CHAPTER VIII

Hacktivism

8.1 Hacktivism in Context

Hacktivism was defined as the clever use of technology that involves unauthorized access to data or a computer system in pursuit of a cause or political end. Hacktivism is more than the online equivalent of sit-ins and protesting, acts of online civil disobedience. Hacktivism involves hacking for a cause, often political; however, hacktivism takes that one step further, such as in the collection and disclosure of personal emails, or even of extortion or blackmail for a political cause.

Common forms of hacktivism include information theft (e.g., copying emails, account information, government documents, credit-card information; hacking the viewing habits of Internet users—especially if criminal, e.g., child pornography), virtual sabotage (SQL injection whereby content on the website is replaced with the content of the attacker), insertion of a back door, or manipulation of software development.

It is often assumed that incidents of hacktivism and online civil disobedience are done in order to attract media attention to a cause. While that is true in many incidents, there is also a growing movement of silent activists who view the current political landscape as a long-term information war.[1] When security vulnerabilities are found in government and corporate databases, the information

is kept secret. They are not looking for media attention, but wish to ensure that there continue to be back doors available toward accessing information. In some instances, software or hardware is purposefully developed with a back door included in its coding. In this instance, the software company and contractor are not aware of the default in the product (e.g., surveillance software used by governments and corporations). This type of insertion of a deliberate vulnerability is performed by security experts working in the field. Their active participation in hacktivism is not publicized. They do not seek media attention and there is no media reportage on their activities. Their goal is to fly under the radar. They possess the highest level of computer skills. This type of hacktivism has a particular focus on information related to democracy—censorship, surveillance, and military action.

Software development is another critical form of hacktivism. The technologies used in WikiLeaks, for example, ensure the integrity of the document and the anonymity of the informant. Additionally, WikiLeaks has developed technology that allows people in non-democratic jurisdictions such as China a way to access their otherwise filtered content. Other hacktivism technologies include anonymizers such as the Tor which allow people to view online content anonymously, and browser extensions, such as DoNotTrackMe and TrackMeNot, that block Internet trackers as well as data mining.

8.2 Timelines

Figures 14 to 17 present four timelines which capture select incidences of hacktivism, along with the evolution of Anonymous, the CCC, as well as other hacking groups.

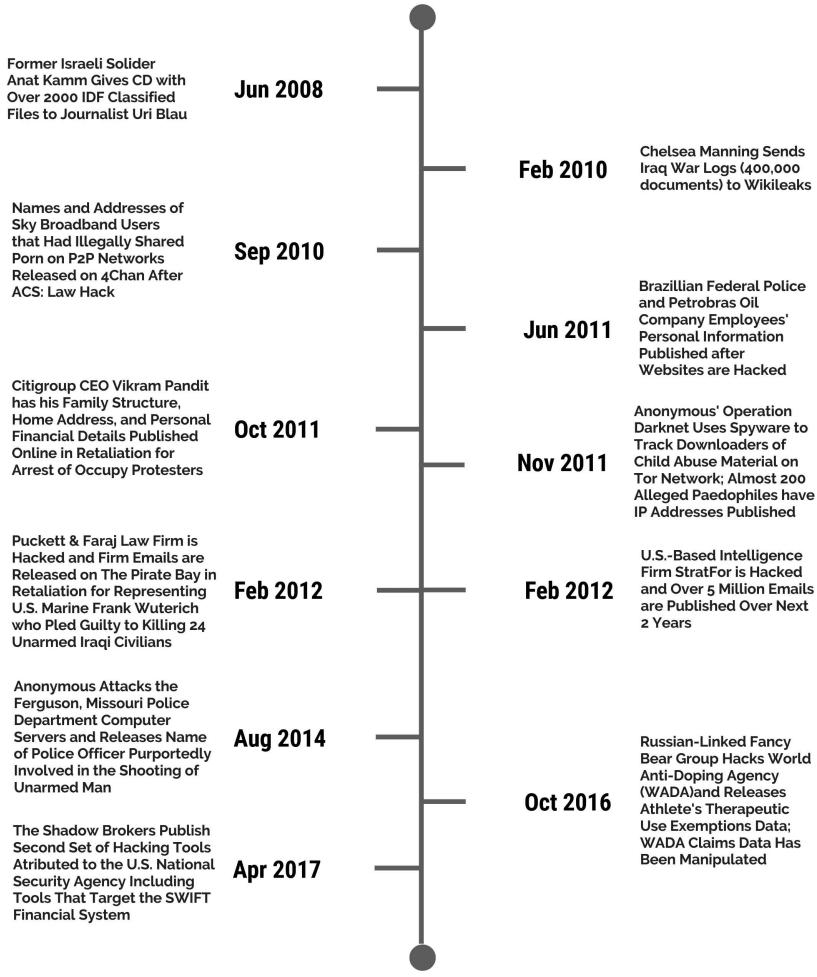

Figure 14. Hacktivism.

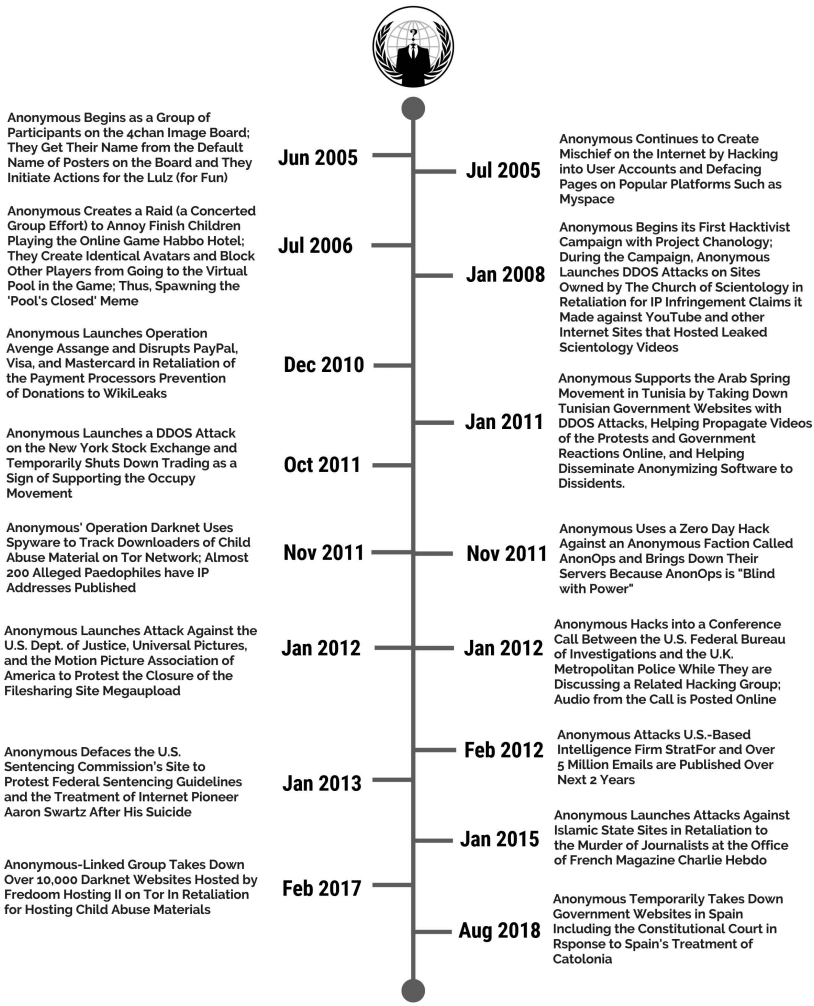

Figure 15. Anonymous.

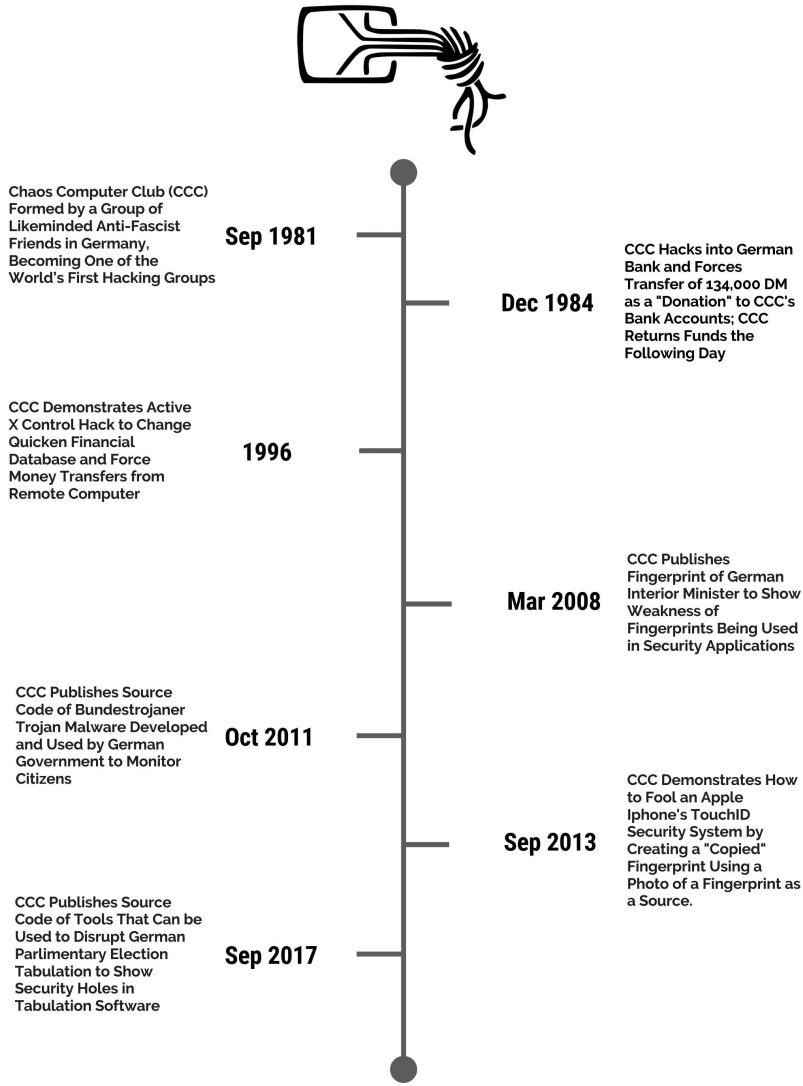

Figure 16. Chaos Computer Club.

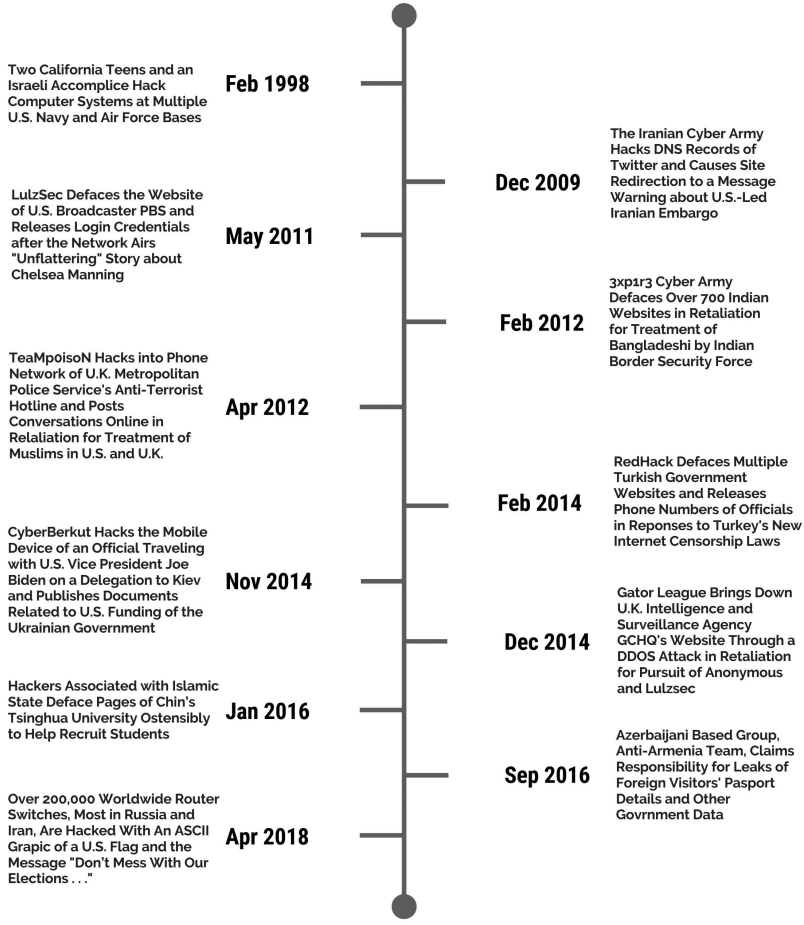

Figure 17. Other.

8.3 Case Studies

There are many instances of online civil disobedience spilling into hacktivism.

There are thousands of incidences, as was seen in chapters 3–6. Three of the most interesting examples, however, are the Christmas charity donation drive by Anonymous and the exposure of key officials linked to the neo-Nazi movement in Europe.

8.3.1 Anonymous, Post-Christmas Charity Donations

The 2011 post-Christmas Anonymous attack targeted credit-card information of the clients of US-based security think tank Stratfor. In

this instance, members of Anonymous were able to access and steal credit-card numbers of Stratfor clients. Clients included members of intelligence agencies, law enforcement, and Fox News journalists. The credit-card numbers were later used to give money, as Christmas donations, to charities such as the Red Cross, Care, and Save the Children.[2]

According to Anonymous postings, the personal information, credit-card details, and emails of Stratfor were not encrypted. This echoes a reoccurring theme of poor and sub-par security practices of large corporations, governments, and even security-minded think tanks entrusted with sensitive data.

8.3.2 Neo-Nazi Website

Anonymous claimed responsibility for an attack on a neo-Nazi website in Finland. Website members had their information stolen and publicly released. The list of members included a parliamentary aide who later resigned from her post. It was later reported that Anonymous had issued a statement, which read, in part,

> We have no tolerance for any group based on racial, sexual and religion discrimination as well as for all the people belonging to them and sharing their ideologies, which is the reason why we decided to carry out last Monday's attack.

Similar types of attacks have been launched to reveal membership of paedophilia groups and organized-crime cartels.

8.3.3 WikiLeaks, Operation Payback

WikiLeaks founder Julian Assange was arrested in London in connection to charges of sexual assault under Swedish law, which sought his extradition. Many viewed this as a false arrest and an indirect way of incarcerating Assange for the release of secret US cables to WikiLeaks. A legal defence fund was quickly established where people could make donations via MasterCard or PayPal. However, MasterCard and PayPal disallowed payments to the Assange defence fund, causing an international uproar, in particular within hacktivism communities.

Members of LulzSec launched a denial-of-service attack against MasterCard and PayPal, which took down their capabilities in December 2010 and then again in June 2011. As will later be seen in chapter 10, there was a denial and counter-denial-of-service attack showdown, which might best be seen as gunfire between warring

factions, with evidence that the US government contracted security firms to perform attacks against WikiLeaks and other journalists. Protest/attack was met with counterattack.

The story becomes much more complicated, and is the type that attracts conspiracy theories and movie scripts. Hacktivist Jeremy Hammond leaked millions of emails by Stratfor to WikiLeaks. The emails revealed disturbing evidence of the corruption in Stratfor, including insider-trading techniques, coercive methods, and off-shore share structures. Revealed emails showed Stratfor's web of informers, pay-off structure, payment-laundering techniques, and psychological methods. Also, the emails revealed its confidential and corrupt connections with large corporations such as Dow Chemical, Lockheed Martin, Northrop Grumman, Raytheon, and governmental agencies including the US department for Homeland Security, the US Marines, and the US Defence Intelligence Agency. One example included emails that revealed secret cash bribes. and Hammond, from Chicago, did what he did to unmask unlawful surveillance and intelligence-gathering efforts—a controversial topic, certainly, but a trend in most countries across the world.

Hammond's motivation is clearly what he perceives to be ethical:

> I felt I had an obligation to use my skills to expose and confront injustice—and to bring the truth to light…. I have tried everything from voting petitions to peaceful protest and have found that those in power do not want the truth exposed…. We are confronting a power structure that does not respect its own systems of checks and balances, never mind the rights of its own citizens or the international community.[3]

Hammond was arrested and charged with conspiracy to violate the Computer Fraud and Abuse Act, in violation of 18 U.S.C. section 1030(b), for a cyber attack in June 2011 on computer systems used by Arizona Department of Public Safety.[4] Hammond pleaded guilty but was quick to refer to claims that the US government, through the FBI, directed his attacks on foreign websites.[5] The leaked emails included emails from the case judge's husband to Stratfor. Further, Hammond has stated that "The government celebrates my conviction and imprisonment, hoping that it will close the door on the full story. I took responsibility for my actions, by pleading guilty, but when will the government be made to answer for its crimes?"[6]

8.4 Observations

There is no singular motivation at the heart of hacktivism. The motivation of such players may often not be well articulated, if articulated at all. There are, however, some reoccurring themes among many hacktivism activities. At the heart of all hacktivism is a sense of some sort of moral wrongdoing that either needs to be exposed and/or needs to be punished, and a wider sense of public loss of confidence in their institutions.[7] Many hacktivism activities expose corruption and/or humiliate the establishment.

Some hacktivists are motivated to expose the insecure practices of corporations and governments handling personal information, as seen in the Sony and Stratfor incidences.

Most hacktivism, however, is related to a political cause. For example, many hacktivists are motivated by exposing censorship and surveillance of individuals by governments and corporations. WikiLeaks, for example, has posted documents outlining the surveillance activities of governments around the world. Secret filtering blacklists of websites blocked by ISPs on behalf of governments frequently find their way to the Internet. Other hacktivists target oppressive governments and enable the free flow of information in and out of areas where media coverage and access to local and foreign press is restricted. These include areas in Iran, China, Egypt, Syria, Libya, and include more local venues in recent Occupy movements around the world. Other hacktivism efforts target child-pornography websites and both the ISPs that host such repugnant content and the customers of this material. Religions such as Scientology have also been targeted with claims that such groups disseminate misinformation and have a corrupt hand in the lobbying efforts of US governments.

Hacktivism and online civil disobedience are linked to empowerment and the strongest desire to find an effective public voice. This also applies equally to social-media movements, including online petitions. The motivation of much hacktivism is closely linked to whistle-blowing. Generally, critical mass is important in determining which causes get taken up. In this sense, it is very democratic. Hacktivism is not anarchy nor does it have a top-down leadership which steers its course. Critical mass is required, and generally speaking, the stronger the cause, the more likely hacktivism activity will be seen as ethical. Equally important, however, is

predictability. Suelette Dreyfus, who is a researcher in both hacking, hacktivism, and whistle-blowing, indicates that hacktivism targets are not predictable. Which causes are taken up by a critical mass remain unpredictable.

As is the case with online civil disobedience, the main targets are the websites and databases of governments and organizations linked to government (e.g., Stratfor), as well as organizations that are viewed as corrupt or who are linked to corrupt organizations.

The main relation between motivation and targets is similar to online civil activism 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. Surveillance, intelligence gathering and contracting security firms to discredit hacktivist groups is currently a strong motive. In other instances, "immoral" is a combination of violation of civil liberties as well as more severe instances where tyrant governments stand in the way of democracy.

Many operations by LulzSec, however, are difficult to qualify as ethical hacking when the release of innocent third-party personal information is disclosed on the Internet, and no motive other than "just for the laughs" is apparent in many LulzSec attacks.

Principles in hacktivism parallel those in online civil disobedience. When Anonymous member Barrett Brown (former journalist and founder of Project PM, an online collective investigating the world of intelligence agencies) was asked to comment on television whether the activities of Anonymous were ethical, he encouraged the public to make a comparison chart. Chart what is good versus what is bad about each Anonymous Operation, then compare it with the issue that Anonymous sought to bring attention to. In other words, compare it with the actions of the traditional institution. For example, the actions of hacktivists must be compared with Arabic states' governments trying to "turn off" the Internet and to control social media; the treatment of WikiLeaks after publishing controversial information and continuing to assert its right of free speech; the heavy-handed crackdown on the non-violent worldwide Occupy movement by various local and national governments; and the lack of law around the shutting off of critical payment services, as in the case of MasterCard and PayPal. Conversely, many hacktivism activities run the risk of being perceived as immoral, especially when the personal information of innocent parties is released online.

Transgressive forms of hacking may be viewed as illegal yet ethical. It remains to be seen whether in ten years' time these same forms of transgressive hacking will become a legal part of the civil-disobedience landscape.

Unlike many people who participate in online civil disobedience, participants in hacktivism are well aware that their actions are not legal and take precautions to ensure their anonymity online. As has been seen with online civil-disobedience groups, many participants are unaware that using software such as LOIC to take part in a denial-of-service attack is illegal; they assume that such is a lawful form of protest. When hacktivists hack, copy, view, and disclose the personal information of others they are clearly aware that their actions are illegal and they have taken a calculated risk, despite the threat of criminal sanction.

Historical evidence shows that some hackers who are caught and later convicted of conspiracy or unauthorized use will either give up such activities or use their talents in a legitimate matter, such as working as a security expert or in some form of technology field. This is well documented in Dreyfus and Assange's interviews with hackers in *Underground*. Raol Chiesa's work in *Profiling Hackers* also notes that the law offers deterrence to younger hackers (script kiddies) but not to other levels of hacking. Both studies, however, reveal that the law offers no deterrence to future generations of hackers; the deterrence value is only individualized and is limited to the person who has been charged with a crime. Criminal prosecutions and convictions fuel the underworld of hackers, have the sole effect of driving the hacking world further underground, and have led to the development of many obfuscation technologies that make traceback to the source of an attack difficult (see ch. 12). As Dreyfus and Assange note, prosecutions and convictions have not sent a message of "don't hack" but, rather, of "don't get caught."

Many of the studies that have been done to date, however, have been about hacking in general and not about ethical hacking. It is not known whether the prosecution and conviction of ethical hackers will act as a deterrent, sending the message "ethical hacking is wrong," or whether such prosecutions will act as a catalyst to even more ethical hacking as a sign of protest. When members of Anonymous were arrested in the United States, there were a series of attacks of law enforcement, news channels (Fox News), and university websites as a form of public protest. Similar attacks were

performed on security firms who contract with governments and corporations to attack Anonymous, LulzSec, and WikiLeaks. This is explored further in chapter 10.

At the heart of all hacktivism is a sense of some sort of moral wrongdoing that either needs to be exposed and/or needs to be punished, and a wider sense of public loss of confidence in their institutions—even if the actions of LulzSec are poorly articulated, if at all (the membership of this group seems to be confined to young males, unlike the membership of Anonymous, with participants of all ages and walks of life).

Hacktivism and online civil disobedience are linked to empowerment and the strongest desire to find an effective public voice. This equally applies to social-media movements such as online petitions.

The motivation of much hacktivism is closely linked to whistleblowing, which is discussed further in chapter 13.

Notes

1. As do WikiLeaks members; see, e.g., Pilger 2011.
2. R. Adhikari, "Anonymous Implicated in 'Robin Hood' Hack on Christmas Day," *Tech News World*, December 27, 2011, available at https://www.technewsworld.com/story/Anonymous-Implicated-in-Robin-Hood-Hack-on-Christmas-Day-74058.html.
3. Video released by Jeremy Hammond in November 2013 on YouTube. It has since been removed and is no longer retrievable via search engines Bing and Google, for example. But there are countless news article and blogs that have quoted Jeremy's speech.
4. *United States of America v. Jeremy Hammond*.
5. Pilkington 2013.
6. Pilkington 2013.
7. Interviews with Dreyfus and Samuel. Dreyfuss interivew, December 2010, Sydney Australia. Samuel, phone interview, December 2010. See also Chiesa, Ducci, and Ciappi 2009.