CHAPTER VII

Online Civil Disobedience

Online civil disobedience is the use of any technology that connects to a network in pursuit of a cause or a political or social end. There are many forms of online civil disobedience. A person or groups of individuals may block access to a website, redirect web traffic to a spoof website, deface a website, or flash messages on screen. The off-line equivalents would be a sit-in blocking access to a building, a protest that prevents people from using a street such that they are redirected, protesting with signs and images, or handing out flyers or placing flyers in mailboxes. Some of these off-line activities are illegal while others are not. As will be seen, some of the equivalent off-line acts are legal while the online equivalent is ambiguous at best, and at worst will attract civil liability or criminal sanction.

It is important to reiterate the difference between online civil disobedience and hacktivism. Because hacktivism (as discussed in ch. 5) involves the unauthorized access and/or use of and/or interference with data or computer or network, it always falls within the purview of a crime. This is because the so-called Budapest Convention—the only institutional arrangement for international cooperation on cybercrime—makes unauthorized access, use, or interference of data, a network, or a computer illegal. There are no exceptions for security research or public interest found in the convention. Many countries, including Canada, Australia, and those of the Europe Union, are signatories to the convention and, as such,

have adopted compatible legal frameworks. By and large, there are few exemptions from criminal and civil liability. The few existing exemptions are specific to jurisdiction, as will be explored further throughout the book. Often hacktivism involves a further crime after unauthorized access, such as credit-card theft or the copying and public posting of private information. Nonetheless, the boundaries between online civil disobedience and hacktivism may be thin at times.

7.1 Online Civil Disobedience in Context

Online civil disobedience incorporates a variety of techniques such as SQL injection,[1] DNS hijacking,[2] adware/spyware,[3] phishing,[4] ransomware,[5] DDoS attack,[6] botnet,[7] cloud,[8] and IoT.[9] These terms were explained in detail in chapter 2 but the most important terms are explained again below for your conenience. The terms are important, as are the specifics of the techniques used to carry out an act of civil disobedience. Why? Because using one method to, for example, perform a DDoS attack may require unauthorized access to data or a network, which is captured by criminal law, while another technical method to perform DDoS does not involve unauthorized access or use, and is therefore less likely to be captured by the law. As will be further demonstrated, there is insufficient case law to fully appreciate how many of these activities would be interpreted by the courts.

One of the most common forms of online civil disobedience is a DDoS attack. I will discuss the different methods of performing DDoS, then I will look at three separate DDoS events. The first involves unauthorized access of data and computer in Anonymous's Operation Titstorm, where criminal law was used to prosecute one of the participants in Australia. The second example looks at a DDoS incident in Germany, where the courts refused to convict the organizer of a DDoS protest. The last incident looks at the Canadian example of a quasi-DDoS as regards a Twitter campaign protesting a Canadian public-safety minister's surveillance proposals, which was clearly an act of legal protest.

There are many ways to launch a DDoS protest, but the most common method is through what is known as a botnet. Recall that a botnet is typically a collection of compromised computers that are remotely controlled by a bot master. Botnets can be made, hired/rented, and purchased. Botnets, however, can also exist with

non-compromised systems where the individual authorizes their computer to become part of a botnet as is the case with LOIC and similar services. These are re-explained further below as the method used is relevant to the legal implications of the protest participant.

Make a Botnet. A person could physically make a botnet, though through painstaking hours of labour since it would entail compromising several hundred if not thousands of computers. This type of botnet would require the botnet master to have a high level of computer skills. Typically, the botnet master installs software onto a third-party system without their authorization, and these computers become compromised and part of the botnet. The compromised machines are then used to launch a DDoS attack/protest.

Hire/Rent a Botnet. A second type is whereby the person merely hires someone to execute a denial-of-service attack. This requires no computer skills but for the ability to use Google. Bot-agent design and bot delivery have become a commoditized service industry.[10] A small botnet is sufficient to launch an effective denial-of-service attack causing much damage, and costs as little as US$200 for a twenty-four-hour attack.[11] A person does not require any special computer skills to use a botnet to commit a crime. Figure 10 is a sample of the commercialization of denial-of-service attacks with a botnet. The customer would merely specify the targeted website to attack,

Figure 10. Denial-of-Service Attack as Commercial Service.[12]

pay a nominal fee of US$200, and a denial-of-service attack would be launched for twenty-four hours against the website.

Purchase Crimeware Kit with Botnet. Commercialization is also occurring within another context known as crime kits. In this instance, a person is able to purchase a copy of the botnet code in the form of a crime kit. The kit comes with a licence to use the botnet, and instructions. ZeuS, for example, is a popular crimeware kit that may be purchased for US$700.[13] Expert computer skills are not required for botnet usage. A criminal may elect to purchase a crimeware kit with simple instructions on how to execute an attack.

LOIC or Similar Software. The last botnet involves the free LOIC software program. LOIC is used for most of the denial-of-service attacks performed by members of Anonymous. Figure 11 captures an image of LOIC executing a denial-of-service attack against PayPal. Use of LOIC requires minimal computer skills. One googles LOIC, downloads the software with a click, types in the URL (e.g., www.paypal.com), and presses start. The denial-of-service attack then commences and people join in from all over the world using LOIC.

Differentiating between these types of botnets has legal implications. In the instance of making a botnet, the botnet master would have had to acquire control over a user's computer without their authorization, thereby attracting cybercrime liability for unauthorized access, modification, or impairment to data. Hiring or renting a botnet also attracts similar criminal sanction. Using LOIC, however,

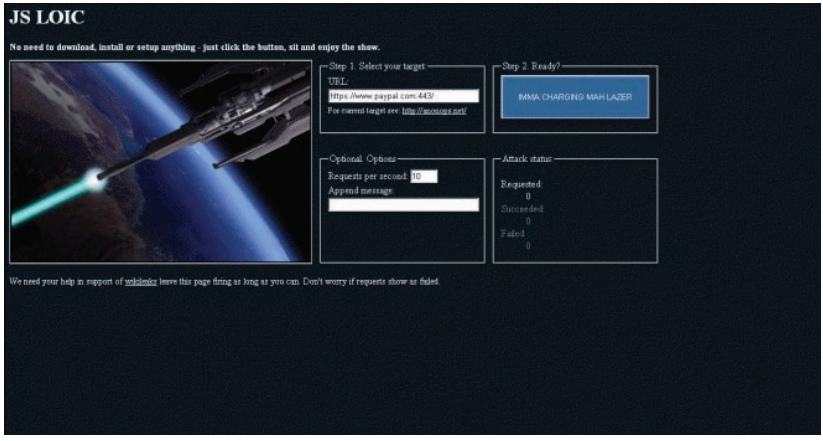

Figure 11. LOIC DDoS Attack Against PayPal.[14]

would not necessarily attract criminal sanction for unauthorized access. This is because users of computers connected to LOIC are doing so voluntarily. The issue of whether an attack involves unauthorized access as opposed to a form of legitimate civil disobedience is contentious, as will be illustrated in the case studies below.

Amplified Junk. To complicate matters further there is speculation that DDoS performed through services that merely amplify "junk" mail would not violate criminal law. Ragebooter is an example of this. In 2012, Ragebooter, a DDoS "testing service" came to surface. The company offered customers the ability to test how robust their systems were in relation to DDoS attacks. The service operates by taking the existing junk mail sent to the server then duplicating it, and then sending significantly more junk mail to the server. In this respect, the junk mail is merely amplified to the point where the server cannot handle the requests and returns an HTTP 503 error page. Essentially, the site's bandwidth is flooded so that it no longer functions properly.

Bandwidths may be flooded in many ways. For example, some web scrapers, such as Google, when retrieving information from websites may scrape too much too quickly, resulting in the overuse of bandwidth, rendering the site unavailable. In another example, when Australia did its first online census, in 2016, they did not anticipate that most people would log-on to complete the census within a narrow band of time; thus, the server's bandwidth was flooded, causing the system to crash. Systems like Ragebooter, however, are set up to deliberately crash a server or system.

In 2013, the journalist Brian Krebs investigated the legality of the Ragebooter service being offered by the site's creator, Justine Poland, uncovering some interesting findings. One of which was that Poland had links with the FBI.

> They allow me to continue this business and have full access. The FBI also use the site so that they can moniter [sic] the activitys [sic] of online users. They even added a nice IP logger that logs the users IP when they login.[15]

Ragebooter proclaimed itself as a "legal testing service," but an investigation by Krebs revealed that the site was being used to launch DDoS attacks outside of legal testing. It is unknown if the site has been used for ethical-hacking purposes, but it remains a strong

possibility, especially if you consider that Poland has gone on record as saying "I also work for the FBI on Tuesdays at 1pm in Memphis."[16] Poland did in fact work one day per week for the FBI, and allowed the FBI to use the site to monitor users' online activities. Ragebooter is one of several similar so-called stress-testing services. Others include Vastresser.ru and Asylumstresser.com. The legality of the service is questionable. From a purely technical perspective, there might not be unauthorized access—junk mail already sent to the server is merely amplified. One would be inclined to think, however, that the intent behind the amplification of junk mail would be a factor in deciding to prosecute. How successful a prosecution might be remains to be seen.

There are also many services that mitigate DDoS events. Cloudflare, for example, is a content-distribution network that protects sites against DDoS attacks. Cloudflare is also used by sites such as Ragebooter and Asylumstresser to shield DDoS attacks. Curiously, the site could be used for ethical-hacking websites or other sites that promote human rights, or that encourage civil disobedience or dissident groups. As will be seen in the case study on a hacktivist and hackback event involving Anonymous, Julian Assange, and MasterCard, Cloudflare was used successfully by Anonymous to thwart counter-DDoS attacks (ch. 8 and 10).

7.2 Timeline

A timeline of selected incidences from chapters 4 to 6 (which provides information about global incidences of online civil disobedience) is shown in figure 12. As you can see, issues of denial-of-service attacks and website defacements have been reported in North America, Europe, China, Russia, and the Middle East. As you will see, you may question how some of these incidences would be deemed "ethical." In fact, many of these incidences could conceivably fall within the parameters of vigilantism, such as the defacement of the *New York Times* website, reportedly related to a book about hackers by a *Times* reporter. Other incidences are clearly within the online protest space.

Figure 12. Online Civil Disobedience Timeline.

7.3 Case Studies

Three case studies using DDoS are explored and contrasted below. They have been specifically selected because they highlight different methods of protest, which, in turn, produced different legal outcomes. These three case studies are Anonymous's Operation Titstorm, in Australia; the German Lufthansa online protest; and the Canadian Twitter campaign #Vikileaks.

7.3.1 Anonymous, Operation Titstorm

In 2010, the Australian government sought to introduce a mandatory internet filter. This was unofficially referred to as a "clean feed" proposal. Internet filtering in this context would mean requiring Internet-service providers (ISPs) such as Optus, Telstra, and iiNet to implement technical means to filter out a set list of illegal websites, most notably websites with images of child abuse and child pornography, but also, potentially, websites about abortion or pornographic images. Internet-filtering techniques are commonly used in authoritarian regimes such as China and Iran, as well as in Western democracies such as Canada, the United Kingdom, France, and Sweden. Although Australia would not have been the first country, authoritarian or democratic, to implement internet filtering, the proposed filtering system has many unique features, separating it from other jurisdictions.

For instance, Australia would have been the first Western democracy to mandate internet filtering through formal legislation. ISPs would have been legally required to block "unwanted" material. In countries such as France, Belgium, and Germany, courts have mandated ISPs to block hate speech and illegal P2P file sharing of copyright-protected materials. In countries such as Canada and the United Kingdom, informal government pressure led to voluntary internet-filtering frameworks by the countries' major ISPs.

There was no Australian legislation on internet filtering at the time (2010), just the proposal; therefore, the prospective consequences were vague. The criteria for the evaluation of websites to be blocked remained equally uncertain and ambiguous. As it stood, the clean-feed proposal had two tiers. The first tier—blacklist filtering—was not controversial. The second tier—content filtering—was.

1. *Blacklist Filtering:* The first tier was an Australian Communications and Media Authority (ACMA)–issued blacklist of "child pornography" websites and "other prohibited" materials to be blocked by ISPs at the URL level. The scope of "other prohibited" materials was unknown. This would be mandatory for all Australians with no ability to opt out of the scheme. Circumvention of the blacklist would have been illegal. The blacklist would only block those URLs found on the ACMA blacklist. It would not have blocked

websites with child pornography and other prohibited content as found on:

- P2P systems (e.g., BitTorrent, Winnie),
- encrypted channels,
- chatrooms,
- Microsoft's MSN messaging service,
- mobile phones, and
- other websites, as it was unknown whether a blocked URL would block every website operating on a domain name or merely the specific offending material (e.g., www.youtube.com versus a specific video on YouTube).

2. *Content Filtering:* The second tier was intended to block types of materials which were legal but potentially unwanted. The scope of such material had not been delineated, but examples would likely have included adult pornography and other "R"-rated material—material inappropriate for children but clearly legal for adults. The advocacy group Australian Christian Lobby indicated that they wanted many forms of pornography filtered, regardless of whether they were legal or not. What types of filtering techniques to used was undetermined. Potentially, these could have included URL blacklists, deep packet inspection, P2P content inspection, and URL- and http-content inspection. Users would have been able to opt out of content filtering, as well as legally circumvent this type of filtering.

There were a number of off-line, marching protests in response to the Australian government's decision to introduce a mandatory filter, with protest signs in Canberra and online acts of protest. Many websites and ISPs participated in "Black Australia," wherein they blackened their websites as a form of protest against censorship.[17] One of these online protests was the online defacement and DDoS attack of the Australian parliamentary website, in 2010.

The Anonymous operation was dubbed Operation Titstorm (see fig. 13). The operation saw the parliamentary website taken down and images of penises and breasts were splashed on the parliamentary landing page for the website. Australia has a long history of both censorship and opposition to censorship. Unlike Canada, the United

Figure 13. Advertisement, Operation Titstorm.

States, and many parts of Europe, in Australia human rights are not constitutionally protected.[18] The courts in Australia have less ground to strike down legislation that infringes civil liberties. Emphasis is, therefore, placed on protesting policy proposals and bills before they become acts of parliament.

Figure 13 reproduces the global advertisement of the protest. Communications about the event could be found on IRC channels, on websites, and on social media. Dedicated websites were listed, whereby people could participate in DDoS in a variety of ways, such as using their own botnet, hiring a botnet, or sending individual requests to the parliamentary website server, but most popular was the use of LOIC to participate in the attack.

As evidenced in the figure, participation was not limited to Australians. The campaign sought participation from anywhere.

Matthew George was an Australian member of Anonymous who participated in Operation Titstorm by using the LOIC software. He was charged and convicted of incitement. A magistrate stated that George had incited others to attack government websites, and went so far as to liken his activities to cyber terrorism—a claim that is truly outrageous given the context of the protest. George was given a $550 fine. George was not a ringleader but merely a participant, using LOIC software. Furthermore, he did not deface the government

websites; he merely participated in a coordinated DDoS protest against the government. As George told the *Sydney Morning Herald*,

> We hoped to achieve a bit of media attention to why internet censorship was wrong...
>
> I didn't think that I would ever get caught. I was actually downloading connections from other computers in America, so I didn't think the Australian government would be able to track me down.
>
> I had no idea that what I was doing was illegal. I had no idea that there was incitement and it was illegal to instruct others to commit a legal [sic] act.[19]

The above represents an underlying theme, whereby many DDoS protest participants do not realize that they are participating in an illegal activity. This can be clearly contrasted, as will be seen in chapter 5, to participants in hacktivism when they know that they are breaking the law but continue to do so as a form of activism. In other words, hacktivists know that what they are doing is illegal and they continue to do so for ethical reasons. With online civil disobedience, the line of legality is not clear, and participants do not always realize that they are engaging in illegal activities. They assume that a virtual sit-in or denial-of-service attack is a legitimate form of protest, similar to picketing, barricading, and physical sit-ins.

Meanwhile, many users of the LOIC software are unaware that the software provides no anonymity, even when they are participating in an act under the umbrella movement Anonymous. Many of the arrests of members of Anonymous who participated in other operations, as was seen in chapter 5, were LOIC users, but they often went further in their protest, such as in defacing a website. Hacktivism as defined in this book typically requires proficient computer skills and involves more than the ability to use LOIC.

7.3.2 German Lufthansa Protest

In 2001, two civil-rights activist groups, Libertad and Kein Mensch ist illegal (No One Is Illegal), had called for protests against Lufthansa for their policy of helping to identify and deport asylum seekers. There was an off-line protest at the Lufthansa shareholders' meeting.

This was met with an online protest. The online protest consisted of a DDoS attack where over 13,000 people participated, shutting down Lufthansa's server for two hours (this is pre-LOIC).[20]

One of the protest organizers, Andreas-Thomas Vogel, was convicted of coercion by a German regional court. On appeal, a higher court found that there was no coercion under section 240 of the German criminal law. They reasoned that there was no violence or threatening behavior. Further, the court reasoned there needs to be a permanent and substantial modification of data to be deemed guilty of an incitement of alteration of data. The court viewed the DDoS attack as a modern form of non-violent blockade, one fully within the right to freedom of expression. In Australia, a similar attack attracted comments from the court as falling within terrorist activity, with no mention of freedom of expression or freedom of assembly.

7.3.3 Twitter #TellVicEverything Campaign

In 2012, the Canadian government introduced a lawful-access bill, known as Bill C-30, that would require ISPs to monitor and store a range of communications data about its users. Canadians took to both off- and online means to protest the surveillance bill, which the government called the Protecting Children from Internet Predators Act, including signatures to the "Stop Spying" petition, letters to Members of Parliaments, and a unique Twitter campaign. The minister of public safety, and the person responsible for introducing Bill C-30, Vic Toews, had been publicly vocal about standing with the government against child pornographers, and was actively using Twitter. Canadians responded with the hashtag #TellVicEverything, whereby hundreds of thousands of Canadians sent tweets to Toews's account, telling the minister about all sorts of mundane events in their life, such as "I flushed the toilet," "my dog barked," "I had cereal for breakfast," and so forth; it was a rather humorous protest.[21] While there were record-breaking Canadian-based Twitter peaks for the campaign, no server was crashed. This was not a DDoS. However, had the same traffic been amplified to the Canadian Parliament's website, or to Toews's email, these services would likely have been overloaded. Sending tweets is a legal form of online protest. Sending requests directed at a server, even if in protest, is a DDoS attack. This is illogical and, as will be seen in chapter 10, likely a contravention to the Canadian Charter of Human Rights and Freedoms.

7.4 Observations

Online civil-disobedience participants are motivated by the same reasons as participants in traditional off-line acts of civil disobedience. For example, a sit-in may have similarities with virtual sit-ins. Barricades with denial-of-service attacks and website redirection. Political graffiti may be aligned with website defacements. Wildcat strikes might also be similar to denial-of-service attacks and website redirection. Site parodies, blogs, social-media protest posts are similar to underground presses. Petitions exist both off- and online.

The motivation is derived from a strong desire to protest that which is seen to be immoral, corrupt, undemocratic, and, above all, to send a strong message to ensure transparent governance. There is a strong link between the protection of civil liberties and online civil-disobedience activity.

The main targets are often the websites and databases of governments and organizations linked to government, including departments of defence, intelligence agencies, and law enforcement. The other main target is organizations that are viewed as corrupt.

The main relation between motivation and targets is perception of the target behaving immorally. In many instances "immoral" means infringing civil liberties, whether this be freedom of the press, freedom of expression, or privacy. Police brutality is another common link between target and motivation. There are many videos of police brutality that are shown in Anonymous, LulzSecm and CabinCr3w Twitter feeds. For instance, there is a video on CabinCr3w's Twitter, from January 3, 2012, showing the beating of a fifteen-year-old boy by Harris County police in Texas after the accused had turned himself in.[22] The video can no longer be found on Twitter or any other messages on Twitter by CabinCr3w. This may have something to do with the subpoenas to Twitter to ascertain the identities of members of CabinCr3w who were arrested and jailed. The Texas court later blocked the viewing of the video but community activist Quanell X legally acquired access to the video which was later aired on television channel ABC. In other instances, "immoral" is a combination of violation of civil liberties as well as more severe instances, where perceived "tyrant" governments stand in the way of democracy.

With the case of Operation Titstorm, the convicted Matthew George stated that it was his first and last experience with online protests. Arrests of LulzSec members in the United States and the

United Kingdom has had the opposite effect. Other members of the group, as seen in chapters 5 and 8, have met the arrests with counterattacks on law-enforcement databases and any organization which they see as having aided in the arrest of these individuals. It is important to note that companies such as Twitter have fought court orders to reveal account details and other information about their clients. Twitter has been taken to court on many occasions to assist with the revealing of identities behind accounts, such as those of WikiLeaks supporters.[23] Further, academics from around the United States appeared in a US Senate hearing in January 2012 to give evidence of the acute lack of transparency in the American regulation of Internet matters, where they expressed their concerns about a growing surveillance state.

The issues with online civil disobedience are in many ways the same issues with off-line civil disobedience. One commenter asks, "If a building is blockaded by protestors, is it civil disobedience or infringement on freedom of assembly? Is a book burning activism or censorship? Are causes more important than rights?"[24] There have been a paucity of cases addressing the issue; therefore, the issues are very much open for debate. Critical mass is important as to which causes get taken up. Which causes are taken up by a critical mass remain unpredictable, but perhaps not for long. Social-media data and data on the surface Web are routinely used to feed into big-data algorithms that allow governments or corporations to use machine learning to perform predictive analytics—such predictive analytics could in theory predict which events or incidences are likely to attract activism.

Notes

1. SQL: Defacing a website involves the insertion of images or text into a website. This is often done via a SQL injection. A SQL injection is an attack in which computer code is inserted into strings that are later passed to a database (see Security Spotlight 2010). A SQL injection can allow someone to target a database giving them access to the website. This allows the person to deface the website with whatever images or text they wish.
2. DNS hijacking allows a person to redirect web traffic to a rogue domain name server (Security Spotlight 2010). The rogue server runs a substitute IP address to a legitimate domain name. For example,

www.alanna.com's true IP address could be 197.653.3.1 but the user would be directed to 845.843.4.1 when they look for www.alanna.com. This is another way of redirecting traffic to a political message or image.

3. Adware refers to any software program in which advertising banners are displayed as a result of the software's operation. This may be in the form of a pop-up or as advertisements displayed on the side of a website such as Google or Facebook.
4. Phishing refers to the dishonest attempt to obtain information through electronic means by appearing to be a trustworthy entity.
5. Ransomware is a type of malicious software that prevents the user from accessing or using their data (often through encrypting the data) where a fee must be paid or service performed before the user's data is decrypted).
6. DDoS is the most common form of online civil protest. A denial-of-service attack is distributed when multiple systems flood a channel's bandwidth and/or flood a host's capacity (e.g., overflowing the buffers). This technique renders a website inaccessible.
7. A botnet is a collection of compromised computers that are remotely controlled by a bot master.
8. The cloud is a term for web-based applications and data-storage solutions. Companies such as Google, Microsoft, Yahoo, and Amazon are among the many companies that offer cloud computing services for individuals, corporations, and governments to store and access their data online, on the cloud (Soghoian 2009).
9. The IoT refers to "the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these things to connect, collect and exchange data" (Wikipedia, "Internet of Things"). IoT sees traditionally non-Internet-connected devices or objects becoming connected to Internet-connected devices in a network, thereby rendering such devices or objects monitorable and controllable.
10. Ollmann 2010.
11. Ollmann 2010.
12. Image from Ollmann 2010.
13. See Trend MICRO 2010.
14. Image from Poulsen 2013.
15. Krebs 2016.
16. Krebs 2016.
17. Moses 2010.
18. Cook et al. 2011.
19. Whyte 2011.
20. Bendrath 2006.
21. CBC News 2012.

22. See http://twitter.com/#!/search?q=%23CabinCr3w. This link has been removed from Twitter. The video of the beating can now be found on news websites such as https://www.youtube.com/watch?v=Doh_gGIzuHQ (February, 2011).
23. Shane and Burns 2011.
24. Thomas 2001.