HOW TO PLAN AND EXECUTE AN ACT OF ELECTRONIC CIVIL DISOBEDIENCE (ECD)

PUBLISHED ANONYMOUSLY IN THE YEAR 2010

This zine is for informational purposes only. Nothing in this zine should be construed as encouraging you to break the law. If you decide to break the law, it is your own choice and you will have to face responsibility for it. This text is provided to you exclusively for research and academic purposes. It provides an example of how one might plan and execute an ECD attack but does not encourage you to do so – consider it a hypothetical exercise.

Distributed denial of service attacks, also called electronic sit-ins, online protests, or ECDs, are becoming a popular tool to target those who destroy the earth and our communities while gaining ridiculous amounts of money and power at the expense of others.

Demonstrations are often seen mainly as an act of propaganda – they are useful as a means of giving a movement a visible presence, informing people about its existence, and getting people involved. Without a wider movement, demonstrations turn into empty sign holding which accomplishes nothing except draining energy from the participants. Demonstrations can be powerful when showing people's support for a particular cause, but if that is the only tactic a movement has in their toolbox, it will likely be ineffective in creating any change. Distribute denial of service attacks, like demonstrations, generate media coverage, discussion, and provide a clear visible measurement of the support any particular movement has. They also provide an easy way for people to become involved in a movement and participate, especially if they don't know anybody else in their area who has the same ideas they have.

Distributed denial of service attacks are easy to organize, participate in, and successfully use to advance social movements. All one needs to do is pick a target, package the ECD software in a way which will work, distribute the tools and a call-out, charge your lasers, and fire! Most websites do not have DDoS protection because such protection is expensive and 364 days of the year they likely won't be needing it. As a result, most DDoS attacks

A **denial-of-service attack (DoS attack)** makes a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all during the attack.

A **distributed denial of service attack (DDoS)** is when multiple systems flood the bandwidth or resources of a targeted system. Flooding a government office with phone calls, sending black faxes, or setting up human blockades at protests are examples of lower-tech forms of DDoS attacks.

Electronic civil disobedience (ECD) can refer to any type of civil disobedience in which the participants use information technology to carry out their actions. For the purposes of this zine, we'll be using the term DDoS attack and ECD interchangeably.

Hacktivism is the use of hacking skills in the furtherance of a political goal.

Bandwidth is the amount of data you are transferring or capable of transferring.

An **IP (Internet Protocol) Address** is a number used to identify and correctly route traffic to a device connected to a network (such as the internet). Think of it as the street address of a house, except for a computer or server.

A **domain name or hostname** is a name which is useful for the human brain to remember the location of a device (such as a web server) on a network. The name is converted to an IP address using the DNS system.

An **Internet Service Provider** is a company that sells access to the internet.

A **bandwidth limit** is a certain amount of network traffic that a particular computer is allowed to have by their hosting or internet service provider. When it passes this amount, it results in the disabling of the site or extremely expensive bandwidth bills similar to what happens when one goes over the minutes on their cell phone.

only require between a few dozen and a few hundred people to successfully knock a site offline. Of course, you'll need more than a dozen people to pull off the attack successfully as anonymity loves a crowd.

Picking a Target and Doing Research Anonymously

Let's assume you already have an evil entity in mind which you want to attack. You'll need to figure out what part of their electronic infrastructure you want to target. As large sites may have significantly more bandwidth, it might make sense to pick smaller targets for your attack. Many websites also host the mail server for your evil entity which, if taken down, will disrupt internal and external communications for the duration of the attack. You'll need to do some research to find these servers.

When doing research, it's important to do your research in a way that can't be easily traced back to you. As what you're doing will likely be illegal, you'll want to cover your tracks well. A mantra of hackers is "never hack on your own connection" and it holds true in this case. Regardless of how many proxies or anonymity systems you use, you don't want to rely solely on them for your security. The best way to do this is to find a public wireless hotspot (such at a library, coffee shop, or office building), run your connection through anonymity software, and then do your research from there. Relying on anonymity software to keep you safe is akin to relying on your friends to not rat on you – the best solution is simply to never tell them in the first place. Depending on the level of security you desire, you may want to be sure to check that no cameras or people are watching what you do. If you use your proxy system correctly, the attack will never be traced to the connection to used.

> Every evil corporation relies on the internet for everything from communications to sales to public relations. As they become more reliant on networked solutions, the possible disruption an attack can cause increases exponentially. Instead of attacking a public website, maybe it would make more sense to attack the devices that they use to connect to the internet or their internal mail server. This still works as a powerful act of propaganda but adds additional strategic value and bite to your attack.

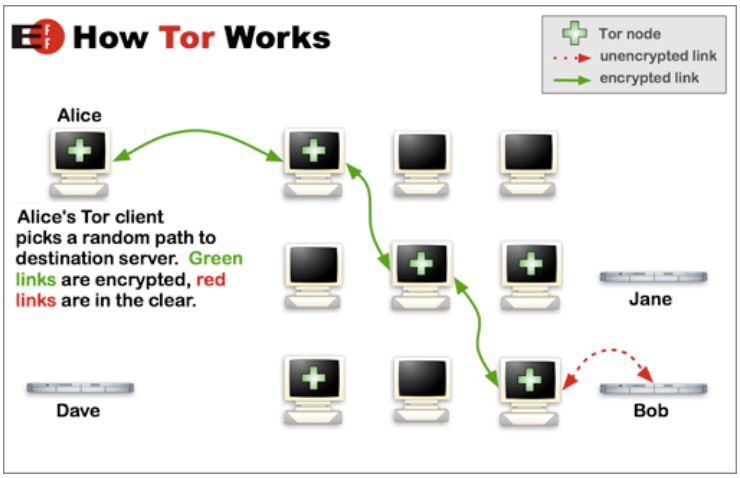
People who plan ECDs take on additional risk compared to those who simply participate in them. Targets of ECDs and law enforcement will often try and find who started the ECD in order to pin it on them. The first step law enforcement takes when investigating politically motivated crimes is to trace the communique.

You'll need to know both the hostname (ie example.com) and the IP address of your target for the various tools covered in this manual. In order to find the IP address, simply look online using a search engine for "online ping" which will bring up a number of tools that will retrieve the IP address for you. Online ping services are simply servers that perform the ping command for you (think of it like a proxy for pings). You can also use the ping command on Windows, Linux, or OSX but this won't work through a web proxy so it

may reveal you as the initiator of the attack.

Most anonymity software is simply a network of open proxies. Open proxies are systems that either accidentally or deliberately allow you to route your connection through theirs. When you connect to the website you are trying to reach they will see the IP address of the proxy instead of yours.

Many people suggest using "one hop" proxies to protect your privacy online but this is very dangerous advice. When you rely on a one hop proxy, you are putting your security in the hands of one server operator who may or may not have your best interests at heart. Even if they do, if they have logs they will probably have to legally turn them over when requested by a court. Some one-hop proxies also add "forwarded-for" headers to HTTP requests (your web browsing traffic) which reveal your true IP address. Your ISP and their ISP will also maintain logs which show who connected to that one hop proxy and when. Your connection is also usually not encrypted, meaning anybody on your home network, your ISP, their ISP, anybody on their network, and anybody sitting in-between can see what you're doing.



Right now the best anonymity software available is Tor (https://www.torproject.org). Tor is a network of proxies run by volunteers. It is used by whistleblowers, online dissidents, spies, police, corporations, lawyers, and just about everybody in-between to protect their privacy. By mixing in with all of these users, you gain additional privacy as it becomes harder and harder to pinpoint who is using the service. When you route through Tor, your connection actually goes through three proxies and while the speed may be a bit painful at times, it's worth the wait. No individual server operator knows both who you are and who you are connecting to. Your traffic is encrypted between the proxies, called Tor nodes, but becomes unencrypted when you connect to the target just like when you browse the web without a proxy.

Tor server operators are not legally responsible for what you do online but remember that if anything gets traced back to that server, you put that operator at risk of receiving a nasty letter, getting their internet disconnected by their ISP, or getting raided because the police hate anonymity or don't understand what a proxy is. Tor server operators are aware that people will use their service for illegal ends and believe that the benefits of having an anonymous way to use the internet outweigh the risks. That being said, please tread lightly while using Tor and try not to get any of those volunteer server operators in trouble.

Once you install and configure Tor (instructions are available on their website), make sure your connection is actually going through Tor by going to check.torproject.org. Nobody has ever been traced back through Tor as a result of flaws in the software. However, people have been traced back because they did stupid things while using Tor such as logging into an email address which is tied to them while also doing something sketchy, posting their personal information online, etc. Use Tor only for one particular identity and do not mix it up! If you must use multiple identities through Tor, clear the private data from your browser and use the "New Identity" function of Tor.

Congratulations. You are using Tor.

Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously.

Additional information:
Your IP address appears to be: **192.251.226.206**
This small script is powered by tordnsel
You may also be interested in the Tor Bulk Exit List Exporter

This server does not log any information about visitors.

Tor offers a number of configuration options and the easiest one is probably the "zero install bundle" which comes nicely packed in a zip file, stores no information about your browsing, and can easily be deleted when you are done. You can put it on a flash drive and run it on most any computer. They have zero install bundles for Windows and Linux.

Choosing an ECD tool

There are a number of tools available for you to do your dirty work. There's a few here to look through but there are literally tens of thousands of them available online. Finding the one you like best is up to you.

GreekSolidarity ECD Tool

This tool was used during an ECD done in solidarity with Alexandros Grigoropoulos (a teenager who was killed by Greek Police). I was unable to find any older uses of this tool but find it hard to believe that it was developed specifically for this attack. This tool is javascript-based so users can simply load the page in their browser regardless of operating system and participate in the ECD without downloading any programs. Many people are wisely concerned about downloading executable files onto their computer so this helps them participate without taking significant security risks. The tool repeatedly reloads images from your target's website in order to monopolize the available bandwidth. When lots of people run this tool, it can knock a server offline or simply use up their bandwidth limit.

There are a few sections which you'll need to edit. Simply open GREEKECD.html with a text editor such as notepad. Do not open it in a rich-text editor (an editor which can apply formatting such as bolding or headings) such as Word as it will not save properly and could compromise your anonymity. Below are a few sections which you'll need to edit. There are other easy-to-edit sections in the code which you may

look for but this covers the essentials.

In order to find the sections referenced here, simply search for the SearchKey, which will bring you to that section. In most text editors, Control+F will get you to the search box.

SearchKey: WRAP YOUR TEXT AT THE SAME LENGTH AS THIS LINE

This section allows you to display a message to people participating in your ECD. This should be similar to your call-out. Make sure each line of text isn't too long or it will display incorrectly.

SearchKey: NOTE: All numbers should be whole (ie: 1, 10, etc.) or tenths (ie: 1.3, 10.1, etc.).

This section allows you to set how much bandwidth your tool should use up. You'll probably want to keep these values the way they are or make them high if they are set low.

SearchKey: // This will be put into the server logs of the target.

This section allows you to flood the server logs of your target with the message of your choice. When the evil corporation looks through their logs, they'll see your demands, angry rantings, or whatever else you put in there. This works by loading example.com/image.jpeg?YOUR_MESSAGE_HERE. You can add as many messages as you want. Be sure not to use spaces or punctuation.

A Few Examples of Past ECD Attacks

1989: Wank worm attacks computers at NASA and military installations to protest use of nuclear power on the Galileo spacecraft and the proliferation of nuclear weapons.

1998: Electronic Disturbance Theater leads lengthy campaign against Mexican Government targets for brutal repression of the resistance in Chiapas.

1999: Week-long ECD against the WTO (World Trade Organization) to co-inccide with protests at Seattle WTO Summit.

December 13th, 2003 Animal rights activists attack a customer of HLS (Huntingdon Life Sciences), which is a notorious animal "testing" laboratory that has been the subject of a vicious and effective decade long campaign.

Feb 25th, 2004 in a large ECD, thousands of websites host copies of The Grey Album (a free mash-up between Jay-Z and The Beatles) and turn their web sites gray in response to EMI attempting to legally intimidate those who shared or discussed it.

December 15th 2008: Animal rights activists attack HLS (Huntingdon Life Sciences) in a continuing campaign against their cruel animal testing. There are only two such attacks listed here, but the animal rights movement has a long history of using these attacks.

Dec 29, 2008 ECD Launched Against Greek Government websites in solidarity with Alexandros Grigoropoulos, a 15-year-old who was murdered by Greek Police, and the rioters who took to the streets in his remembrance.

June 2009 Anonymous launches DdoS attacks against websites of the Iranian government in

SearchKey: // Number of load failures before image status is changed...

This tool is designed to attack multiple targets at once. So, you could attack example.com, mail.example.com, and examplesfriend.com. Once a particular image fails to load a number of times, it works on loading the other images to use your bandwidth in the most efficient way possible. The colors of the boxes around the image will change according to the "health" of the server you're targeting. You'll probably want to keep these values the way they are.

SearchKey: // Place two forward slashes (//) in front of a line to 'comment out' that line so

This section is the hardest to edit but also the most important. This is where you define the images which you'll be repeatedly reloading to suck bandwidth from your target. When picking images, it's important to pick the largest images you can and also images which the target website can't disable. For instance, if you pick an image that isn't important to the operation of the website, your target may just delete that image. For this reason, you'll have to find a good medium between large images and important images. You can find out how large various images are by saving them to your hard drive or going to Page Properties in Firefox and going to the media tab where it will list the various sizes.

February 2010 Anonymous takes down countless sites of the Australian government in response to plans to implement a country-wide net filter. These attacks were dubbed "Operation Titstorm" due to the proposed banning of pornography which contained women with breasts under a certain cup size. The attack not only included online DDoS attacks but black faxes, porn faxes, and other forms of DdoS.

July 2010 Website of the European Climate Exchange (an exchange for trading carbon credits) is defaced by decocidio to bring awareness to greenwashing and false climate change solutions.

December 2010 Mastercard and Visa credit card processing systems are hit by a DdoS during their most profitable time of the year: the holidays. Anonymous executed this attack in their response to stop processing payments for Wikileaks.

2008-Current: Anonymous leads a series of DDoS attacks against the Church of Scientology in Operation Chanology.

Most images will be accessible by clicking around on the site, but you can also check directories like example.com/images and example.com/pictures. Be creative when looking for images. The other option is to do a Google images search for that particular domain and sorting the images by size. Use insite:target.com as your query instead of "puppy" or whatever you normally put in there.

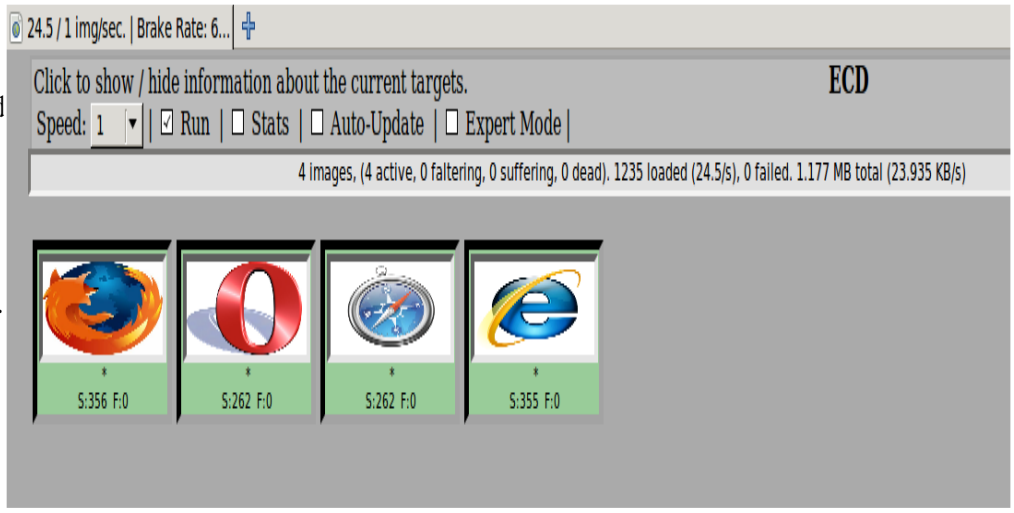
Assuming all of your images are on one site, there's no reason not to find fifty different images to make it difficult to blunt the force of your attack. If you're attacking multiple sites, be sure to include an equal

number of images for each if you want each site to get hit equally hard. You can also weight your attack by picking larger images or a larger amount of images from any particular site.

You can add images in the format below, which is difficult to understand at first. Each "section" is divided by quotes.

["http://", "www.target.com", "/image/image.jpg", "14827", "0"],

The first section defines the protocol through which you'll be loading this image. Most images will load over the HTTP protocol but if you can find some that load via the HTTPS protocol, they can be better as they are encrypted and force the target server to work harder to decrypt and encrypt data back to you. Right click on an image and choose "copy image location" to get its location.



The second section defines the domain you'll be targeting. The third section defines the path of the image relative to the webserver. Basically what you'll be doing is splitting up the image address into three parts.

The next section is the size of the image you're loading in bytes. This section is not critical to the operation of the tool but gives your users an accounting of how much they've contributed to the ECD. Most images will show their size in KB (kilobytes) or MB (megabytes). A kilobyte is roughly one thousand bytes and a megabyte is roughly 1000 kilobytes. For instance, a 3.5kb image would be 3500 bytes. A 2.5mb image would be 2,500,000 bytes. Make sure not to include commas when putting the byte amount in the script.

The final section defines which message will be put in the server logs when you load your image. You can choose ONE message per image OR choose to randomize which message it puts in on a per-image basis. If you're attacking two domains, you can include several different messages by choosing one message per image. Be sure to add a comma at the end of each line.

Once you've made your edits, you'll need to check that they work. Open your browser running through whichever anonymity software you choose and open the html file you edited. When you load images from any site, a "referrer" header is sent to the server you load them from to tell them which page you are on. In this case, the referrer header will tell them where you loaded this page from. Make sure the HTML file is not stored in a directory which can identify you such as C:\Documents and Settings\John

James\Desktop\ECD.html. Just put it in C:\ or another directory which can't be tied back to you. If you don't know whether the directory you are in can identify you, move the file.

You can grab a copy of the tool at:

http://tinyurl.com/32z2chl (hotfile)

http://tinyurl.com/39ljtce (sendspace)

http://tinyurl.com/333eocg (hotfile, zip version)

http://www.sendspace.com/file/c8njjq (sendspace, zip version)

Unfortunately the only available mirrors I could locate are on temporary file hosting sites. If anybody has any longer-term mirrors, please update this guide and re-distribute it.

Low Orbit Ion Cannon

The Low Orbit Ion Cannon is a DDoS tool that has become a favorite of Anonymous in their attacks against recording instustry lobbying groups, the Australian Government, Scientology, and others who threaten freedom on the internet. It runs on Windows operating systems and can be run on Linux operating systems with some tinkering

The tool works by flooding a server with HTTP, TCP, or UDP requests. HTTP requests are mainly useful for taking down web servers while TCP requests are useful for everything from web servers to mail servers.

Other Tools

Another tool of interest is Floodnet which was built by the Electronic Disturbance Theater during the 90s and used extensively by the Zapatistas. The tool is Java based and many browsers are not set to run Java so it may be difficult to deploy on a wide scale. It also seems fairly difficult to configure and requires a webserver to run. The page for floodnet is available at http://www.thing.net/~rdom/ecd/floodnet.html

Sometimes the simplest way to participate in a DDoS attack (and the hardest thing for web servers to block) is to constantly refresh the target's website. The web browser Opera supports this by default but Firefox and Internet Explorer do not. There is a Firefox extension called ReloadEvery that can refresh a page as frequently as you like available at https://addons.mozilla.org/en-US/firefox/addon/115/.

There are thousands of tools out there so explore them but be cautious running scripts and programs from untrusted sources. Always run them with a firewall and anti-virus in place while you're testing them and research the tool before downloading it.

In order to use the tool, simply put the IP address or domain name of your target in, hit "lock on", and then hit "IMMA CHARGIN MAH LAZER". You can also work with some options in the lower portion of the program for more advanced targets,

You can grab the tool from http://sourceforge.net/projects/loic/. There is also an attempt to make a Linux-friendly version at http://loiq.sourceforge.net/.

Slow Loris

Slow loris is a DoS/DDoS tool which operates differently than most bandwidth-leeching tools. Instead of overloading servers with the amount of bandwidth it is pulling, it overloads the server by keeping a smaller number of requests open, forcing the server to keep those requests open, and preventing the server from taking more requests. A single user can often take down a web server with this tool. Slow Loris requires very little bandwidth and only runs on Linux systems.

To run it on Linux, simply use the following command from the directory which contains the slowloris script.

perl slowloris.pl -dns target.com

If you get any errors using this command, it could be that you don't have the necessary perl modules to run the program. Run the following commands separately.

perl -MCPAN -e 'install IO::Socket::INET'
perl -MCPAN -e 'install IO::Socket::SSL'

Depending on your system, you may need to add "sudo " before running these commands in order to run them in super-user mode. The modified command would look like this:
sudo perl -MCPAN -e 'install IO::Socket::INET'
sudo perl -MCPAN -e 'install IO::Socket::SSL'

Some servers such as IIS6.0, IIS7.0, lighttpd, nginx, Cherokee, Squid, and a few others are not affected by this tool. Most sites running Apache and other servers (most websites on the internet) are vulnerable.

You can get slowloris at http://ha.ckers.org/slowloris/slowloris.pl.

http://packetstormsecurity.org/filedesc/slowloris.pl.txt.html

Distributing Tools and Posting a Call-Out

This step is the most dangerous one. You'll want to create a call-out so that people know the ECD is happening and how to get involved. Like with your preliminary research, you'll want to make sure you do it

as anonymously as possible. The call-out should say why the ECD is happening, when it's happening, how to use the provided tools, and links for the tools. Since you don't want your target to put preventative measures on their servers to blunt attacks, you probably don't want to give them more than a few days notice.

When planning the length of your ECD, it's important to be realistic. If you set an ECD for an entire week, there's a good chance you won't reach your goal and that people won't participate because they see it as unrealistic. Most ECDs last a day or two unless they're part of a larger campaign. Be sure to list what timezone this attack is taking place in.

When linking to and explaining the tools, be sure to give clear, concise instructions as most people won't know how to use them or understand how they work. Be sure to explain what they do and any legal risk the person participating in the ECD will take.

Unless you're using a widely available tool like the LOIC, you'll need to find places to host your tool. There are literally thousands of free hosting places to choose from. Another good option is file-locker sites such as rapidshare.de, megaupload.com, and depositfiles.com. They allow you to host your file for download by other people. There is a good site to compare free web hosts at http://www.free-webhosts.com/ but you know how to use a search engine. Some web hosts won't let you host executable files so it might work to hide them inside a zip file or other archive. Many web hosts require a lot of personal information so plan to fill in fake information. Plan for one or two of the sites hosting your tool to get taken offline and make mirrors which will be listed in your call-out. You can't have too many mirrors but you can have too few.

Depending on your goals for the campaign, you may want to send a press release to various groups in your movement, media outlets, or websites. Like the call-out for participation, it should be brief and explain your goals. If you do this, you might want to send out a press release after the ECD is complete describing the success you inevitably had. You'll need to sign up for a temporary email and like web hosting services, there are thousands of them out there.

Participating and Monitoring the Attack

Once your call-out has been posted and you've waited till the pre-determined time, it's time to start the attack. If you feel like the numbers you have are insufficient or the attack is not working, it may be best to simply not participate as it may put you at significant risk. Whether to attack or not is a weighing of the risks and the benefits and each participant must make this decision. Since you won't be using your own internet connection anyways, this shouldn't be too difficult. You can also go to many libraries and other locations with public computers that aren't monitored too well and load up your tools there depending on the configuration of the computers. This is probably something you should not do if you planned the attack.

You should not use a proxy system like Tor for participating in the attack. Doing so is equivalent to firing a

rocket launcher from behind a fence, you'll end up destroying the fence instead of your actual target. If you can find a fast one-hop proxy, it can be suitable for participating in an attack but be sure to keep an eye on the bandwidth you're pulling.

Throughout the ECD, you'll want to check to see if the targets are still up and monitor the comments on sites where your call-out has been posted (you can search for a portion of your call-out using a search engine to find places it got re-posted). There could be people who are confused or who are deliberately spreading FUD (fear, uncertainty, and doubt) to blunt your attack. In the case of FUD, you should vigorously and anonymously respond to it.

Once the attack nears its end, you'll probably want to quit sooner than everybody else. If you are the first to attack and the last to stop, it weakens the anonymity you gain by getting a bunch of other people involved. Remember to make your connections indistinguishable from other participants.

Attacking corporations is one thing but attacking legally protected systems such as government computers will entail substantial risk. Before you participate in or plan an ECD, you should look up relevant laws such as the Computer Fraud and Abuse Act. In previous prosecutions for ECDs, the tactic of choice has been picking out a select few participants and making examples out of them. In the case of prosecutions against alleged members of Anonymous, they have picked 2-3 people out of the tens of thousands of people who participated in the attacks. These prosecutions could have been easily avoided by not using one's own internet connection.

The Legality of ECD Attacks

ECD attacks exist in a strange realm where there is no concrete legal ruling that can be applied. Always assume they are very illegal and adapt your strategy from there. The author of this manual isn't a lawyer so this shouldn't be considered legal advice. This section is based solely on the author's personal knowledge and observations.

ECD attacks may be considered free speech. You're sending messages to your target using their server logs. This is an argument that has been put forth by groups like the Electronic Disturbance Theater and Professor Ricardo Dominguez. While this has not been tested by a court, these groups have publicly participated in, planned, and promoted many ECD attacks without significant legal repercussions. They also developed ECD tools.

We do know that people have been put in jail for participating in DDoS attacks. For instance, Dmitriy Guzner, an alleged member of Anonymous, was charged with unauthorized impairment of a protected computer because of his alleged participation in a DDoS attack against Scientology. Because Scientology is classified as a religious institution under US law, they gain additional legal protection for their servers. If he

was involved in this attack, he was likely using LOIC or another tool which would not gain the potential first amendment protection that tools like the Greek ECD Tool and Floodnet provide.

A large part of the ability to charge a person for participating in or planning a DDoS attack boils down to their intent. If they intended it as an exercise of free speech instead of shutting down a website and causing damage to their operators, the first amendment defense stands a greater chance of being approved by a court.

Additionally, attacking targets outside of their own country can provide you additional legal protection. When they are looking for people to prosecute or sue, they'll pick the lowest hanging fruit which will not be you if they have to extradite you or go through the other hassles associated with international borders.

Like any action, one must make an evaluation of the potential risks and rewards. When you attend a large demonstration, you take on a full spectrum of risks from receiving a jaywalking ticket to being charged with a variety of things to having the shit beaten out of you or even death. Very few people who participated in DDoS attacks have been given jail time as opposed to the countless people who have been given it in large amounts simply for attending a demonstration. While it might be hard to be anonymous at a demonstration, it's easy to be anonymous on the internet.

Resources for a Budding Hacktivist

HackerGames.net – A conglomeration of various simulated hacking challenges to sharpen your skills

Hackbloc.org – A clearinghouse for information about hacktivism. Publishes HackThisZine and has an interesting mailing list.

HackThisSite.org – A clearinghouse for information about Hacktivism. Contains hacking challenges to sharpen your skills.

CriticalSecurity.net – A forum for hackers and hacktivists.

Wikileaks.org – A site that produces leaks of significant ethical and political importance. They have been extremely effective in obtaining leaked materials and obtaining maximum political impact.

Cryptome.org – A leak site mainly focusing on law enforcment and government intelligence.

Ubuntu.com – A great Linux distribution which is newbie-friendly and versatile.

2600.com – Website of 2600 magazine, the longest running Hacker magazine. It traces its roots back to the Yippies and hosts a conference bi-annually in New York City.

Torrentfreak.com – Coverage of action in the file sharing universe particularly as it relates to BitTorrent.

Wired.com/threatlevel – A blog covering major events in the cyberworld. Fails to do adequate research on stories.

Oldskoolphreak.com – Phreaking information with links to other similar sites. Home of "Project Wal-Mart Freedom", an effort to index information about Wal-Mart security and telecommunications.

Sectools.org – "Top" 75 security tools.

ActivistSecurity.org – What it sounds like