances (if caught violating the license) of prevailing in court -- that your client should go ahead and openly start using the software, without any concern about risking the consequences of losing? Eben Moglen has, for years, been inviting all the skeptics of the GPL to call his "bluff" (which, in our view, is no bluff at all), and take the Free Software Foundation to court. The mere fact that nobody has done so serves as a powerful argument that the GPL-skeptics are not very confident of their legal argument. I can't say that I'm looking forward to testing the HESSLA in the courts. That would suggest that yet another human rights violation has occurred. But I am proud of attempting to provide even an untested remedy when the alternatives remain far from perfect. When Hacktivismo started germinating in Las Vegas I had no idea I'd end up speaking at Yale Law School. But when you roll the dice, you never know where you'll land.

```
   .-.                    _   _                      .-.
  /   \         .-.      ((___))         .-.        /   \
 /.ooM \       /   \    .-.  [ x x ]  .-.     /   \      /.ooM \
-/-------\-------/-----\-----/---\--\   /--/---\-----/-----\-------/-------\-
/lucky  13\    /      \  /    `-(' ')-'    \  /      \    /lucky  13\
       \  /       `-'        (U)        `-'       \  /
        `-'            the original e-zine            `-'   _
    Oooo                eastside westside              / )   __
 /)(\ (   \              WORLDWIDE                   /  (  /  \
 \__/  )  /  Copyright (c) 2004 cDc communications and the author. \   ) \)(/
     (_/    CULT OF THE DEAD COW is a registered trademark of    oooO
       cDc communications, 1369 Madison Ave. #423, NY, NY 10128, USA    _
  oooO            All rights left.  Edited by Myles Long.        __   ( \
 /   ) /)(\                                            /  \  )  \
 \  (  \__/      Save yourself!  Go outside!  Do something!      \)(/ (   /
  \_)                xXx   BOW to the COW   xXx                  Oooo
```