Hacktivism and the Government of British Columbia

Prepared by: Morgan Beach

Client: Information Security Branch, Office of the Chief Information Officer, Government of British Columbia

School of Public Administration
University of Victoria
2012
Disclaimer

Although intended for an academic and professional audience, there are instances within this report where explicit language is used. The inclusion of this language is not gratuitous, and is meant to accurately reflect the realities of hacktivist culture. It is by no means the intent of the author to offend any readers, and the use of any explicit language is used simply to provide context to this report’s discussion.
Acknowledgements

I would firstly like to extend a gracious thank you to Stu Hackett, without whom I would not have had the opportunity to write this report. His support over the last several months has been incredible. I would also like to thank Dr. James MacGregor and Dr. Henry Lee. Their encouragement, guidance, and expertise throughout the writing of this report has been beyond words, and I am truly grateful.
Executive Summary

Objective

The British Columbia (BC) government’s Information Security Branch (ISB) is responsible for establishing information security governance in BC, implementing information security policies for the Province, and promoting security awareness amongst the Province’s employees. As such, the ISB has an interest in reviewing the information security environment for emerging threats. One such potential threat is hacktivism, which has become increasingly prominent over the last few years. As a proactive measure, the purpose of this report is to analyse current trends within hacktivism and assess the likelihood that the BC government may be an attractive target for hacktivists.

The key research question for this report is: in consideration of current trends within hacktivism, to what extent may hacktivists consider the Government of BC an attractive target?

Methodology

In order to achieve the objectives of this report, the environmental scan methodology was used. The environmental scan methodology is a useful tool for improving organizational knowledge, and operates as an early warning system for potential threats that may exists in the external environment. For the purposes of this report, the environmental scan approach provides an effective method for reviewing and analyzing hacktivist threats to the BC government that may exist.

A range of data sources were used throughout the development of this report. Sources included academic journal articles, books, online magazines and news articles, blogs, government websites, and information made available by information security practitioners.

Key Findings

Because of the confrontational tactics that hacktivist use, coupled with the ambiguity about what hacktivism denotes, there is a great deal of disagreement amongst academics and security practitioners about what in fact constitutes a hacktivist attack. For the purposes of this report, hacktivism may be understood as the act of committing a cyber attack for the purpose of protesting, or drawing attention to, a social or political issue; without the intent to obtain financial benefit or grievously harm the target.

There are a number of groups today that are quite prominent within hacktivism, as defined by this report. These groups include the Anonymous collective, LulzSec, AntiSec, TeamPoison, and the People’s Liberation Front. Of these groups, the Anonymous collective is perhaps the most public and well-known. Some of the tactics used by these groups to commit cyber attacks may include website defacements, website redirects, distributed-denial-of-service (DDoS) attacks, and unauthorized data releases. Techniques to carry out these attacks include brute force attacks, SQL, pronounced sequel, and cross-site scripting (XSS) injections, and the use of programs to automate DDoS attacks. Interestingly, there is a great deal of uncertainty about whether or not
instances of hacktivism are in fact increasing. Speculative statements and overstated findings have all contributed to this ambiguity.

When hacktivist attacks do occur, it appears that they are triggered by changes to the status quo, or perceived instances where people’s rights and freedoms have been infringed upon. However, it is unclear why hacktivists have engaged in certain issues, while neglecting others. Nevertheless, many hacktivists have articulated a willingness to target government bodies in particular. The desire to target government organizations may come from their high profile in society, a general disdain for government bodies, or the view that all governments are intrinsically corrupt.

Implications of successful hacktivist attacks may include public embarrassment, a slight to an organization’s reputation, and costly data breaches. The overall effect of hacktivist attacks appears to depend upon the type of organization that is targeted, the tactic used to commit cyber attacks, and what, if any, information is compromised as a result of the attack. Interestingly, recent studies have suggested that the financial costs associated with data breaches may be decreasing. Nevertheless, hacktivist attacks can have an impact upon both the targeted organization and the individuals who have entrusted an organization to manage their private information.

Looking at recent instances of hacktivism, there appear to be a number of recurring themes that have triggered hacktivist attacks. As such, hacktivist attacks can be understood as typically aligning with one of seven categories: privacy concerns; perceived instances of censorship; alleged corruption; elections; wrongdoing on the part of law enforcement; retaliation for arrests of alleged hacktivists; and general contempt. Drawing upon this analysis, there appear to be issues within BC that could trigger hacktivist attacks against the BC government. Examples include censorship surrounding the Enbridge Northern Gateway Project review process, the perception that the BC government is a corrupt institution, the upcoming 2013 BC provincial election, the behaviour of law enforcement officers in BC, and general contempt for the BC government.

Despite this observation, there is nothing at this time to suggest that hacktivists have any intent to launch attacks against the Government of BC. While the reasons for this are not clear, it is possible that the BC government is simply not considered to be an attractive, deserving, or interesting target. Nevertheless, there is still the potential that hacktivists could target the Government of BC in the future. By affording proper consideration to the on-going contentious issues in BC, and recognizing the types of issues that have stimulated hacktivists, it is expected that the BC government will be better prepared to anticipate and mitigate the likelihood of successful hacktivist attacks in the future.

Regardless of whether or not the BC government is in fact facing impending attacks from hacktivists, it is essential that the BC government is proactive in its efforts to protect its information management (IM) and information technology (IT) infrastructure, and thus all information under its custody. The best security practices presented in this report include: investing the time and resources needed to regularly audit servers and conduct penetration tests of IM/IT systems; patch systems when vulnerabilities are discovered; develop a system for
classifying sensitive information; establish clear policies for how sensitive data should be managed; do not store sensitive data on public servers; encrypt all sensitive and private information; establish measures for mitigating the effects of DDoS attacks; establish requirements for strong passwords; temporarily lockout user accounts after predetermined number of failed login attempts; and make usernames more complex. The inclusion of these best security practices in this report however does not imply that the Province does not already have some or all of these practices in place.

Conclusion

While there may be issues in BC that could stimulate hacktivists into targeting the BC government, there is nothing at this time to suggest that there are any impending hacktivist threats to the Government of BC. By continuing to regularly review instances of hacktivism, and remaining cognizant of the policies and activities that could trigger hacktivist attacks though, it is expected that the BC government will be much more prepared to anticipate the likelihood of hacktivist attacks. By adopting this proactive approach, coupled with the use of best security practices, the BC government may be better prepared to guard against potential hacktivist attacks, and better protect the resources and information under its custody.

Recommendations

Overall, there are three recommendations provided in this report for how the BC government may improve its ability to anticipate and guard against hacktivist attacks.

1. **The BC government should continue to monitor trends within hacktivism.**

2. **The BC government should continue to periodically identify issues in BC that may attract the attention of hacktivists.**

3. **All areas within the BC government should be proactive about exercising best security practices for managing resources and information under their custody.**
Table of Contents

Disclaimer .............................................................................................................................................. i
Acknowledgements ................................................................................................................................. ii
Executive Summary .................................................................................................................................... iii
Definitions ................................................................................................................................................ viii
Figures .................................................................................................................................................. x
Chapter 1: Introduction .............................................................................................................................. 1
  1.1 Project client and objective ............................................................................................................. 1
  1.2 Rationale ......................................................................................................................................... 1
  1.3 Organization of report .................................................................................................................... 2
Chapter 2: Background .............................................................................................................................. 3
  2.1 Information Management and Information Technology .............................................................. 3
  2.2 Information Security ......................................................................................................................... 3
  2.3 Open Government ............................................................................................................................. 4
Chapter 3: Methodology ............................................................................................................................. 5
  3.1 Environmental scan .......................................................................................................................... 5
  3.2 Scope ............................................................................................................................................... 5
  3.3 Data Sources ..................................................................................................................................... 6
  3.4 Research Limitations ....................................................................................................................... 6
Chapter 4: Literature Review ..................................................................................................................... 7
  4.1 Introduction ....................................................................................................................................... 7
  4.2 Activism and cyber activism ............................................................................................................. 8
  4.3 Hacktivism conceptualized ............................................................................................................. 9
  4.4 Evolution of hacktivism ................................................................................................................... 9
  4.5 Hacktivist tactics .............................................................................................................................. 11
  4.6 Legal ambiguity ................................................................................................................................. 12
  4.7 Overlapping categories .................................................................................................................... 14
  4.8 Hacktivism: a definition ................................................................................................................... 15
Chapter 5: Hacktivism Background ........................................................................................................... 17
  5.1 Introduction ...................................................................................................................................... 17
  5.2 Technological development ............................................................................................................. 17
  5.3 Malware .......................................................................................................................................... 18
  5.4 DDoS attacks .................................................................................................................................. 21
  5.5 Website defacements and website redirects ................................................................................... 22
Definitions

1. **Antipiracy** – efforts to prevent or prohibit the free exchange of copyrighted materials, such as music or movies, online.

2. **Bandwidth** – a measurement of how much data a server is able to manage and transfer at any one time. Bandwidth is measured by how much data is transferred per second.

3. **Botnet** – a jargon term used for a computer system that has been infected by a malware program that allows a remote user to control the computer without an owner’s knowledge or consent. Another term that has been used to describe a botnet is a zombie computer.

4. **Cleartext** – unencrypted information.

5. **Cross-site Scripting (XSS) injection** – a hacking technique in which JavaScript is exploited, allowing an attacker to redirect or gain unauthorized access to a website.

6. **Cyber attack** – a deliberate attempt to compromise, infiltrate, or sabotage a computer system or network.

7. **Distributed-Denial-of-Service attack (DDoS)** – a form of cyber attack in which continuous requests are sent to a website with the intent of overloading a server’s bandwidth capabilities. If a server’s bandwidth capabilities are exceeded, the server will shut down and the website will temporarily become inaccessible. This type of attack relies upon multiple computers and multiple Internet connections sending requests simultaneously, and is often much more effective than an attack launched from a single computer. DDoS attacks can be carried out by both actual users and botnets.

8. **Firewall** – a computer program that defends a user’s computer or network from cyber attacks and other forms of unwanted online traffic.

9. **Internet Relay Chat** – an online chat protocol that allows users to communicate via the Internet in real-time.

10. **Lulz** – an adaptation of the acronym lol, which stands for ‘laugh out loud’.

11. **Malware** – broad terminology used for malicious software that is made for the sole purpose of infiltrating, manipulating, or damaging a computer.

12. **Meme** – a term used to refer to any cultural phenomenon that can be shared between persons. This can include, but is not limited to, trends, jokes, and ideologies.

13. **Moralfaggotry** – a derogatory term used within hacktivist and online culture to label cyber attacks that are committed for the purpose of good or morality, rather than simply for the fun of it.
14. **Phishing** – an attempt to defraud Internet users for the purpose of eliciting information such as usernames, passwords, or credit card details.

15. **Scriptkiddies** – an unfavourable term used within hacker culture to describe low-level hackers that use pre-fabricated hacking software and code, rather than writing their own, to carry out cyber attacks. The use of pre-fabricated software and code requires little technical knowledge on the part of the user.

16. **Server** – a computer system designed to host services for computer users connected to a network.

17. **Source code** – the programming code that is used to develop a computer program. It may best be understood as the blueprint for software, and is often regarded as an important piece of proprietary information.

18. **SQL injection** – a hacking technique in which SQL statements are input into a website’s script, and users are able to gain unauthorized access to an organization’s online databases. This type of hacking will only work against databases that use the SQL programming language.

19. **Uniform Resource Locator (URL)** – a text string used to identify a particular file or website on the Internet.

20. **Virus** – a common form of self-replicating malware that can transmit itself to other computers by attaching itself to a file or program.

21. **Website defacement** – the unauthorized modification of a website’s message or content.

22. **Website redirect** – the modification and redirection of a website’s uniform resource locator.

23. **Worm** – a self-replicating form of malware that can send itself to other computers, but does not need to attach itself to a file or program in order to do so.
Figures

Figure 1. Message displayed by the WANK worm ................................................................. 19
Figure 2. Dialogue box displayed by the InJustice virus ....................................................... 20
Figure 3. Dialogue box displayed by the Mari@mm worm .................................................. 21
Figure 4. Screenshot of the Low Orbit Ion Cannon program ............................................. 29
Figure 5. Screenshot of the tweet from the Anon_Central twitter account ......................... 34
Figure 6. Screenshot of the BART website defacement ..................................................... 42
Figure 7. Screenshot of the defaced Boston Police Department website ........................... 49
Figure 8. Screenshot of the defaced A3P website ............................................................... 52
Figure 9. List of best security practices .............................................................................. 66
Chapter 1: Introduction

1.1 Project client and objective

The British Columbia (BC) Government’s Information Security Branch (ISB) operates within the Office of the Chief Information Officer (OCIO), in the Ministry of Labour, Citizens’ Services, and Open Government. The ISB’s mandate includes the overall governance of the BC government’s information security policies, which are applicable throughout the Province\(^1\) (Province of British Columbia, 2011c, para. 2). In addition to the responsibility of ensuring that appropriate security programs, plans, and processes are in place, the ISB also works with the rest of the BC government and the Broader Public Sector (BPS) to promote security awareness amongst the Province’s employees (Province of British Columbia, 2011c, para. 2-3). As part of the ISB’s mandate to provide security support to the Province, the ISB also has an interest in reviewing the information security environment for emerging trends and security incidents. By conducting such reviews, it is expected that the ISB, and thus the Province, may be better able to improve its understanding of potential threats, and respond to the information security needs of BC appropriately.

The objective of this report is to discuss some of the emerging trends within hacktivism, which has increasingly gained the attention of the media and security practitioners over the last few years, and assess the extent to which hacktivists may consider the BC government an attractive target. This report is intended to improve the ISB’s awareness and understanding of hacktivist threats within the context of the BC government.

Research question: In consideration of current trends within hacktivism, to what extent may hacktivists consider the Government of BC an attractive target?

1.2 Rationale

As the BC government continues to develop its technology infrastructure, an increasing amount of information and support services have been made available online. Everything from job opportunities to medical coverage applications and remote workplace desktops have been made available online by the BC government. As a result of this growth, information and support services have become much more accessible. This growth has also increased the Province’s susceptibility to cyber attacks (Province of British Columbia, 2011b, p. 3-9). Activists, potential criminals, and other individuals within society now have a new avenue by which they may block access to government resources, protest government policies, or gain unauthorized access to governmental resources and information. In consideration of this, there is a growing expectation on the part of BC’s citizens, business partners, and employees that the BC government will take proactive measures to protect their information (Province of British Columbia, 2011b, p. 3-8). The BC government has recognized this expectation, and is mindful of the fact that the protection of personal information is essential to the continued trust of its citizens, business partners, and employees (Province of British Columbia, 2011d, p. 3).

\(^1\) For the purpose of this report, the Government of BC, the BC government, and the Province may be used interchangeably.
Although hacktivism is not a new phenomenon, instances of hacktivist cyber attacks have become much more pronounced over the last few years (Ferguson, 2008, para. 7). The motivations for these attacks vary, but often include social or political intentions. It is largely expected that the next few years will see an even greater number of hacktivist cyber attacks occur, particularly against government bodies (Harms, as cited in Acohido, 2012, para. 3; Yin, 2011, para. 14; Reidy, 2012, p. 1). Given the implications and possible ramifications of a successful hacktivist attack against the BC government, this is a topic that warrants the attention of those within the BC government who are responsible for managing and protecting information.

1.3 Organization of report

This report is comprised of ten chapters, including this introduction. In Chapter 2 the BC government’s information security and open government policies are reviewed, and an overview of information management (IM) and information technology (IT) development within the Province is provided. In Chapter 3 the research methodology used for this report is presented. Chapter 4 conducts a review of literature pertaining to hacktivism, with particular attention being paid to the disparate ways in which hacktivism has been defined, and provides the definition of hacktivism that will be used to guide this report. In Chapter 5 a history of hacktivism is presented, noting how the tools and issues popularized by hacktivists have developed since the late-1980s, while Chapter 6 discusses current trends within hacktivism. In Chapter 7, some of the current social and political points of contention in BC are presented, and the extent to which the BC government may be an attractive, and thus likely, target of hacktivists is discussed. Chapter 8 then presents a number of best security practices for mitigating successful cyber attacks. In Chapter 9 the report’s findings are summarized and final insights are offered. Chapter 10 provides recommendations for how the BC government may improve its ability to anticipate and guard against hacktivist attacks.

This chapter has provided an overview of the objective and rationale of this report, and how this report has been organized. The following chapter provides a review of IM/IT development within the BC government as well as the Province’s policies for information security and government transparency.
Chapter 2: Background

2.1 Information Management and Information Technology

The expansion of the BC government’s IM/IT infrastructure has afforded the Province’s employees greater workplace flexibility, and its citizens improved access to information and support services. Online resources, virtual desktops, remote email access, and the move towards cloud computing are just some of the ways that the BC government is, or will be, providing improved online access to resources (Province of British Columbia, 2011b, p. 2-25). In its Being the Best 2010/11: human resource plan, the Province expressed the understanding that improved technologies and tools will improve the quality and accessibility of online resources, which is of benefit to both employees and citizens (Province of British Columbia, 2010, p. 11).

As the Province expands its online resources and increases the amount of information that it stores electronically there will be a growing number of touch-points, online points of access, which may be vulnerable to cyber attacks (Province of British Columbia, 2011b, p. 3-9). The increased use of IT to store information increases the likelihood that a growing amount of data may be compromised in the event of a successful data breach (“With new tactics,” 2011, para. 9). The Province has recognized the need for the development of its IM/IT infrastructure to be complemented by enhanced security capabilities and improved information security awareness amongst employees (Province of British Columbia, 2011c, p. 2)

2.2 Information Security

In 2005 the International Organization for Standardization (ISO), an international group that is comprised of 163 member countries, developed an international standard for how information security should be managed. It is upon this international standard that the BC government’s Information Security Policy (ISP) is based. This ISP is applicable throughout the Province, and establishes an array of guidelines and requirements for how information assets should be protected and managed.

The management and security of information is recognized as a key responsibility of the BC government (Province of British Columbia, 2011a, s. 12.2.1). Section 30 of British Columbia’s Freedom of Information and Protection of Privacy Act (FOIPPA) (1996) establishes that the BC government is responsible for protecting all records and information under its control, and has a legal responsibility to ensure that reasonable security arrangements are in place. In the event that there is an information security breach or an unauthorized disclosure of personal information, an employee of the Province is legally required to report the incident to the proper authorities (Freedom of Information and Protection of Privacy Act, 1996, s. 30.5(2)(2)). In the event that a person commits a security breach, or fails to reports one, a financial penalty may be issued.

---

2 ISO 27002:2005
2.3 Open Government

As the BC government continues to develop and expand its IM/IT infrastructure, it is also using new technologies to promote transparency and openness within government, and increase the ability of citizens to access government records (Province of British Columbia, 2011c, p. 6; Province of British Columbia, 2012b, para. 2). The goal of the open government initiative is to engage citizens in the decision-making process, demonstrate that government does not have hidden agendas, and promote the notion that the BC government is accountable to the general public (Province of British Columbia, 2012a, “About,” para. 1).

Key aspects of this initiative include the BC government’s *Open Information*[^3] and *DataBC*[^4] websites. These resources allow the broader public to access a great deal of information online, including thousands of datasets, Ministers’ travel expenses and pay levels, and Freedom of Information (FOI) requests that have previously been made. It should be noted that these strategies do not replace the right of BC’s citizens to request records under FOIPPA, but are only intended to supplement the FOI process (Province of British Columbia, 2012b, para. 5). The proactive efforts of the BC government to promote open government have even been recognized nationally. In both 2011 and 2012 the BC government was awarded a silver award at the Institute of Public Administration of Canada (IPAC)/Deloitte Public Sector Leadership Awards.

While efforts to further develop transparency within the BC government are still ongoing, the achievements that have been made thus far reflect a growing recognition by the BC government that openness and citizen engagement are important initiatives. Further, the recognition that the Province has received greatly suggests that the BC government’s strategies are both effective and commendable.

This chapter has provided background information about IM/IT in the BC government, and the recognized need for proper information security management. Also discussed in this chapter were the BC government’s policies for open and transparent government. The next chapter will present the research methodology that has guided this report.

[^3]: http://www.openinfo.gov.bc.ca/
[^4]: http://www.data.gov.bc.ca/
Chapter 3: Methodology

3.1 Environmental scan

To assess the extent to which the BC government may be an attractive target for hacktivists, this report employs the environmental scan methodology. Increasingly environmental scanning is being used by both private and public-sector organizations as a method for conducting analysis (Choo, 2001, para. 13). A key benefit of environmental scanning is that it allows organizations to review and address external forces which may influence their decision-making processes and general operational stability (Albright, 2004, p. 40; Neubaur & Solomon, 1977, p. 13). In order to adequately review and assess the external environment, it is important that information is gathered systematically and objectively (Choo, 2001, para. 41). The benefit of this approach is that it allows the researcher to develop an analysis that is, ideally, more objective, and thus more accurate. For a more detailed account of the research approach used in this report, please see Appendix 1. By improving an organization’s understanding of the external environment, it is expected that organizational learning will be benefited (Choo, 2001, para. 1; Hambrick, 1982, p. 159), and that an organization may be better situated to manage potential pitfalls and external threats that exist (Albright, 2003, p. 40; Neubaur & Solomon, 1977, p. 13).

For the purposes of this report, an environmental scan is an effective and useful tool for assessing the extent to which the BC government may be an attractive target for hacktivists. As Albright (2003) notes, “[e]nvironmental scanning serves as an early warning system, identifying potential threats to an organization” (p. 33). By reviewing current trends within hacktivism, identifying the types of organizations that are being targeted by hacktivists and the motivations behind such attacks, and comparing these to social and political concerns involving the BC government, it is expected that this report will enhance the ISB’s, and thus the Province’s, understanding of hacktivism and its potential implications.

3.2 Scope

The intent of this report is to analyze and discuss the likelihood that the BC government may be a target of hacktivists. Although there are a number of areas related to the topic of hacktivism and the BC government, they are beyond the scope of this report. For that reason, this report does not include an assessment of the BC government’s security capabilities, nor does it offer an assessment of its preparedness to either manage or mitigate, or both, potential attacks by hacktivists. Further, the Province’s current efforts to promote transparency and open government are not reviewed in this report. This report also does not provide an in depth discussion about whether hacktivism should be deemed legal or illegal, as this is a topic that is fraught with legal debate and beyond the purview of this report. While this report does briefly touch upon all of these topics, this is done for the purpose of context.

In consideration of the fact that incidents of hacktivism are discussed by the media on a seemingly daily basis, it should be noted that the examples of hacktivist-related cyber attacks. Examples discussed in this report were selected because of their relevancy to the topic of current trends within hacktivism and government bodies as targets of hacktivists. While the omission of some
hacktivist-related cyber attacks may have limited the applicability of this report to a broad analysis of hacktivism as a phenomenon, the inclusion of such examples was beyond the scope and intent of this report.

3.3 Data Sources

Data used in this report were collected from a range of sources. Academic journal articles and books were integral to developing a thorough understanding of how socially and politically motivated cyber attacks have developed since the late 1980s. These works were also important in this report’s discussion about concepts such as cyber crime and cyber activism. Online news articles, magazines, and security blogs provided a great deal of information about current hacktivist incidents and insight into the groups that often commit hacktivism. Government websites helped provide background information about the BC government, while online news articles were essential to the review and discussion of current incidents of hacktivism. Documents from information security practitioners were also used to develop an understanding of smart security practices for the management and protection of information.

3.4 Research Limitations

As with other research designs the environmental scan approach also has limitations. The prominent concern with the environmental scanning approach is that it presents a researcher with such a wealth of information that the researcher may be overwhelmed by the sheer volume of information that needs to be reviewed (Neubaur and Solomon, 1977, p. 14). This potential overload of information may consequently result in the researcher overlooking materials which are integral to a report’s analysis (Albright, 2003, p. 44). This concern, coupled with the fact that time constraints on the part of the author limited the amount of time that could be devoted to the research phase of this report, is a limiting quality of the environmental scan research method.

Another potential limitation of the research methodology employed for this report is that it relies primarily on qualitative, rather than quantitative, analysis. While quantitative data may have better illustrated the extent to which incidents of hacktivism are in fact increasing or decreasing, such an analysis was beyond the scope of this report. The omission of such data has impacted the ability of the author to definitively state whether or not incidents of hacktivism are in fact increasing, or if the perceived increase of hacktivism is simply the result of the phenomenon becoming more pronounced by the media.

The benefits and limitations of the environmental scan approach, the scope of this report, and the range of data sources used were examined in this chapter. The following chapter discusses the number of ways hacktivism has been defined and the legal ambiguity surrounding hacktivism, and offers the definition of hacktivism that will be used to guide the remainder of this report.
Chapter 4: Literature Review

4.1 Introduction

The term hacktivism, a blending of the words hacking and activism, has become increasingly pronounced amongst academics, security analysts, and the media since its inception in the late 1990s. Yet despite this growing prominence, the existing literature is far from consistent in its discussion of the phenomenon. In addition to on-going debate over the criminality of hacktivism, the word hacktivism itself has been interpreted and defined in many different ways. Because of these discordant interpretations, Krapp (2005) even goes so far as to describe the term hacktivism as controversial (p. 73). Given that the words hacking and activism are ripe for interpretation (metac0m, 2003, p. 1), the competing views surrounding hacktivism are perhaps not surprising.

The term hacking originally referred to the alteration of technology for the purpose of making it do something other than its intended purpose (Jordan & Taylor, 2004, p. 6; Taylor, 2005, p. 488; Levesque, 2006, p.1203). An example of hacking would be reengineering computer speakers so that they work as microphones. It was a way to describe the efforts of computer enthusiasts to develop, or re-develop, technologies in creative and innovative ways. Hacking ethos encouraged open-source data and the sharing of information. Cracking, on the other hand, was the term used to describe the commission of computer attacks. Individuals who participated in cracking, known as crackers, would develop and use technologies for illicit purposes (Levesque, 2006, p. 1203), rather than for the interest in technological development.

By the mid-1990s cracking and hacking had become largely synonymous (Jordan & Taylor, 2004, p. 5), with hacking coming to encapsulate both its original meaning as well as cracking. Expectedly, the word hacking now elicits both positive and negative connotations. This stigma has been carried over into hacktivism, which is often recognized as having both constructive and destructive aspects (McAfee, 2012, p. 30), but has been largely popularized for the latter.

Similar to this new definition of hacking, activism too is not an easily definable phenomenon. While activism can be defined as an action, statement, or movement that is politically or socially motivated, the motivations for any such activity may not always be obvious. Further, while some may view instruments of activism, such as sit-ins, boycotts, or instances of civil disobedience, as completely legitimate, others may view them as intolerable or even criminal.

The blending of these two distinct and complex phenomena is part of the reason for the ambiguity which often surrounds hacktivism today. It has even been suggested that it may be better to describe the idea of hacktivism, rather than try to define it (metac0m, 2003, p. 1). In this chapter, an array of literature pertaining to hacktivism is examined. By discussing what has been said about the phenomenon, and reviewing the numerous ways hacktivism has been defined, this chapter aims to develop a concise and accurate definition of the term. This understanding will establish the parameters that are used throughout the remainder of this report.
4.2 Activism and cyber activism

Traditional forms of activism have involved a range of tactics, including boycotts, blockades, protest marches, information pamphlet campaigns, and civil disobedience. While the social and political motivations behind instances of activism vary, the features that all activist movements seem to have in common are the desire to draw the public’s attention to a particular issue, show support for a cause, and bring about immediate change (Jordan, 2002, p. 9). Activism can be a powerful tool if it has the support of the public and a sense of solidarity amongst the activists involved. Another important component of traditional activism is that its participants are willing to put their own well-being at risk in order to spread their message (McCaughey & Ayers, 2003, p. 5). Risks to activists may come in the form of arrest or police crowd control methods like pepper-spray and rubber bullets.

Cyber activism, which has also been labeled as Internet, online, and electronic activism, is the use of technology and the Internet by activists for the purpose of achieving their social or political goals (Vegh, 2003, p. 71). Given that everything from grocery stores to banks to governments is now using the Internet as a tool for communication and information delivery, it has been argued that it is reasonable that activists would do the same (Haley as cited in Smith, 2011, para. 8). Using the tactics of traditional activism, cyber activism has the advantage of being able to spread information quickly and cheaply and make it much more accessible to people everywhere (Jordan & Taylor, 2004, p. 80; Langman, 2005, p. 60). As Anderson (2008) notes, this embrace of technology provides persons who are discontent with the status quo a new avenue, or voice, by which they can express their frustrations and even take action (p. 4).

Cyber activists often employ tactics which mirror those used in traditional forms of activism. Online stores can be boycotted, and virtual sit-ins can be conducted in the form of distributed-denial-of-service (DDoS) attacks. These tactics serve to call public attention to a particular issue, disrupt an organization’s online operations, and can prevent general Internet users from accessing services online (Denning, 2001, p. 264). In 1996, members from a performance art group called Critical Arts Ensemble (CAE) called upon hackers to become more politicized and for the development of electronic civil disobedience (Jordan, 2002, p. 120). This sentiment was shared by a group of cyber activists and artists called Electronic Disturbance Theatre (EDT) (Anderson, 2008, p. 6). Considering the connotations that the term civil disobedience shares with the American Civil Rights Movements of the 1960s, electronic civil disobedience is a compelling term that certainly attempts to legitimize the use of such tactics. Information websites, online petitions, and widespread email distributions are other examples of how traditional forms of activism have been adopted by cyber activists.

The shift from traditional to cyber activism may not be quite so clear-cut. Hill and Hughes (1998) argue that those participating in cyber activism represent a subset of the general public, and can thus be expected to hold distinct attitudes and beliefs from those who would participate in traditional forms of activism (p. 28). Consequently, according to Hill and Hughes, the issues raised by cyber activists may be different from the types of issues that traditional activists would raise. Another difference between these two forms of activism is that cyber activists do not, necessarily, take on the same level of risk that traditional activists do (Jordan, 2002, p. 132; Himma, 2008, p. 203). This is not to suggest that cyber activism is any less legitimate than
traditional forms of activism though. Rather, the recognition of these differences is merely intended to highlight some of the changes that occur when activism occurs online.

4.3 Hacktivism conceptualized

The term *hacktivism* was coined in 1996 by a member of the online hacking group Cult of the Dead Cow (cDc) known as Omega. Combining the words hacking and activism, hacktivism was used to describe hacking that was committed for political purposes (Ruffin, 2004, para. 1). As Taylor (2005) asserts, this understanding of hacktivism arose at a time when hackers were becoming more politically conscious and activists were becoming increasingly technologically adept (p. 490). Because activism as a broad concept includes both political and social motivations though, this definition seems somewhat incomplete.

Building upon Omega’s description, Oxblood Ruffin, another cDc member, re-defined hacktivism to mean improving human rights through the use and development of technology (Ruffin, 2004, para. 7; Costello, 2001, para. 5). Drawing upon Article 19 of the United Nations’ Declaration of Human Rights, Oxblood Ruffin espoused freedom of expression and opinion, and the right to spread and receive information and ideas through any media, as unconditional human rights (Ruffin, 2004, para. 5). This new definition of hacktivism, which places a strong emphasis on the importance of technological development and the protection of rights, seems to reflect an understanding of hacktivism which is much more aligned with the traditional hacker ethos.

Oxblood Ruffin established a new branch of cDc, known as Hacktivismo, which focused its efforts towards the protection of human rights on the Internet. Members of this group developed and disseminated software that allowed users to circumvent government firewalls and Internet filtering programs. Efforts were also made to bolster anonymity amongst Internet users. Interestingly, the efforts of Hacktivismo did not emphasize two key components of activism: drawing public attention to a social or political issue; and demanding change. As such, it can be argued that while Oxblood Ruffin’s definition of hacktivism does reflect the traditional hacker ethos, it does not seem to altogether embrace the concept of activism.

4.4 Evolution of hacktivism

Drawing upon the idea that hacking and activism could work in combination, proponents of electronic civil disobedience, virtual sit-ins, and other cyber activists tactics increasingly began to identify with the concept of hacktivism; a shift which Oxblood Ruffin (2004) strongly denounced (para. 12). The main criticism was that individuals who did not develop new technologies did not deserve the affiliation to hacking culture (“4 signs ‘hacktivism’ has gone mainstream, 2012, para. 18). The term cracktivism was even coined in an attempt to differentiate between the two hacking ideologies (metac0m, 2003, p. 2). Nevertheless, many still viewed cracking and hacking as interchangeable. As such, when computer attacks began to be committed for social or political reasons, the term hacktivism was generally seen as a befitting description (Vamosi, 2003, para. 3), and the concept of hacktivism was no longer limited to just technological development.
Amongst academics, hacktivism has been subject to a number of labels: politically motivated hacking (Jordan, 2002, p. 19); online grassroots resistance (Delio, 2004, p. 1; McCaughey & Ayers, 2003, p. 3); digital intrusions motivated by moral positions (Himma, 2008, p. 200); and the electronic bombarding of websites (Langman, 2005, p. 45). While all of these definitions do highlight an aspect of what hacktivism has now come to encapsulate, no single definition seems to offer a complete understanding of the phenomenon. What these divergent views do illustrate is the fact that hacktivism is a complex concept that is comprised of numerous, sometimes competing, ideologies.

This shift within hacktivism also fuelled debate about whether hacktivists were “wired activists” or if they were merely “politicized hackers” (Vegh, 2003, p. 83). In fact, cyber activists began to find themselves being labelled as hacktivists (Jordan & Taylor, 2004, p. 30). Given that some of the tactics employed by cyber activists, such as virtual sit-ins and DDoS attacks, are in fact types of cyber attacks though, this labelling is perhaps not surprising. Yet because of these overlapping characteristics that cyber activism and hacktivism share, it can be difficult to determine where one phenomenon ends and another begins.

The discerning principle between the two concepts seems to be how the Internet and technology are being used. If cyber activism can be considered the online form of traditional activism, hacktivism may best be understood as being the online version of “disruptive [and] expressive politics” (Krapp, 2005, p. 88). Whereas cyber activism is more about using technology and the Internet as an avenue for achieving social or political goals, hacktivism was now coming to be seen as the use of technology as a tool for direct action (Manion & Goodrum, 2000, p. 15; Jordan & Taylor, 2004, p. 1). Accordingly, it can be understood that some aspects of cyber activism are in fact more closely aligned to the concept of hacktivism.

Using the same tools and techniques as hackers (Milone, 2003, p. 77; Jordan, 2001, p. 9), many self-identified hacktivists were now focusing less on technological development, and more on committing cyber attacks for the purpose of protesting issues. Website defacements, data breaches, and DDoS attacks were becoming increasingly popular tools of protest (Smith, 2011, para. 1). These tactics were much more confrontational than other, more conventional, forms of cyber activism, such as online petitions. As a result, hacktivist tactics could range from the more passive to the highly damaging and illegal (Information security forum, 2011, p. 1). This shift was motivated by the expectation that these new tactics would be more effective at instigating change (Samuel, 2004, p. 3), which is a key aspect that differentiates hacktivism from other forms of cyber attacks. While some cyber attacks are committed for reasons of malice or entertainment, hacktivist attacks are intended to garner public attention, spread a social or political message (metac0m, 2003, p. 2; Information security forum, 2011, p. 1), and incite change.

Participants in hacktivism also began to use humour as a way of spreading their message (Samuel, 2004, p. 7). While some may view this tactic as a sign that hacktivists do not take themselves seriously, others may see it as trivializing the issues. Regardless, hacktivist attacks were increasingly sensationalized by the media (Jordan, 2002, p. 9; Krapp, 2005, p. 88), and attracted a great deal of attention. As Vegh (2003) notes, this widespread attention provides hacktivists with an “effective forum for publicizing the issues in contention” (p. 92). By drawing
widespread attention to a particular social or political issue, hacktivism has the ability to engage people in a particular issue (Jordan, 2002, p. 125), garner public support, and act as an agent of change (Levesque, 2006, p. 1213; McAfee, 2012, p. 29). It is this aspect of hacktivism that clearly echoes aspects of traditional activism, and strongly differentiates hacktivism from other types of cyber attacks.

4.5 Hacktivist tactics

Hacktivists have used a number of tactics to protest and draw attention to social and political issues. While the intent of hacktivist attacks vary, the most common tactics appear to be website defacements, website redirects, DDoS attacks, and unauthorized data releases (Rashid, 2011, p. 1). The use of malicious software programs, such as viruses and worms however is generally not considered by participants in hacktivism to be an acceptable tactic (metac0m, 2003, p. 3). The impact of successful hacktivist attacks range from the negligible to the hurtful.

Website defacements and website redirects

Website defacements, which have also been labelled as e-graffiti, cyber vandalism, and cyber sabotage (Auty, 2004, p. 216), entail the unauthorized altering of a website’s message or content. Aspects of websites that have been subject to modification in the past include images, information provided on the website, and political party slogans. Many have denounced website defacements, arguing that they are pointless acts of vandalism and the equivalent to activists who graffiti buildings (Levesque, 2006, p. 1213; Jordan & Taylor, 2004, p. 130). This understanding of website defacements views the tactic as being both destructive and juvenile.

Website redirects entail the redirecting of a website’s uniform resource locator (URL) to a different website. This can be done to make a social or political message, or for more malicious purposes, such as a phishing attack. Website redirects occur as a result of a person or persons gaining unauthorized access to a website. A successful website redirect may be embarrassing for the owners of a targeted website, and in some cases has been described as infringing upon an organization’s freedom of expression (Auty, 2004, p. 218).

If website defacements or website redirects are to be considered acts of hacktivism, they need to draw attention to a particular social or political concern. Without this intent, they become mere forms of cyber attack or fraud. If a website defacement or website redirect is clearly politically or socially motivated, it serves as an effective way for hacktivists to spread a message, draw attention to an issue, and embarrass the organization that operates the website (Himma, 2008, p. 202). Because both a website defacement and redirect are completely reversible, the overall damage incurred is largely insignificant (Himma, 2008, p. 202). Recognizing this, the overall threat from website defacements and website redirects appears to be significantly less than terms like cyber vandalism and cyber sabotage would otherwise imply.

DDoS attacks

This tactic, which was first used by cyber activists, may best be understood as the deliberate attempt to exceed the bandwidth capabilities of a targeted server. By overloading a computer
network’s servers, a targeted website will temporarily shut down, and access to the site will be blocked. DDoS attacks may be perpetrated by both botnet computers and the involvement of many individuals. The involvement of numerous persons in a DDoS attack has consequently led to some DDoS attacks being viewed as the online version of a sit-in. While a sit-in protest in the real world may be seen as a legitimate form of activism, the virtual equivalent has been described as criminal (Brenner, 2007, p. 384). It should be noted though that DDoS attacks are only able to shut down a website for a short period of time, and they do not entail the destruction or unauthorized release of any data that is stored in the targeted server (Neeley, 2000, p. 30).

DDoS attacks have also been described as a form of reverse censorship (Oxblood Ruffin, as cited in Delio, 2004, p. 1). Given that hacktivists often espouse the importance of open access to information, the intentional effort to temporarily shut down a website, and thus prevent others from accessing the targeted site, is often viewed by critics as hypocritical (Jordan, 2002, p. 133; Ruffin, 2004, para. 11). This understanding of DDoS attacks overlooks the fact that hacktivists are committing these attacks to protest or draw attention to a political or social issue though. In the case of hacktivist DDoS attacks, censorship is a by-product of the attack, and is not the primary intent. Moreover, the censorship attributed to the attack will only occur as long as the DDoS attack is able to continue.

Unauthorized data releases

An unauthorized data release, also known as data dumping, entails the unwarranted release of a person’s or an organization’s data onto the Internet; where they become publicly accessible. Materials and information that may be released in a data dump include employee names, passwords, credit card information, personal emails, personal photographs, and internal documents. Hacktivists commonly gain unauthorized access to this data through the use of hacking techniques, such as SQL, pronounced sequel, or cross-site scripting (XSS) injections. Himma (2008) strongly criticizes these techniques, asserting that they constitute a digital trespass (p. 192).

The implications of an unauthorized data release vary, depending on the type of information that hacktivists are able to access, and the type of data they decide to publish online. An unauthorized data release may simply be embarrassing for a person or organization, or it may include sensitive information. Given this potential threat, some commentators have gone so far as to label hacktivists as information-terrorists (Jordan & Taylor, 2004, p. 30). The publication of data, such as credit card information, also creates the potential for information to be misused by others.

4.6 Legal ambiguity

While some may consider hacktivism to be the online equivalent of civil disobedience, others have argued that hacktivism is emphatically criminal (Information security forum, 2011, p. 2). This debate is further complicated by the fact that the issues hacktivists are protesting may not always be obvious to the public (Anderson, 2008, p. 5). If a hacktivist attack does not have a clear message, the purpose of the attack may be easily misinterpreted. The use of humour or explicit language may also cloud the intent of a hacktivist attack. As a result, instances of hacktivism may be viewed by the public as simply attempts by hackers to do harm or
demonstrate their hacking skills (Gosh, as cited in Acohio do, 2011, para. 8). The ambiguous motivations of some hacktivist attacks may also make it difficult to differentiate a socially or politically motivated hacktivist attack from attempts at intimidation, senseless cyber pranks, or malicious criminal attacks (Strohymeyer, 2011, para. 6; McAfee Labs, 2011, p. 4). Given the level of ambiguity that surrounds hacktivism, critics have also described the phenomenon as a politically immature gesture (Krapp, 2005, p. 87). Hacktivists have been criticized for using pseudonyms online, and not taking on the same level of risk that traditional activists do (Panda Labs, 2011, p. 4). Such statements serve to delegitimize the notion that hacktivism is a form of activism, and reinforce the understanding that hacktivism is criminal, or perhaps simply juvenile.

Concern has also been expressed that even if hacktivism itself is not criminal, those committing hacktivism may attract the attention of organized crime or terrorist groups, who may want to use the computer skills of hacktivists for more insidious purposes (Chabinsky, as cited in Gjelten, 2011, para. 6). While this may be a legitimate concern, the same could be said of any form of activism or technological development. Accordingly, it does not seem justifiable to condemn hacktivism simply for the potential threat that hacktivism could be subject to misuse. Nevertheless, the potential misuse of hacktivists’ capabilities does illustrate an excellent reason for why organizations and government bodies may want to afford proper consideration to potential hacktivist threats.

Contrary to the view that hacktivism is merely criminal, several academics and self-identified hacktivists maintain that hacktivism is an acceptable form of electronic civil disobedience. For example, Himma (2008) suggests that the illegal activities of hacktivists are justifiable if they do more good than harm (p. 192). Some have even gone so far as to compare hacktivists to Diggers, Black Panthers and suffragettes (“A long tradition of dissent,” 2011, para. 4). Yet, whereas hacktivists want their actions to be seen as acts of civil disobedience (Neeley, 2000, p. 30), others maintain that the tactics used by hacktivists, regardless of their motivation, are indisputably illegal and therefore unacceptable (Gjelten, 2011, para. 3; Oxblood Ruffin, as cited in Smith, 2011, para. 15).

In Canada, data interception, data theft, attempts at network interference such as DDoS attacks, gaining unauthorized access to computer systems, website defacements, and malware dissemination are only some of the acts that have been deemed computer crimes (McConnell International, 2000, p. 5). These acts are seen as criminal for a number of reasons, including that they may violate people’s privacy, interrupt online services, and allow for the misuse of information (Boni & Kovachich, 1999, p. 42). A person found guilty of any of these offenses may be liable to a term of imprisonment.

It is of value to note that computer crimes are often subject to the same legal penalties, regardless of motivation or intent (Manion & Goodrum, 2000, p. 16). In fact, in the United States (US) a socially or politically motivated DDoS attack is considered a felony, and subject to the same severity as a DDoS attack that is committed as an act of extortion (“4 signs ‘hacktivism’ has gone mainstream, 2012, para. 28). Interestingly, the German court system has done the opposite of the US and other countries, and even gone so far as to recognize DDoS attacks as an accepted form of social protest (“4 signs ‘hacktivism’ has gone mainstream, 2012, para. 41). This position
clearly illustrates an instance where hacktivism has been deemed a legitimate form of online activism, which supports the notion that hacktivism is a form of electronic civil disobedience.

4.7 Overlapping categories

Related to the issue of hacktivism’s legal ambiguity, academics and the media have often associated hacktivism with acts such as cyber espionage, cyber terrorism, and cyber warfare (Manion & Goodrum 2000, p. 14). While these categories do share some similarities, and it can be difficult to discern between them (Jordan, 2001, p. 8; Auty, 2004, p. 219; Menn, 2011, para. 3), there are distinct differences between these categories that need to be recognized. If disparate phenomena such as these are grouped together, or labels are used interchangeably, it may lead to confusion about what hacktivism actually denotes.

Cyber espionage

One term that has been applied to hacktivism is cyber espionage. Cyber espionage can be understood as meaning the online surveillance of a person or an organization for the purpose of deriving some sort of competitive advantage (Boni & Kovachich, 1999, p. 84). It is an act that can generally be attributed to the state, but may also include private corporations. Cyber espionage may be motivated by economic, social, financial, political, or military interests, and denotes underhanded or secretive actions.

Hacktivism, unlike cyber espionage, is an act committed by sub-state actors. Also, hacktivism is intended to be a very public act, with very public results. In fact, hacktivist attacks are often announced ahead of time (Shulman, as cited in Schwartz, 2012a, para. 5). While hacktivism may be politically or socially motivated, it is committed for the purpose of protesting or drawing attention to an issue, not to derive a competitive or financial advantage. Given these differences, the label of cyber espionage seems wholly inappropriate when discussing instances of hacktivism.

Cyber warfare

The use of the word war has strong connotations to destruction and death. As Manion and Goodrum (2000) argue though, hacktivism is fundamentally non-violent (p. 16). Supporting this notion, there does not appear to be any evidence that hacktivist efforts have ever promoted the type of violence that war entails. Jordan (2002) does note though that violence may not always be physical, but emotional as well (p. 126). This potential threat alone does not seem to justify the interchangeability of the terms cyber warfare and hacktivism.

At times, hacktivism has also been referred to as a form of cyber warfare (Vegh, 2003, p. 81). This is problematic for several reasons. Firstly, war may be understood as a prolonged conflict, conducted by a state, in which opposing parties are fighting for control or some sort of advantage (Vegh, 2003, p. 83; Brenner, 2007, p. 401). Given that the overall intent of hacktivism is to spread a message, albeit through somewhat confrontational means, rather than fighting for control over an organization or government, the comparisons between hacktivism and acts of war may be somewhat misleading. Also, since hacktivists are sub-state actors, this definition does not
seem appropriate. Because the tactics used by hacktivists may be similar to those that would be used in cyber warfare (Jordan, 2001, p. 10), such as a coordinated attack against a computer server, there may be some overlap between the categories of hacktivism and cyber warfare.

**Cyber terrorism**

Cyber terrorism is an area of cyber crime that is perhaps the most similar to hacktivism. Cyber terrorism can be understood as acts of terrorism that are orchestrated through the use of online technologies. However, it should be noted that “[t]here is no evidence that terrorists are using computers for…cyberspace attacks” (Krapp, 2005, p. 75). Nevertheless, hacktivism has still been compared to, and associated with, terrorism. Similarities between the two phenomena include the fact that both cyber terrorism and hacktivism entail the committing of confrontational acts by sub-state actors. Also, like hacktivism, terrorism is motivated by social or political ideologies.

The key difference between these two categories is the use of violence (Samuel, 2004, p. 3). Hacktivists attempt to spread their message by using technology to protest, or draw attention to, a particular social or political issue. While the tactics they employ may shut down or deface a website temporarily, publish private information, or cause embarrassment to a target, the overall intent of hacktivism is to spread a message and stimulate discussion; not cause grievous harm (Himma, 2008, p. 200). Terrorist tactics, on the other hand, rely upon spreading fear, demoralizing and harming people, and destroying property as part of their strategy (Boni & Kovachich, 1999, p. 82; Brenner, 2007, p. 388).

By comparing hacktivists to terrorists, it implies that hacktivists too use violence and fear as a tactic. It also implies that the damage caused by hacktivists is irreversible. While it would be naïve to argue that hacktivism does not cause some degree of disruption or negative effect upon targeted organizations, comparing hacktivist tactics to those used by terrorists may be somewhat inaccurate and irresponsible (Krapp, 2005, p. 88). If hacktivists were to begin committing violence and intentionally causing grievous harm though, it would be quite difficult to argue that such actions do not constitute terrorism.

**4.8 Hacktivism: a definition**

While a degree of ambiguity still surrounds hacktivism a concise definition for the phenomenon can still be derived. For the purposes of this report hacktivism may be understood as:

> the act of committing a cyber attack for the purpose of protesting, or drawing attention to, a social or political issue; without the intent to obtain financial benefit or grievously harm the target.

While technological development does still play a role in hacktivism, hacktivism may best be understood as active participation in direct action against an organization or government. This new definition embraces what the phenomenon of hacktivism has now come to denote, rather than focusing on the original, narrower, definition of the term. By articulating that hacktivism has a social or political intent, this definition also serves to differentiate between hacktivist attacks and other forms of malicious cyber attacks.
This chapter briefly examined activism and cyber activism. How hacktivism was conceptualized, and how its definition developed and evolved over time was also discussed. This chapter also looked at the ambiguity surrounding hacktivism, the multitude of ways it has been defined, and presented the definition of hacktivism that will be used to guide the remainder of this report. The next chapter presents background information about how socially and politically motivated cyber attacks have developed since the late 1980s, provides examples of hacktivist attacks, looks at some of the groups that are committing hacktivism today, and reviews some of the techniques that are being used by hacktivists.
Chapter 5: Hacktivism Background

5.1 Introduction

Although the term hacktivism was not coined until 1996, instances of socially and politically motivated cyber attacks had been occurring as early as the late 1980s. The development of new and improved online technologies was instrumental in the ability of individuals and groups to spread their messages, and draw attention to social and political issues (Langman, 2005, p. 44; Juris, 2005, p. 201; Levesque, 2006, p. 1204). Menn (2011) states that this new approach was a much more accessible, and perhaps more effective, means by which individuals could become involved in forms of protest and civil disobedience (para. 28). As a result, new avenues were emerging by which organizations and governments could be susceptible to confrontational forms of criticism and discord.

This chapter will look at a number of the socially and politically motivated cyber attacks that have occurred since the late 1980s. This discussion will illustrate how hacktivism has evolved as a phenomenon, look at some of the tactics that have been used, and highlight some of the specific issues that have garnered the attention of hacktivists. For a timeline of this chapter, please see Appendix 2. Events discussed in this chapter are sorted by themes. Within each theme, events are ordered chronologically.

5.2 Technological development

Technological development, although it does not constitute a form of cyber attack, was the critical component in early notions of hacktivism. While this is not so much the case now, it is still worthwhile to look how hacktivism, as defined by Oxblood Ruffin, took place.

Hacktivismo

As was mentioned in the previous chapter, Oxblood Ruffin formed Hacktivismo as a branch of cDc. Members of Hacktivismo developed a number of new software programs that promoted user anonymity online, and allowed users to encrypt data and bypass government firewalls and Internet filters. Three of the better known programs released by Hacktivismo are Camera/Shy, the Six/Four system, and Scatterchat (Hackett, 2011, para. 3); all three of which can be found online for free.

Camera/Shy is a program that uses an encoding method, known as steganography, to bury digital content into a digital picture file (Ruffin, 2004, para. 23). When someone receives an encoded file, they are able to use Camera/Shy to decode the picture file and extract the buried content. In doing so, users are able to covertly exchange information or pictures online with one another. Another encryption program Hacktivismo produced is Scatterchat. It is a messaging program that encrypts users’ messages. By encrypting people’s online conversations, Scatterchat serves to promote online anonymity, and reduces the likelihood of government surveillance.

Another of Hacktivismo’s projects was the Six/Four system. In some countries, governments have established national firewalls and Internet filters. This limits what information individuals...
within that country are able to access online, even on their personal computers. The Six/Four system allows users to bypass government firewalls and Internet filters through the use of encrypted proxy servers to relay information (Danke, n.d., para. 4; Ruffin, 2004, para. 24). Accordingly, the Six/Four system was a way of circumnavigating Internet censorship and providing improved access to information.

Technological development today

Although hacktivism has come to mean much more than Oxblood Ruffin’s initial definition, technological development for the purpose of protecting people’s rights is still happening today. Hackbloc.org, hacklab.to, binaryfreedom.info, and hellboundhackers.org are just a few examples of contemporary websites dedicated to the on-going development of open source software technologies. Hacktivismo even has a website of its own, although it has not been updated since 2008. While websites such as hacklab espouse the sharing and collaboration of knowledge and technologies, which is very much in line with traditional notions of hacking, websites such as hackbloc are much more aligned with modern ideas of hacktivism and confrontational direct action.

5.3 Malware

There are relatively few cases of malware that fall into the area of hacktivism. The use of viruses and worms has generally been opposed within the hacktivist community (metac0m, 2003, p. 3), and seems to have limited the number of socially or politically motivated malware programs that have been developed. Nevertheless, the fact remains that malware has been used as a means to spread social and political messages (Denning, 2001, p. 278).

Fu Manchu virus

One of the earliest examples of a politically motivated malware program was the Fu Manchu virus, which began infecting computers in 1988. The Fu Manchu virus would bury itself in an infected computer’s memory, and would add explicit text to the names Thatcher, Reagan, Botha, or Waldheim if they were typed by the user5 (Wang, 2003, para. 3). All four of these individuals were world leaders at the time the virus came out.

Although the Fu Manchu virus does not have a clear social or political message, it certainly appears to have been politically motivated. During the late 1980s, there were several political issues which plagued all of the politicians targeted by the Fu Manchu virus. In 1988, Pieter Willem Botha was the President of South Africa, which was still under the apartheid system. Margaret Thatcher meanwhile had opposed trade sanctions that had been imposed upon South Africa. Ronald Reagan’s bolstering of the War on Drugs or the Immigration Reform and Control Act, which made it illegal for someone to knowingly hire an illegal immigrant, are two issues which may explain why he was targeted by the Fu Manchu virus. In 1985, it was discovered that Kurt Waldheim, who was elected President of Austria soon after, was a former intelligence

5 The added text would say: Thatcher is a cunt; Reagan is an arsehole; Botha is a bastard; and Waldheim is a Nazi (Hirst, 1989, “the next fields are encrypted).
While the reasons why Botha, Thatcher, and Reagan were targeted by the creator of the Fu Manchu virus remain merely speculative, Waldheim’s inclusion seems more obvious. Yet rather than draw attention to a specific issue, the Fu Manchu virus seems to do nothing more than simply mock and slander the four targeted politicians. Although certainly a politically motivated virus, the lack of a clear intent or message seems to limit the extent to which the Fu Manchu virus can clearly be understood as being a case of hacktivism. Nevertheless, the Fu Manchu virus is an early example of how malware programs have been used as a tactic to make politically or socially motivated statements.

**Nuclear weapons**

The development of nuclear weapons is another issue that has been the target of politically and socially motivated malware. In 1989, computers belonging to the National Aeronautics and Space Administration (NASA) and the US Department of Energy were attacked by the anti-nuclear WANK worm (Assange, 2005, para. 1). WANK stands for Worms Against Nuclear Killers, but is also a British colloquialism for a lewd act. In addition to an array of messages that the worm would display, it would mislead users into thinking that all of the files on their computers were being erased. The WANK worm was fabricated to protest “against NASA launching space probes that included small nuclear reactors, often described by protestors as potential nuclear bombs” (Jordan, 2002, p. 120). Regardless of whether or not these concerns were justified, the WANK worm was clearly politically and socially motivated. As Jordan (2002) states, “[t]his was hacktivism before the term was invented” (p. 120).

![Image of the WANK worm message](http://www.global1.youth-leader.org/wp-content/uploads/2011/05/wankworm.jpg)

In 1995, six years after the WANK worm, the Ph33r, pronounced _fear_, virus was created. The virus was created to protest French nuclear testing that was going on at the time, which had garnered a great deal of international attention and criticism (“Fifth French nuclear test,” 1995, para. 1). The Ph33r virus would infect the user’s Microsoft Word program, inserting text at the end of Word documents (Wang, 2003, para. 4). The text would read “STOP ALL FRENCH
NUCLEAR TESTING IN THE PACIFIC!” This text would only appear when a Word document was printed or faxed, limiting the likelihood that the user would notice the message (Hypponen, 2009, para. 6). This is another example of how hacker tactics were being used to make political or social messages before the term hacktivism was even coined.

InJustice virus

The on-going conflict between Israel and Palestine is another issue that has been the target of socially and politically motivated malware. In 2001, the InJustice virus, also known as the Staple virus, began infecting computers. This virus was spread as an attachment in an email titled injustice.TXT.vbs. In order to activate the virus however, the attachment needed to be intentionally opened by the email recipient (Meserve, 2001, para. 3). Once the attachment was open, a message apologizing for the intrusion would appear, and then the story of a Palestinian boy who was killed by the Israeli military was recounted (Weisman, 2001, as cited in Samuel, 2004, p. 12; Wang, 2003, para. 6). The virus would then direct the computer’s Internet browser to six pro-Palestinian websites (Meserve, 2001, para. 4). The intent of this virus was to increase public awareness of the perceived injustices that were being committed against the Palestinian people and amass public support.

Figure 2. Dialogue box displayed by the InJustice virus

Mari@mm worm

The Mari@mm worm, which came out in 2001, was a malware program that promoted the legalization of marijuana. Spread via email, the worm would put a marijuana leaf icon on the infected computer’s taskbar. If the icon was clicked, a dialogue box would open, explaining the rationale for why marijuana should be legalized (Wang, 2003, para. 5). Recognizing that the

7 Image available at http://www.f-secure.com/v-descs/staple.shtml
worm may simply be dismissed as another harmful malware program the author of the
Mari@mm worm emphasized the fact that the worm was intended to spread a message; the
legalization of marijuana. It is of value to note then that although hacktivists generally dismiss
malware as an acceptable tactic, the Mari@mm worm is a very good example of how malware
can align with the notions of hacktivism, as defined in this report.

Figure 3. Dialogue box displayed by the Mari@mm worm

5.4 DDoS attacks

Originally used by cyber activists as a form of virtual sit-in or electronic blockade, there are a
number of instances where DDoS attack have been used as a mechanism for protest or making
social or political statements.

Intervasion of the U.K.

The first socially or politically motivated DDoS attack is said to have happened in 1994, in an
attack known as the Intervasion of the U.K. The group that coordinated this attack was a group
called The Zippies. This week long DDoS attack, in which websites belonging to British
politicians were shut down and email flow was disrupted, was in response to the Criminal Justice
and Public Order Act of 1994, which had first been introduced by British MP Michael Howard
(Wikileaks infowar, 2010, para. 1). While this Act included several amendments to pre-existing
British criminal law, the provision that garnered the attention of The Zippies was the
criminalizing of unlicensed music festivals that played rave music (Wikileaks infowar, 2010,
para. 3).

It is of value to note that The Zippies conducted the Intervasion of the U.K. attack from San
Francisco, California. This is because this campaign illustrates the willingness of international
groups to take on issues which are seemingly restricted to a particular country. Further, the attack
was launched on November 5, two days after the Bill received Royal Assent, which is Guy
Fawkes Day. Guy Fawkes, who attempted to blow up the British Parliament in 1605, has been
largely romanticized and become “an icon for people looking to stand up to power” (Merica,
2011, para. 1). While this DDoS attack was ultimately unsuccessful in decriminalizing

---

99&tabid=2

Hacktivism and the Government of British Columbia 21
unlicensed raves, it is an interesting example of how groups were beginning to use technology as a method for conducting confrontational forms of direct action.

**Strano Network**

In 1995, an Italian group known as the Strano Network conducted network DDoS attacks against a number of French government sites. This campaign was in protest to the French government’s policies regarding nuclear weapons (Taylor, 2005, p. 488). The efforts of the Strano Network coincided with international condemnation of the French government’s on-going testing of nuclear weapons in French Polynesia, as well as the anti-nuclear Ph33r virus.

**Zapatista Movement**

The Zapatista Army of National Liberation is a revolutionary group that operates in Mexico. Formed in 1994, the group works in opposition to the Mexican government and promotes the implementation of more libertarian-socialist policies. Members of this group are known as Zapatistas. In 1998, attacks against Zapatistas by the Mexican government received the attention of the Electronic Disturbance Theatre (EDT), a group of cyber activists and artists (Jordan, 2001, p. 8). Using a JavaScript-based software program called Floodnet, EDT launched a DDoS campaign against Mexican government networks to show their support for the Zapatistas (Taylor, 2005, p. 488). Because the effectiveness of Floodnet was dependent upon the number of persons actively involved in the attack (Shachtman, 2004, para. 8), it can be understood as having been an early example of a virtual sit-in.

**World Trade Organization Protest**

The World Trade Organization (WTO) Ministerial Conference was hosted in Seattle in November 1999. Real world protests and sit-ins were conducted for the purpose of disrupting the conference and drawing public attention to concerns surrounding globalization. To complement the real world protests, a group of cyber activists known as the Electrohippie Collective organized a virtual sit-in (Jordan, 2002, p. 122; Samuel, 2004, p. 12). This DDoS attack used a tool that was based on the Floodnet tool that the EDT had used the previous year (Jordan, 2001, p. 8).

5.5 Website defacements and website redirects

Website defacements and website redirects are distinct, yet similar, tactics by which individuals and groups have drawn attention to social and political causes. Both tactics entail the unauthorized modification of a website, and both affect what Internet users see when they attempt to access the modified website.

**US Department of Justice**

In 1996, Congress passed the Communications Decency Act (CDA), which criminalized the transmission of materials online that were deemed offensive and obscene. Civil liberties and online groups protested the CDA, saying that it infringed upon people’s freedom of speech.
As part of the growing opposition to the CDA, the US Department of Justice even had its website defaced by an anonymous hacker. The website found itself plastered with swastikas, racist slogans, and pornographic images (Help!!...We’ve been hacked!!, 1997, “Government agencies”) in what can only be interpreted as being a sardonic and satirical message to the US Government.

The Chinese government

The Chinese government has also been the target of website redirects. For example, in 1998 a Chinese government website for human rights was redirected to the Amnesty International website. The attack was conducted in response to human rights and freedom of speech abuses that the Chinese government had been accused of (Vegh, 2003, p. 79). By redirecting the Chinese government’s website, the perpetrators of the attack were able to voice their concerns with the Chinese government’s efforts to protect its citizens’ rights.

Anti-nuclear message

In July 1998, the hacker groups Milw0rm and Ashtray Lumberjacks worked together to redirect the homepages for over 300 websites. Users attempting to access any of the 300 websites were redirected to a Milw0rm site that displayed “a message protesting the nuclear arms race” (Denning 2001, p. 273). The anti-nuclear message was quite clear, urging people to promote world peace “and put a stop to this nuclear bullshit”. By defacing so many websites, Milw0rm and Ashtray Lumberjacks were able to spread their message to a large audience.

The Ku Klux Klan

In 1999, in an attack very similar to the website redirect on the Chinese government the year before, the website for the Ku Klux Klan (KKK) was redirected to hatewatch.org. HateWatch is an organization concerned with bigotry and racism online (Samuel, 2004, p. 10). As was the case with the Chinese government’s human rights website, the website redirect of the KKK certainly appears to have been intended to be both ironic as well as send a social message to users attempting to access the site.

5.6 Groups that commit hacktivism

The discussion thus far has made mention of several groups: Cult of the Dead Cow (cDc), Hacktivismo, The Zippies, Strano Network, Electronic Disturbance Theatre, and the Electrohippie Collective. While Hacktivismo is the only one of these groups that has actually identified itself as being a hacktivist body, all of these groups demonstrated aspects of both hacking and activist culture. Still, it would be inaccurate to simply categorize all of these groups as hacktivist. By labelling a group as hacktivist, it implies that any cyber attack committed by the group is an act of hacktivism; which may be misleading. For example, many of the groups today that are committing acts of hacktivism have also been involved in activities that lack political or social objectives. Failure to discern between a group’s motivations for a cyber attack merely fosters confusion and uncertainty about what hacktivism truly denotes. Despite the potential for groups to be broadly mislabelled as hacktivist, there a number of contemporary online groups.
that have become prominent within hacktivism. Today, perhaps the most notable are Anonymous, LulzSec, and AntiSec. Lesser known groups include the People’s Liberation Front and TeamPoison. The motives behind hacktivist attacks will be discussed in Chapter Six.

**Anonymous**

In 2003, Christopher Poole, who goes by the online alias moot, created the website 4chan.org. 4chan is an online image and message board where users are able to post pictures and comment anonymously. The decision to make users anonymous was based on the belief that users’ comments should be judged on their own merit, rather than who was making them (Landers, 2008, para. 13). It is from this valuing of anonymity on 4chan that the idea, or meme, of Anonymous developed. People identifying with the Anonymous meme formed a unique online subculture, initially using 4chan as their means of connecting with one another.

While Anonymous has often been labelled as a loose group or collective, others have insisted that this is not the case (Stryker, 2011, p. 244). Rather than view Anonymous as a group, it has been suggested that Anonymous is simply an idea that anyone can choose to identify with and follow (Anon_Central, 2012b; Albanesisu, 2011c, para. 11), or that Anonymous is better thought of as a brand (Stryker, as cited in Pan, 2012, para. 11). Because people cannot be a member of an idea or a brand, it would seem inappropriate to declare someone a member of Anonymous. However, once co-ordination and organization occurs, it becomes difficult to argue that Anonymous is not in fact a group. As such, for the purposes of this report, Anonymous may be best understood as being a loose collective. So-called members of Anonymous can be understood as denoting individuals who have participated in activities on behalf of, or along with, the Anonymous collective.

Early activities that individuals who identified with Anonymous were involved in included cyber pranks, signing people up for junk emails, and ordering pizzas to people’s houses (Norton, 2011a, para. 34). These coordinated cyber pranks, called raids (Norton, 2011a, para. 32), were not committed for any social or political purpose. Rather, raids were carried out for the humour that was derived. One of the better known cyber pranks committed by Anonymous is the 2005 raid known as the Habbo Hotel raid. Habbo Hotel is an online virtual reality networking site designed for teenagers. A group of individuals identifying with Anonymous accessed the site, gave themselves African American avatars with oversized afros, and blocked access to the online hotel’s pool area, saying that the pool was closed due to AIDS (Single, 2012).

Although the early activities of Anonymous were largely done for the humour of the raids, and were more along the lines of online mischief, concern was beginning to grow about whether Anonymous posed a threat to the public. A 2006 news story by Los Angeles News, an affiliate of Fox News, referred to Anonymous as ‘hackers on steroids’ and an ‘Internet hate machine’ (Landers, 2008, p. 17). While this description of Anonymous is perhaps exaggerated, it does illustrate the growing concern about Anonymous’ growing presence online, and the potential harm that their raids could pose.

As time progressed, members of the Anonymous collective began to involve themselves in social and political issues. Targets included the Church of Scientology in 2008, the film and music
industry, and groups that were seen as imposing upon freedoms on the Internet. Whereas Anonymous was originally concerned with cyber pranks, it was now committing acts that were socially and politically motivated. The shift from pranks to activities that were morally or ideologically driven was reproached by some however. It was felt that the motivation to do good was contrary to what Anonymous stood for. In a rather brazen effort to condemn this transformation, some labelled the socially and politically motivated efforts of Anonymous as moralfaggotry (Norton, 2011b, para. 19; Menn, 2011, para. 13). Norton (2011a) states that the attacks against the Church of Scientology, known as Operation Chanology, signalled the beginning of Anonymous’ political consciousness (para. 41). It was also during Project Chanology that members of the Anonymous collective began wearing the Guy Fawkes mask, which has since become the constant symbol of Anonymous members.

**People’s Liberation Front**

The People’s Liberation Front (PLF) is a small group that operates within the Anonymous moniker. It has been stated that the PLF is best understood as being a contingent within the Anonymous collective (Commander X, personal communication; as cited in Tynan, 2011, para. 26). Notwithstanding, the PLF only becomes engaged in the efforts of Anonymous when it deems it suitable.

**LulzSec**

LulzSec, a combination of words lulz and security, is a small group that branched out from Anonymous in 2011. Unlike Anonymous, which anyone can identify with, LulzSec was comprised of a small number of individuals who are reportedly proficient at hacking (Poeter, 2011, para. 12). As the name of the group suggests, LulzSec focuses its efforts on finding and exploiting security flaws online. Yet rather than being motivated by specific political or social concerns, LulzSec claims to only commit the acts for the humour that it derived, and for the purpose of embarrassing organizations (McAfee, 2012, p. 29). Regardless of their explicit motivations, Albanesiuss (2011a) states that the efforts of LulzSec serve to draw attention to poor security practices amongst companies and governments (para. 22), which is a social and political issue. Recognizing this then, many of the attacks committed by LulzSec do align with this report’s definition of hacktivism.

During the summer of 2011, LulzSec managed to launch numerous successful attacks. At one point, LulzSec was successfully attacking organizations “about once every three to four days” (Poeter, 2011, para. 8). The list of organizations LulzSec targeted is numerous, but includes HBGary, Sony, the US Senate, and the US Central Intelligence Agency (CIA). DDoS attacks, website defacements, and unauthorized data releases are all tactics that LulzSec used.

In July of 2011 LulzSec announced that it was disbanding. While the reason for this sudden change was unclear, members of LulzSec attributed the decision to disband to boredom on the part of its members (Murphy, D., 2011, para. 3). Despite this initial claim, in early March 2012 it was announced that Sabu, the leader of LulzSec, had been arrested by the FBI right around the time LulzSec had decided to disband. In fact, Sabu, whose real name is Hector Xavier Monsegur, has been working as an informant for the FBI since being taken into custody (“Hacker ‘Sabu”
worked full nights,” 2012, para. 1). Shortly after this information was made public, a group calling itself LulzSec Reborn announced that it would be continuing the efforts of the original LulzSec group. At this time it is unclear whether LulzSec Reborn is in fact affiliated with the now-defunct LulzSec group, or if it is merely borrowing the moniker (Schwartz, 2012b, para. 10).

**Operation Anti-Security**

Prior to disbanding during the summer of 2011, LulzSec had announced that it would be amalgamating itself with members of Anonymous to participate in Operation Anti-Security, more commonly referred to as simply AntiSec (Albanesius, 2011a, para. 1). Similar to LulzSec, AntiSec focuses its efforts on exposing and drawing public attention to security weaknesses and inefficiencies within the information security industry (Mansfield-Devine, 2011b, p. 6). These attacks serve to embarrass the organizations that have been attacked (McAfee, 2012, p. 29). Targets have included law enforcement agencies, Monsanto, and the US Department of Homeland Security.

**TeamPoison**

TeamPoison, also written as TeaMp0isoN, is a group of hackers that formed in 2009. The group has been associated with a number of anti-US and anti-Israel hacking collectives (Team Poison, 2012, para. 1), and has been a critic of Anonymous and LulzSec. Members of TeamPoison have expressed disapproval of Anonymous and LulzSec, considering them to be scriptkiddies with low hacking ability, and thus undeserving of the media attention they have received (Winter, 2011, para. 1; Team Poison, 2012, para. 6). In addition to illicit hacking efforts, TeamPoison has also stated that it has an interest in holding governments accountable (Winter, 2011, para. 15). Targets of TeamPoison have included LulzSec, the United Nations (UN) and Research in Motion (RIM).

In 2012, TeamPoison announced that it would be working with Anonymous in a campaign called Operation Robin Hood. The intent of this campaign is to acquire credit card information, and make donations to activist organizations using the stolen credit cards (Team Poison, 2012, para. 13). While this may certainly be of concern to credit card holders, it is of an even larger concern to the banks, which would have to refund the hacked accounts. Echoing the need for better security practices, TeamPoison has said that Operation Robin will encourage people to keep their money with secure, not-for-profit, credit unions (Team Poison, 2012, para. 13).

5.7 How groups operate

**Anonymous**

The Anonymous collective is often purported to have a flat hierarchy, with no leader (Carabott, 2011, para. 4). Jordan (2002) asserts that having a flat hierarchy is an ethical statement; advocating the belief that all who participate have something to offer (p. 69). Nevertheless, it has been speculated that there is in fact a core group within the Anonymous collective that is responsible for managing Twitter accounts, producing videos that are posted on YouTube, and
coordinating attacks (Mansfield-Devine, 2011b, p. 5). The alleged leader of Anonymous is an individual named Christopher Doyon, who goes by the alias Commander X (Solyom, 2012, para. 1; Tynan, 2011, para. 1). Regardless of whether or not there is a central body within Anonymous, anyone can identify with Anonymous, and subsequently claim to speak on behalf of the collective. The problem with allowing anyone to identify with Anonymous is that Anonymous’ message is often fractured (Tsukayama, 2012, para. 5; Stryker, 2011, p. 260). For example, there have been instances where members of Anonymous have made threats, such as to take down the Internet, only to have them denounced by other Anonymous members.

Anonymous will often preannounce attacks, distributing poster-like images online and posting videos on YouTube that explain who a target is and why they were selected (Stryker, 2011, p. 260). These posters and videos allow Anonymous to issue threats to the target and draw attention to the particular issue in question. They also serve as recruitment tools, allowing Anonymous to mobilize and organize willing participants in preparation for an attack (Schwartz, 2012a, para. 8). Although Anonymous originally organized itself using the 4chan message board, the collective now primarily uses Internet relay chat (IRC) channels to coordinate attacks (“Anonymous hacking group uses IRC channels,” 2011, para. 10).

The PLF, LulzSec, and TeamPoison

For groups such as the PLF, LulzSec, and TeamPoison, there is not a great deal of literature about how they operate. It is known that these groups are much more concentrated than Anonymous, and are only comprised of a handful of select individuals (Poeter, 2011, para. 12; Team Poison, 2012, para. 1). Also, unlike Anonymous, it is understood that the PLF, LulzSec, and TeamPoison do have designated leaders. Commander X, the alleged leader of Anonymous, is the admitted leader of the PLF. Sabu was the leader of LulzSec, but it is unclear who, if anyone, is leading the group now. The leader of TeamPoison is an individual who goes by the alias TriCK.

The PLF, LulzSec, and TeamPoison also appear to be much more covert in their operations than Anonymous. Given that these groups are comprised of a few select individuals, and do not attempt to recruit persons for cyber attacks, it is not surprising that they are much less public. Although merely speculative, it can be assumed that these groups, like Anonymous, communicate and coordinate attack online via IRC channels, or similar online messaging programs.

5.8 Techniques

There are a number of techniques that hacktivists use to conduct cyber attacks. Brute force attacks, SQL or XSS code injections, and DDoS programs are some of the more common methods by which cyber attacks are committed. It is important to acknowledge that many of these techniques are not sophisticated, and are in fact largely rudimentary (Montalbano, 2011, para. 1; McAfee, 2012, p. 29). Because the level of programming knowledge that is needed to commit a number of these attacks is minimal, the success of hacktivist attacks can often be attributed to poor security defenses on the part of the target, rather than to the skill of those
committing the attacks (Bradley, 2011b, para. 5). This is not to suggest however that there are not hacktivists who do possess high levels of hacking and programming skills.

**Brute force attack**

A brute force attack is a deliberate attempt to gain unauthorized access to a network or user’s account by testing all possible passwords against a particular username. While a brute force attack can be done manually, this can be extremely time consuming and difficult if the password is complex. For that reason, there are brute force attack software programs that have been developed and made available for purchase and download. These programs are able to cycle through possible passwords much more quickly than can be done manually. Examples of brute force attack programs include Bruteforcer and Md5.

If a brute force attack is successful, the individual who orchestrated the attack may gain unauthorized access to a network, or a user’s emails, passwords, internal documents, or other such data. While the notion of a brute force attack may be somewhat alarming, this method of intrusion will only work if a login does not have a limit on the number of failed entry attempts that are permitted. For example, if an account is automatically locked after six failed password attempts, an intruder will be prevented from testing any additional passwords.

**SQL and XSS injection**

Two other methods for gaining unauthorized access to websites or databases are SQL and XSS injections. SQL and XSS injections will only work against websites or databases that are using the corresponding programming language. These methods entail finding coding errors or vulnerabilities in a website or database, and injecting commands into the existing code (Temple, 2011, para. 6). If someone is able to find coding errors or vulnerabilities, he or she may gain unauthorized access to the targeted website or database. While SQL and XSS injection vulnerabilities can be searched for manually, there are also software programs available that can do this as well. Examples of automated programs that search for coding vulnerabilities include Pixy, Hajiv, Acunetix Scanner, and Nikto Scanner (Schwartz, 2012a, para. 6).

Successful SQL and XSS injections may allow an attacker to deface a website, redirect users to a different website, or provide an attacker with access to internal databases (Trend Micro, 2010, p. 2). Because databases can include usernames, passwords, credit card information, email addresses, and other personal information, the breach of a database can have serious consequences. Recognizing this, it is a common security practice to ensure that information stored in databases is encrypted (Temple, 2011, para. 6). This ensures that even if a SQL or XSS injection is successful, an intruder will not be able to access the stored information. If data is not encrypted though, an intruder may have open access to all information contained within the breached database.

**DDoS programs**

Although DDoS attacks can be orchestrated through the use of botnets (“Hackers of the world unite,” 2011, p. 8), or conducted by manually sending multiple requests to a website, DDoS
programs have also been developed to automate the process. The Floodnet program used by the EDT group in 1998 is one of the earlier examples of a DDoS program. Another DDoS program, which has been popularized by Anonymous, is a program known as the Low Orbit Ion Cannon (LOIC). The name for this software is taken from the Command and Conquer computer game franchise. The LOIC program can be downloaded by anyone, and requires no skill to use. Users simply input a target’s Internet protocol (IP) address, and push the ‘fire’ button (Mansfield-Devine, 2011a, p. 5). Yet in order to be effective, a DDoS attack using the LOIC requires the involvement of multiple parties (Norton, 2011b, para. 24).

Figure 4. Screenshot of the Low Orbit Ion Cannon program

A JavaScript version of LOIC has also been developed, known as LOIC2. LOIC2 works as a web page that executes a DDoS attack against a pre-determined target when users visit the page (Schwartz, 2012a, para. 9; Mansfield-Devine, 2011a, p. 6). This approach is interesting as it does not require users to download the LOIC program. Rather, users simply follow a link to the page and automatically become involved in the DDoS attack. Given that the link to an LOIC2 web page may be unsuspecting though, there is the likelihood that some of the participants in an LOIC2 DDoS attack may have become involved inadvertently (Peckham, 2012, para. 2). This approach within hacktivism is quite new, first appearing in January 2012, and illustrates a somewhat underhanded approach to orchestrating DDoS attacks.

A 2012 study by Imperva, a US security company, suggests that Anonymous tends to launch DDoS attacks only if application weaknesses and other vulnerabilities, such as SQL or XSS coding errors, are not found (Schwartz, 2012a, para. 10). This revelation suggests that DDoS attacks are somewhat of a tool of last resort, and that hacktivists may prefer other techniques for committing cyber attacks.

This chapter has provided an overview of how socially and politically motivated cyber attacks have developed since the late 1980s. A number of specific incidences were discussed, highlighting the tactics that have been used to commit such attacks and the motivations behind them. This chapter also looked at a number of the more prominent groups involved in

hacktivism, how they operate, and the types of techniques they employ to conduct cyber attacks. Chapter Six will discuss whether or not hacktivist attacks appear to be increasing, and will look at what has been said about governments in general being a potential target for hacktivists. The chapter will also discuss some of the factors that may trigger hacktivist attacks, and the effect a successful attack may have upon a targeted organization. Lastly, Chapter Six will look at some of the trends within hacktivism today, and provide examples of relevant hacktivist cyber attacks.
Chapter 6: Hacktivism Today

6.1 Increasing or decreasing

When the word hacktivism is used to refer to various phenomena, such as malicious cyber attacks and cyber pranks, it becomes difficult to discern whether or not hacktivism, as defined in this report, is in fact increasing. If any form of cyber attack is branded as hacktivism, regardless of whether or not it the attack has a social or political motivation, hacktivism becomes a misleading and hackneyed phrase. As such, there is currently a great deal of ambiguity over the extent to which hacktivism has grown over the last few years. While some have asserted that hacktivism is a growing and serious risk to information security, others have denounced such claims.

Several academics and analysts argue that hacktivist attacks are continuing to grow in frequency and severity (Dayal, 2012, para. 4; Boni & Kovachich, 1999, p. 179; Temple, 2011, para. 3; Dickinson, A., 2011, para. 6). Because hacktivist attacks are socially or politically motivated, rather than financial, organizations that may have been immune to financially motivated attacks may now find themselves the targets of hacktivists (Information security forum, 2011, p. 2). Further, Anderson (2008) proposes that third parties may find themselves increasingly the target of hacktivist cyber attacks (p. 11). This suggests that an organization may be targeted by hacktivists because of who its business partners are, or because it may have data pertaining to the primary target.

McAfee Labs (2011) has even gone so far as to state that in the coming year, public figures such as politicians and law enforcement officers will increasingly become the victims of hacktivist cyber attacks (p. 4). This perception, which is largely speculative, is based on the belief that technological development will make it much easier for individuals to participate in politically or socially motivated cyber attacks (“4 signs ‘hacktivism’ has gone mainstream, 2012, para. 1; Anderson, 2008, p. 11). While it is true that IM/IT development does provide a new avenue by which organizations may be vulnerable to attack, this outlook seems to assume that there is not only a growing number of discontented members within society, but that they are also willing and able to commit hacktivist attacks.

It has also been suggested that individuals may be drawn to participate in hacktivism due to the perceived lack of risk that they assume (Information security forum, 2011, p. 1). This belief is supported by the fact that the number of persons who have been arrested for participating in cyber attacks is quite low; less than one percent of all cases (Menn, 2011, para. 33). Adopting the mentality that there are simply too many people committing hacktivism for the authorities to prosecute every individual involved (Mansfield-Devine, 2011a, p. 7), participants in hacktivism may believe that they are generally invulnerable to prosecution. The arrest of five members from Anonymous in early March, 2012 (Wong & Sachdev, 2012, para. 1) indicates that this may not necessarily the case.

Somewhat contrary to the assertion that incidents of hacktivism are increasing, there is the argument that hacktivism, and the susceptibility of organizations to cyber attacks, has merely been exaggerated and dramatized (Jordan & Taylor, 2004, p. 21; Hansen & Nissenbaum, 2009,
For example, Dvorak (2011) claims that there has been no outbreak of hacktivism whatsoever (para. 3). Instead, Dvorak states, hacktivism and other forms of cyber attack have simply become more prominent because of the media, who are now able to attach names, such as Anonymous, to cyber attacks when they occur (para. 4). Accordingly, the perception that hacktivism is increasing may simply be the result of the media’s efforts to sensationalize the phenomenon. This is not to suggest that hacktivism is something that organizations should simply overlook though. The fact still remains that hacktivism is occurring, and cyber attacks can pose a risk to organizational and information security.

Website defacements and website redirects, although embarrassing for an organization, are temporary and easily fixed. It is data breaches that are perhaps the most potentially damaging to an organization. As the discussion thus far has illustrated, the release of sensitive documents and personal details of employees and web users may be detrimental to an organization’s credibility and reputation, as well as to the security of those who have had personal information stolen. Pastebin.com, an online resource where users may store and publish text online, has frequently been used by hacktivists to post information attained from data breaches. Information posted on Pastebin can be made accessible to anyone on the Internet. Recognizing the serious implications that the publication of sensitive materials may have, the owner of Pastebin announced in early April 2012 a plan to improve his company’s ability to manage and remove unauthorized data releases more quickly (Leyden, 2012, para. 1). The increased efforts of Pastebin to impede the efforts of hacktivists supports the notion that instances of hacktivism are increasing, and that the efforts of hacktivists can have serious implications.

According to a survey released by Verizon Communications Inc. in March 2012, incidents of external data breaches dramatically increased in 2011, and hacktivists were responsible for 58% of all data breaches that occurred (Finkle, 2012, para. 1). Verizon’s analysis was based upon 855 data breach incidents. This strongly implies that hacktivism is a growing, and serious, threat. However, it is of value to note that the scope of the study was limited to Australia, the US, the Netherlands, Ireland, and England. Further, Verizon only defines hacktivists as activist groups that conduct cyber attacks (Verizon Communications Inc., 2012, p. 17), yet offers no explanation as to what ‘activist groups’ denotes. As such, the findings of Verizon’s study may be somewhat misleading.

An earlier study, released by Telus Corp. and the University of Toronto’s Rotman School of Management in November 2011, found that the number of external breaches amongst government bodies in Canada was down nearly 25% since 2010 (Berkow, 2011, para. 4). Of these breaches, 42% were the result of insider breaches (Berkow, 2011, para. 4). The other 58% of breaches were not attributed to merely hacktivists though, but also cyber criminals (“Hackers target Canada,” 2011, para. 6). These findings seem to somewhat contradict Verizon’s findings that external data breaches are occurring more frequently, and that the majority of data breaches are the result of hacktivist efforts. These differences illustrate the

---

10 In response to the efforts of Pastebin to curb unauthorized data releases, members from the Anonymous collective and the PLF jointly created an alternative to Pastebin in April 2012, known as AnonPaste. Information published on AnonPaste is not censored, and information about the users who publish information is not made available to authorities (Kelion, 2012, para. 9; Geuss, 2012, para. 1-2).

11 In 2011 there was an average of 17 government breaches, compared to 22 in 2010.
difficulty of discerning the exact threat that hacktivists may pose to government organizations, and the conflicting views that exist within the security industry.

Jordan (2002) points out that socially and politically motivated campaigns tend to fail if they do not have the support of existing social institutions (p. 35). While many political and law enforcement groups have condemned hacktivism, the general public seems to be much more accepting of the phenomenon. For example, on March 25th, 2012, #ILoveAnonymous began trending on Twitter. At its peak, #ILoveAnonymous was the fourth most popular trending topic worldwide on Twitter. While some of the tweets with this hashtag were critical of Anonymous, the majority of them were positive (Walton, 2012, para. 2). Supportive tweets praised Anonymous for defending people’s rights, holding governments accountable, and fighting against corporations. While this should by no means suggest that public support for Anonymous is universal, it does illustrate that public support for Anonymous does exist, and seems to be increasing.

6.2 Government as a target

Governments make decisions, develop regulations, and set policies; many of which impact the daily lives of the average person. Because everyone is not always going to agree with a government’s actions, government bodies can become the targets of criticism and public protest. Petition campaigns and public demonstrations are just two of the ways individuals can express their opposition to a government. The issues which may motivate an individual to protest in the street against a government though may easily be transferred into the realm of hacktivism (Hammack, personal communication; as cited in Smith, 2011, para. 3). The wealth of information that government bodies are responsible for managing, coupled with the financial and resource limitations that many governments face, further increases the vulnerability of governments to the efforts of hacktivists (Vegh, 2003, p. 92). If a government becomes involved in a contentious issue or is considered to have infringed upon people’s rights (Manion & Goodrum, 2000, p. 14), there is the risk that it may become the target of hacktivists.

Hacktivists may also target governments because of their high profile in society (Boni & Kovacchich, 1999, p. 99; Vegh, 2003, p. 92). For example, individuals or groups may target government organizations simply because they have a general disdain for government and bodies of authority. A successful cyber attack against a government website or server may be seen as much more impactful or rewarding than an attack against a smaller, less public, organization. Further, governments may simply be seen as more deserving of the public embarrassment that may come along with a successful cyber attack. Again though, in order to be considered an act of hacktivism, the cyber attack must have some sort of social or political motivation.

Groups such as LulzSec, TeamPoison, and the Anonymous collective have published statements condemning the activities of all governments. Accusations of governments lying to their citizens, infringing upon people’s rights, and widespread corruption (“Anonymous and LulzSec security statement,” 2011, para. 5; AntiSec, 2011, para. 4; Rashid, 2011, p. 2) are just some of the criticisms that have been made. It is interesting to note that these comments advocate the understanding all governments are intrinsically bad. For example, a tweet that was issued on
behalf of the Anonymous collective asserted that “[n]o modern government is innocent” (Anon_Central, 2012a).

Figure 5. Screenshot of the tweet from the Anon_Central twitter account

If all governments are assumed to be guilty of wrongdoing, any government body can then be considered a potential target of hacktivists. Anderson (2008) notes that a government may become the target of hacktivists because of the perception that the government is corrupt, or any other similar criticism, regardless of what is actually true (p. 11). The claim that governments are somehow the enemies of hacktivists (“Anonymous and LulzSec security statement,” 2011, para. 6) only reinforces the notion that hacktivists should target governments. This understanding is supported by the efforts of the AntiSec movement, which explicitly encourages individuals to target governments and expose wrongdoing (Albanesius, 2011c, para. 12).

6.3 Triggering hacktivist attacks

According to Boni and Kovachich (1999) there is general desire within hacking culture to defy authority, cause disruption, and respond to challenges (p. 77). It is these values which seem to stimulate the confrontational tactics used by hacktivists today. Yet given the array of organizations that have been targeted by hacktivists, and the different tactics that have been used, the rationale and motivation behind hacktivist attacks “are almost never reducible to a common cause” (Krapp, 2005, p. 73). Still, there are also a number of specific and recurring issues that hacktivists today are targeting in many of their attacks: freedom of speech; privacy rights; intellectual property freedoms; and access to free or open source software (Samuel, 2004, p. 42). Tying into these issues is a valuing of open access to information, and a general disdain for censorship.

Many hacktivists have carried out cyber attacks in an attempt to draw attention to efforts that would curb the freedom of Internet users (“4 signs ‘hacktivism’ has gone mainstream, 2012, para. 16). Attempts to reduce online anonymity or regulate and filter the Internet are two examples of online issues that hacktivists have confronted. Hacktivists have also engaged in issues that do not directly relate to the Internet, such as police brutality and government corruption. This illustrates that participants in hacktivism seem to be concerned with defending

---

12 Tweet available at http://twitter.com/#!/Anon_Central/status/157066096678154240
democratic freedoms, both in the real world and online. However, the tactics used by hacktivists are limited to the latter.

As Vegh (2003) observes, it is usually a particular incident that triggers activism online (p. 73). Although not always the case, hacktivists tend to involve themselves in issues when there has been some sort of change to the status quo, or a sudden infringement upon people’s rights and freedoms is perceived to have taken place. As such, the question has been raised whether or not hacktivist collectives such as Anonymous should be considered agents of change or merely reactionary (Wlasku, 2011, para. 13). Examples of possible triggers include the introduction of new legislation, the implementation of certain policies, or the arrest of hacktivists. There are a number of contentious issues that hacktivists do not appear to have engaged in though, including genocide, poverty, sweatshops, or pollution offences. Stryker (2011) suggests that collectives such as Anonymous are simply more concerned with online offenses than other issues (p. 266). However, this view overlooks hacktivist attacks that do not appear to have been motivated by so-called online offenses. Nonetheless, it remains unclear as to why hacktivists choose to engage in some issues but not others.

6.4 Implications of an attack

Public embarrassment, a slight to an organization’s reputation, and the costs of a data breach are three of the more prominent challenges that may arise from a hacktivist attack. While security companies such as Trend Micro and Symantec allege that hacktivism poses a serious threat to governments and corporations, Mansfield-Devine (2011b) contends that there are simply too many factors associated with hacktivism to identify all of the implications of a single incident (p. 11). The overall implications of an attack may depend upon the type of organization that is targeted, the tactic that is used in an attack, and what, if any, information an intruder is able to glean. Auty (2004) provides three criteria for determining the overall effect of a hacktivist attack: “how much nuisance was caused; how widely it was covered (in the press); and, fundamentally, did anything change as a result?” (p. 219). It can be understood that the amount of disruption caused by a hacktivist attack will depend upon the tactic that is used. In regards to the third component, change can be assumed as referring to both the organization that was attacked and society as a whole.

While it has been suggested that the efforts of hacktivists have largely failed to bring about long-term policy change (Auty, 2004, p. 219), this view seems to neglect the fact that the intent of hacktivism is to increase public awareness of a particular issue or concern, rather than directly bring about change (Wlasku, 2011, para. 27). One key implication of hacktivism is that it has highlighted the generally poor state of information security amongst organizations (Ghosh, personal communication; cited in Rashid, 2011, p. 2; Vamosi, 2011, para. 6; Menn, 2011, para. 3). It is for this reason that organizations seem to be putting more of an emphasis on addressing and correcting potential security vulnerabilities in their systems. For example, Sony, which has had its security system compromised numerous times over the last few years, recently announced that it would be restructuring its security system. It is interesting to note that Sony’s new model will put more of an emphasis on mitigating the risks posed by hacktivists in particular (Pauli, 2012, para. 1).
Whether it is the defacement of a website, website redirection, a DDoS attack, or an unauthorized data release, a hacktivist attack may be quite embarrassing for the affected party (Himma, 2008, p. 202). In addition to being disruptive, a hacktivist attack may illustrate gaping security vulnerabilities within an organization’s information security system. This may consequently reduce people’s confidence in the organization to manage information securely (Auty, 2004, p. 217), which can be destructive to an organization’s reputation and credibility (Boni & Kovachich, 1999, p. 16; Dayal, 2012, para. 4). For organizations that manage vast amounts of sensitive data, or pride themselves as leaders within the security industry, a hacktivist attack may negatively impact the organization in the long-term.

It would be remiss to suggest that website defacements, website redirects, DDoS attacks, and data breaches may have equally as great an impact upon organizations. Website defacements, website redirects, and DDoS attacks all have short-term consequences that are entirely amendable. Yet such attacks may easily become sensationalized by the media (Anderson, 2008, p. 7). As a result, a relatively low-key hacktivist attack may become a popular topic of discussion. Although the direct consequences of an attack may be minimal, media coverage of the attack may serve to bolster the embarrassment of the organization that was targeted.

In a 2011 study from the Ponemon Institute, which was sponsored by Symantec, it was estimated that a data breach will cost organizations, on average, $5.5 million, or approximately $194 for each record that is compromised (Constantin, 2012, para. 2). The Ponemon Institute’s calculation takes into account the projected notification, legal, and lost-business costs associated with a data breach. Factors incorporated in this calculation13 include an organization’s industry classification, the types of information an organization manages, and the authentication measures used to protect data. For reasons that are unclear, this calculation also takes into account what the respondent considers to be the most likely cause of a data breach. The possible answers for this question are entirely subjective, and may by no means reflect reality. Nevertheless, how a respondent answers this question will alter the estimated cost of a data breach. Accordingly, the Ponemon Institute’s projected data breach costs may not be accurate.

Another issue regarding the Ponemon Institute’s estimate is that it assumes all data involved in a data breach is of the same level of significance. While there are certainly instances of data breaches that have involved sensitive materials, much of the data that has been leaked by hacktivists has been low-grade and of relatively low significance (Mansfield-Devine, 2011b, p. 9). If the information that is leaked is nonessential or already largely public, it is more likely that a data breach will be inconvenient or embarrassing for an organization (Himma, 2008, pp. 201-202), rather than costly. Accordingly, it may be somewhat erroneous to assume that, on average, each compromised record will cost an organization approximately $194. Because the costs associated with a data breach will vary, depending on the type and amount of information that is released, the overall financial impact of a data breach will not be comprehensible until after a data breach has occurred.

Interestingly, the Ponemon Institute’s 2011 report found that the average data breach costs had decreased from $7.2 million in 2010 to $5.5 million in 2011; a difference of 24%. This suggests

13 An online version of the Ponemon Institute’s Data Breach Calculator can be found at https://databreachcalculator.com/GetStarted.aspx
that the costs associated with data breaches are perhaps becoming less severe. The joint Telus-Rotman study (2011) supports this notion, having found that the costs of data breaches decreased in all organization types in Canada between 2010 and 2011 (p. 2). For example, the study found that the average cost of a government data breach fell 27% between 2010 and 2011\(^4\) (Telus-Rotman, 2011, p. 3). While these findings should not imply that data breaches are a matter of little consequence, they do suggest that the costs associated with data breaches are decreasing.

Although data breaches do occur for criminal and malicious purposes, the overall intent of hacktivist data breaches is to embarrass the organization by highlighting its poor information security. This sentiment is supported by the fact that rather than keep the information for themselves, hacktivist often publish the stolen information online (Samuel, 2004, p. 11). If high-grade information is released, such as an organization’s internal project plans, it can be extremely damaging to an organization’s ability to operate and compete (Boni & Kovachich, 1999, p. 14). Releasing data of this calibre may be the most destructive to an organization. In the event of a data breach, there is also the potential that released data may be represented entirely out of context or misinterpreted (“Anonymous called hard to kill,” 2012, para. 3). For example, an email from a disgruntled employee may only illustrate one side of an issue. Although this in itself may not necessarily be costly to an organization, it may certainly contribute to the on-going embarrassment and scrutiny attached to the initial data breach.

The unauthorized disclosure of low-grade information, such as an employee’s name, address, or email address, may have less of an impact on an organization’s stability. Nevertheless, it can still have a serious impact upon those who have had their personal information released. For example, data releases may increase the likelihood that individuals become the victims of spamming or ID theft (Feinmann, personal communication; as cited in Acohido, 2012, para. 10; Mansfield-Devine, 2011b, p. 10). For individuals in certain careers, such as law enforcement, the unauthorized disclosure of information could even endanger lives (Vamosi, 2011, para. 13). As such, while the intent of a hacktivist attack is to draw attention or protest a political or social concern, there may in fact be serious risks and unintended implications associated with unauthorized data releases.

### 6.5 Current trends

Looking at the instances of hacktivism that have taken place over the last few years, there are a number of recurring issues that have galvanized hacktivists to commit cyber attacks against governments and private corporations. In fact, it appears that the majority of recent instances of hacktivism may be understood as fitting into one of seven categories: privacy concerns; perceived instances of censorship; alleged corruption; elections; wrongdoing on the part of law enforcement; retaliation for arrests of alleged hacktivists; and general contempt. While there may be instances where hacktivist attacks do not clearly align with any one of these categories, these seven trends seem to be the most common reasons why hacktivists are motivated to commit cyber attacks. The examples drawn upon for this section are intended to demonstrate the range of organizations that have been targeted by hacktivists, but by no means provides an exhaustive list.

---

\(^4\) According to the Telus-Rotman study, the annual cost of a government data breach in 2011 was $58,929, compared to $80,910 in 2010.
of recent hacktivist attacks. For a timeline of the events discussed in this chapter, please see Appendix 3.

6.5.1 Privacy

One of the major issues that hacktivists have addressed is Internet surveillance. Any form of Internet surveillance, either by a government or a private corporation, is seen as an infringement upon a person’s right to anonymity and privacy online (Jordan, 2002, p. 131; Levesque, 2006, p. 1209). It is felt that privacy online provides individuals the security to use the Internet as they see fit, without interference (Amis, 2001, para. 4). Further, online anonymity is often considered a vital tool for promoting freedom of speech, and allowing individuals the ability to express their views and ideas online without fear of retribution (Levesque, 2006, p. 1204; Jordan, 2002, p. 131; Amis, 2001, para. 6). If online privacy is infringed upon, people may be reluctant to voice their opinions or beliefs, or even use the Internet as they normally would. Accordingly, there have been several examples over the last few years where hacktivists have targeted organizations that are considered to have infringed upon people’s right to privacy online.

Fine Gael

In January 2011, the election website for Fine Gael, an Irish political party, was defaced by members of the Anonymous collective. Included in the website defacement was the changing of the page’s message so that it read “The problem with politicians is they lie” (“Fine Gael website defaced,” 2011, para. 4). Additionally, the personal data of approximately 2,000 people who had registered with the website had been compromised in the attack (“Teenagers arrested over Fine Gael website hack,” 2011, para. 5). Given that the Irish general election was scheduled for February of that year, this attack initially seemed to be politically motivated (McDonald, 2011, para. 6).

While there may certainly have been some political motivation on the part of the hacktivists who participated in this attack, it is interesting to note that two days before the attack TheJournal.ie, an Irish news website, reported that the Fine Gael website was housed on servers in Miami (“Fine Gael website defaced,” 2011, para. 10). This consequently raised concerns over whether or not Fine Gael was in compliance with Ireland’s Data Protection Act (“Fine Gael website defaced,” 2011, para. 11). By storing Irish citizens’ information in the US, the US government may have been able to access that data. It seems likely then that the attack was carried out as a reprisal for this perceived slight to people’s privacy and security. Given that TheJournal’s report also found that a number of other Irish political party websites were also housed in the US (“Smart economy,” 2011, para. 4), it remains unclear as to why Fine Gael alone was targeted. Perhaps Fine Gael was targeted for both political and privacy reasons.

The lack of clear intent on the part of those who committed the attack against the Fine Gael website makes this a somewhat lacking example of hacktivism. Yet it does highlight how a particular incident, in this case the report from TheJournal, may have triggered a hacktivist attack. Moreover, the implicit effort to embarrass Fine Gael, rather than cause grievous harm, does support the notion that this attack can be categorized as hacktivism.
Booz Allen Hamilton

Booz Allen Hamilton is an American management and technology consulting firm that has worked with the US government and military. In July 2011, the Booz Allen Hamilton website was breached, and an unauthorized user was able to access the log-in credentials, such as usernames and passwords, for 90,000 military employees (Rashid, 2011, p. 3). All of this information was published online soon thereafter.

It is understood that the attack was prompted by Booz Allen Hamilton’s on-going work for the US government. The company’s “participation in government surveillance and intelligence-gathering programs” (Rashid, 2011, p. 3), coupled with an alleged campaign to intentionally spread disinformation (“Hacked off,” 2011, para. 2), appear to have been the motivating factors behind the attack. For individuals concerned with protecting their privacy, the efforts of Booz Allen Hamilton may certainly have been considered worrisome.

Research in Motion

In August 2011 a series of riots broke out across England following the police shooting of a man named Mark Duggan. During the post-riot investigation, British authorities approached RIM, requesting its assistance. It was alleged that many of the rioters had used RIM’s Blackberry instant messaging service to coordinate riot activities (“England riots,” 2011, para. 3), and that Blackberry would be able to help identify those individuals.

After the company’s agreeing to assist with the investigation, members of TeamPoison defaced RIM’s Blackberry website. TeamPoison threatened to publish the personal information of RIM staff if the company provided authorities with user data (“England riots,” 2011, para. 2, 9). It was argued that providing information to police would be an infringement upon people’s privacy, and could lead to innocent people being targeted in the investigation (“England riots,” 2011, para. 8). Despite this threat, there was no retaliation on the part of TeamPoison when RIM did follow through with its offer to cooperate with the investigation.

Facebook

An individual purporting to be a member of the Anonymous collective posted a video on YouTube in January 2012, threatening to temporarily take down the Facebook website. The stated reason for the threat was ongoing issues regarding Facebook’s privacy policies (Tsukayama, 2012, para. 3). Shortly thereafter, other members of the Anonymous collective denounced the threat (Tsukayama, 2012, para. 1). Perhaps for this reason no attack against Facebook was executed.

The threat made against Facebook is an excellent example of how Anonymous’ message is sometimes fractured and discordant. While there has certainly been criticism of Facebook’s efforts to protect user privacy (Vascellaro, 2010, para. 1), there does not appear to be a great deal of support to launch a cyber attack against the social networking website; although the reason for this is not clear. Yet despite the fact that no attack was ever launched against Facebook, the
issuing of the threat did draw public attention to concerns surrounding Facebook’s privacy policies.

Bill C-30

In February 2012, the Government of Canada introduced the Investigating and Preventing Criminal Electronic Communications Act; more commonly referred to as Bill C-30. The proposed legislation would “allow police to access basic personal information about Internet users without first obtaining a warrant” (Mackrael, 2012, para. 3). Public opposition to the Bill began to grow, declaring the proposed legislation excessive and unnecessary (Mackrael, 2012, para. 3). In an attempt to curb criticism of the Bill, Public Safety Minister Vic Toews stated that critics could either stand with the Federal Government or “with the child pornographers” (Baluja, 2012, para. 9).

Provoked by this statement, members of the Anonymous collective posted a video on YouTube threatening to disclose personal information about Vic Toews if the Bill was not abandoned (Mackrael, 2012, para. 1; Baluja, 2012, para. 12). This campaign was called Operation True White North. Personal information about Vic Toews’ divorce had previously been published on the now-defunct @vikileaks30 twitter account15. A statement was also published on Pastebin16, again threatening to release information about Vic Toews. Included in the Pastebin statement was an email address to which users would be able to send information about Vic Toews.

In response to this strong backlash, Bill C-30 was sent before a committee to be reviewed and amended. While Vic Toews strongly criticized Anonymous for threatening him and his family, Ned Franks, a constitutional scholar and professor at Queen’s University, testified before the House of Commons that such threats to politicians have always existed (Baluja, 2012, para. 8). At the time of writing, Bill C-30 is still under review.

6.5.2 Censorship

Although a topic of concern for many people, censorship is an issue that is particularly important to hacktivists (Hill & Hughes, 1998, p. 42; Vegh, 2003, p. 77; metac0m, 2003, p. 1). Censorship can be understood as the intentional effort to ban or filter certain types of data and information. It can also include efforts to withhold information, impede people’s freedom of expression, or prevent individuals from accessing or sharing information and technology (metac0m, 2003, p. 1). As Hill and Hughes (1998) note, information is a vital component of any democracy (p. 2). Thus, to some, efforts to control or limit information and technology may be viewed as incompatible with democratic principles.

Australian government

Members of the Anonymous collective launched a series of DDoS attacks against several Australian government websites in 2010. The website for the Australian Prime Minister, Kevin

---

15 It was later determined that Adam Carroll, a Liberal staffer, was responsible for creating the @vikileaks30 Twitter account.

16 A copy of the statement can be found at http://pastebin.com/JbEFyGGh
Hacktivism and the Government of British Columbia

Rudd, and the Australian Communications and Media Authority website were both targeted in the attack. The campaign, known as Operation Titstorm, was in response to the government’s plan to require Australian Internet service providers to block certain content online (Zetter, 2009, para. 1). Content that would be filtered included child pornography, and images depicting rape and bestiality (Zetter, 2009, para. 9). The proposed legislation also included pornographic images of small-breasted women, as they could be mistaken for images of children (Hasham, 2011, para. 19).

While participants in the attack viewed the government’s plan as an unwarranted attempt to regulate the Internet (Anonymous, as cited in Kravets, 2010, para. 4), the Australian government argued that the attack was misguided (Zetter, 2009, para. 9). Following Operation Titstorm, real-world protests were held. These protests were known as Project Freeweb. In response to a number of concerns regarding the legislation, a Senator in the Australian government ordered that the legislation be brought before a committee for review (Foo, 2010, para. 3). To date there has been no progress made with the plan to filter Internet in Australia.

**Bay Area Rapid Transit, San Francisco**

In July 2011 a homeless man named Charles Hill was shot and killed by transit police who worked for San Francisco’s Bay Area Rapid Transit (BART). Officers involved in the shooting alleged Hill had knives and had threatened police officers; a claim which witnesses have denounced (Eskenazi, 2011, para. 4-5). Provoked by the perceived instance of excessive force by police, members of Anonymous organized weekly protests at BART stations (Sherbert, 2011a, para. 5). Protestors blocked fare gates and entrances to stations, and disrupted BART passengers who were commuting (Sherbert, 2011d, para. 2).

Prior to one planned protest, cell phone service throughout BART stations was shut down. This was done in an attempt to disrupt individuals who were coordinating the scheduled protest (Sherbert, 2011b, para. 4). Linton Johnson, a spokesman for BART, was the individual who admittedly came up with the idea. As a result, the scheduled protest did not happen. Shortly thereafter, members of the Anonymous collective defaced the BART website, and published personal information about hundreds of BART customers online (Burack, 2011, para. 1). Although members of Anonymous did issue an apology to people who had their information released, they suggested affected persons contact BART officials to “ask them why [their] information wasn’t secure with [BART]” (Burack, 2011, para. 7).
Anonymous then went on to provide BART officials with a list of demands that needed to be met before the protests would stop. The demands included firing Johnson, taking guns away from BART transit police, and issuing a public apology for shutting down cell phone service (Sherbert, 2011a, para. 3). Before BART officials had an opportunity to respond to the demands, members of the collective released racy photos of Johnson\(^\text{18}\), one of which included a “full-frontal view of his genitals” (Sherbert, 2011b, para. 2). While it was initially unclear how Anonymous had attained the images, members involved in the release later claimed that the photos were acquired from Johnson’s personal website (Sherbert, 2011c, para. 1), and were thus already publicly available.

The clash between Anonymous members and BART is a unique example of hacktivism, as the campaign also included real-world protests and the publication of data that were already publicly available. Interestingly, it was not until Linton Johnson blocked cell phone services throughout BART stations, and thus prevented the free and open exchange of ideas and information, that members of the Anonymous collective resorted to hacktivist tactics. Overall, the efforts of Anonymous members served to disrupt BART operations, highlight security vulnerabilities in BART’s system, and publicly shame the individual who had attempted to hinder the protests.

**Sony**

In 2011 the Stop Online Piracy Act (SOPA) was introduced before the US House of Representatives. The Act was designed to combat the unlawful exchange of copyrighted materials online, such as music and movies, by extending the ability of law enforcements groups and copyright holders to seek legal recourse (Sumner, 2012, para. 6). While SOPA was supported by many organizations in the film and music industries, there was also a great deal of opposition to the Act. Critics maintained that the Act was excessive and impeded free speech.

---


\(^{18}\) The release of the photos was accompanied by a message that read: “If you are going to be a dick to the public, then I’m sure you don’t mind showing your dick to the public” (cited in Sherbert, 2011b, para. 3).
over the Internet (Kanjilal, 2011, para. 1). In a video posted on YouTube, Anonymous declared that SOPA would prevent people from sharing information freely online, and was thus a form of censorship that would not be tolerated (Anonymous, 2011a).

Sony is one company that had articulated its support for SOPA. Largely due to this support, Sony became the target of the Anonymous collective (Sumner, 2012, para. 1). In early January 2012, the website for Sony Pictures and the Sony Facebook page were defaced by members of Anonymous (Humphries, 2012, para. 3). Although the effects of the attacks were only temporary, the attacks signified the willingness of Anonymous members to target organizations that supported SOPA; and thus censorship on the Internet. As criticism of SOPA become much more pronounced in the weeks after the attack against Sony, the House of Representatives announced that its plans to draft the SOPA legislation would be postponed indefinitely.

**Operation Megaupload**

While the issue of SOPA was still on-going in the US, the US federal government exercised an international warrant to bring down Megaupload.com, an online file sharing service, and arrest its employees. Megaupload offered users access to copyrighted material, including music, television shows, and movies, for free or at a relatively low cost. In retaliation for the raid against Megaupload, members of Anonymous responded by launching a series of DDoS attacks against a number of websites. This campaign was known as Operation Megaupload. Websites that were temporarily shut down as a result of these attacks included the Federal Bureau of Investigation (FBI) website, the website for the Department of Justice, and the websites for Universal Music and the Warner Music Group (“Anonymous down government,” 2012, para. 2).

6.5.3 Corruption

Another issue that hacktivists have confronted is corruption. Corruption can be understood as meaning dishonesty or unethical behaviour on the part of governments or private corporations, using one’s power or influence to one’s own benefit, or impeding the democratic process. Statements made on behalf of groups such as LulzSec, AntiSec, and TeamPoison, have strongly articulated the disdain felt for corrupt activities, and the willingness to expose them.

**Operation Tunisia and Operation Egypt**

In 2010 WikiLeaks began publishing hundreds of thousands of classified US diplomatic cables that it had obtained. These cables exposed corruption and human rights abuses on the part of a number of countries, including Tunisia (“Secret US embassy cables,” 2011, para. 6). Already plagued by social and political unrest, the release of the cables sparked massive protests and demonstrations throughout Tunisia (Walker, 2011, para. 2). The issues being protested included widespread unemployment, limitations on freedom of speech, and rampant government corruption (Dickinson, E., 2011, para. 1).

As demonstrations began to spread across Tunisia, anti-government sentiments spilled over into neighbouring countries including Egypt, Libya, and Syria. This wave of uprisings is known collectively as the Arab Spring. Although corruption was only one of the issues addressed during
the series of revolutions, it appears that the issue of government corruption was one of the more prominent. The uprisings in Tunisia and Egypt were two revolutions in particular that attracted the attention of Anonymous members.

Members of Anonymous were initially drawn to the uprising in Tunisia because of government efforts to crack down on dissent and monitor foreign journalists (Stryker, 2011, p. 265). As demonstrations continued, the collective began to actively coordinate their efforts to support the Tunisian demonstrators in their overthrow of their government (“Anonymous hacking group uses IRC channels,” 2011, para. 8). This campaign was known as Operation Tunisia. Tactics used in Operation Tunisia included a series of DDoS attacks, whose targets included the Tunisian president’s website and the Tunisian stock exchange, and disseminating information to Tunisian protestors about how to protect their anonymity online (Stryker, 2011, p. 266; Hasham, 2011, para. 21).

Shortly after the overthrow of the Tunisian president, protests and demonstrations began occurring in Egypt. The grievances of the Egyptian demonstrators mirrored that of Tunisia: unemployment, government corruption, and limitations on the freedom of speech (Knell, 2012, para. 3). As was the case with Operation Tunisia, members of the Anonymous collective worked to curb government efforts to disrupt protests. This campaign was known as Operation Egypt. Throughout the revolution in Egypt, members of Anonymous worked to circumvent sites that had been censored by the Egyptian government, kept Internet servers running, and launched prolonged DDoS attacks against Egyptian government websites (Wlasku, 2011, para. 11; Stryker, 2011, p. 266; “Anonymous hacking group uses IRC channels,” 2011, para. 3).

New Alliance Party, Mexico

In November 2011 the website for Mexico’s New Alliance Party was defaced by members of Anonymous. Prior to the attack, the party had actively been supporting the efforts of the Mexican president’s sister to become elected governor in an upcoming state election (“Mexican party website hacked,” 2011, para. 1). The defaced website showed a video of an individual wearing a Guy Fawkes mask, urging the Mexican people to find and expose evidence of government corruption (“Mexican party website hacked,” 2011, para. 2). Although only speculative, it is possible that the New Alliance Party was targeted because of its support for the president’s sister. Perceived nepotism on the part of the party, or concern regarding a potential conflict of interest, are some of the possible reasons why the New Alliance Party may have been attacked. This notion is supported by the fact that the website defacement coincided with a DDoS attack against the website of the electoral institute responsible for managing the upcoming state election (“Mexican party website hacked,” 2011, para. 3).

Symantec

James Gross, a resident of Washington State, filed a class-action lawsuit against Symantec on January 10, 2012. Symantec is one of the world’s most prominent producers of security software. In the lawsuit, Gross accused Symantec of intentionally disseminating trial versions of their software, such as Norton Security, that would inform users that their computer was infected with malware or suffering from other issues, even when such problems did not exist (Parrish, 2012,
It is alleged that this was done in order to coerce users into purchasing the full versions of Symantec’s software (Parrish, 2012, para. 7). At the time of writing, the lawsuit is still ongoing.

Prior to Gross filing the lawsuit, an individual known as Yama Tough began writing on Twitter that he or she had a copy of the source code for Symantec’s Norton Antivirus program. Yama Tough is a member of a group called Lords of Dharmaraja, which is reportedly affiliated with the Anonymous collective (Daniel & Menn, 2012, para. 5). On January 13, Yama Tough announced his or her intent to release the source code for Norton Antivirus to accompany Gross’ lawsuit (YamaTough, 2012a). This statement was soon rescinded when Yama Tough declared that his or her group first wanted to review the source code themselves to search for potential vulnerabilities in the software (YamaTough, 2012b).

Symantec initially reported that the source code for a number of its programs, including pcAnywhere and Norton Antivirus, had been stolen from a third party’s server (Parrish, 2012, para. 4). Symantec later retracted this statement, admitting that the source code had been stolen during a 2006 breach of Symantec’s own network; an incident which had previously not been disclosed to the public (Keizer, 2012, para. 1; Zetter, 2012, para. 1). Regardless, Symantec maintained that because the source code was five years old, any Symantec customers who were using updated versions of the software would not be at an increased risk from the disclosure of the source code (Daniel & Menn, 2012, para. 8). Others have noted though that the older source code could allow potential hackers to find vulnerabilities within current versions of the software (Rashid, 2012, para. 15).

In early February Yama Tough released portions of the source code for Symantec’s pcAnywhere, Norton Utilities, and Norton Antivirus programs (Fisher, 2012, para. 2). Accompanying the source codes, Yama Tough also published a copy of an email exchange that occurred between him or herself and a supposed employee of Symantec. It was later confirmed that the Symantec employee was actually an undercover law enforcement agent (Zetter, 2012, para. 2). The email exchange seems to depict Yama Tough’s failed attempt to extort $50,000 from Symantec as payment to not release the source codes. Yama Tough has subsequently asserted that the extortion attempt was merely a ploy to embarrass Symantec further, and that there was never any intention to take any money (Daniel, 2012, para. 11).

If Yama Tough was in fact attempting to extort money from Symantec, this example would not qualify as an instance of hacktivism, as defined in this report. Yet, because Yama Tough insists that the extortion attempt was merely a ploy, the theft and publication of the source codes may have been socially motivated. This notion is supported by the fact that the initial threat to release the information occurred around the same time as Gross filed his lawsuit against Symantec. At the very least though, Yama Tough’s encounter with Symantec was embarrassing for the security company, and highlighted some critical vulnerabilities in the company’s security infrastructure.

19 A copy of the email exchange can be found at http://pastebin.com/GJEKfLT9
Nigerian and Peruvian governments

The national governments of Nigeria and Peru found themselves targeted by TeamPoison in February 2012. On three different occasions members of the group released thousands of sensitive materials online that they had acquired from servers used by both governments (Vigo, 2012, para. 3). Information that was released included internal documents, administrator passwords, and emails (Kovacs, 2012, para. 2, 5). Additionally, TeamPoison encouraged Nigerians to “raise up and confront [their] oppressors” (TeamPoison, as cited in Kovacs, 2012, para. 6). It is understood that the Nigerian and Peruvian governments were targeted because TeamPoison viewed them both to be corrupt (Kovacs, 2012, para. 1). However, it is not clear what, if anything, actually triggered the attacks.

6.5.4 Elections

During elections the former actions and current policies of political parties become popular topics of discussion amongst the public and the media. While this may provide politicians with the opportunity to highlight the good that they have done, the increased attention may also make electoral candidates more susceptible to criticism and embarrassment. According to Dayal (2012), it is expected that politically motivated cyber attacks will increase during an election year (para. 1). While there have been cases of hacktivists using elections as opportunities to commit politically motivated cyber attacks, instances of such attacks seem to be relatively few. When they do occur, the general motivation seems to be to disrupt the system and voice condemnation, rather than to influence election results. Further, the attacks that have been launched have been targeted at political parties, not the bureaucratic side of government.

US presidential election, 2004

As the US Federal election in 2004 was ensuing, a group known as Black Hat Hackers Bloc announced plans to launch DDoS attacks against the websites for President George W. Bush and the Republican Party, also known as the Grand Old Party (GOP) (Shachtman, 2004, para. 4). The intent of the attack was to shut down the prominent Republican Party websites, thus preventing any users from accessing or promoting the GOP’s message (Shachtman, 2004, para. 5). By carrying out this attack, and very clearly voicing their condemnation of the GOP, the Black Hat Hackers Bloc would have caused a great deal of disruption to the Republican Party.

Following the group’s announcement to launch the DDoS campaign a number of other activist groups condemned the planned attacks. These groups remarked that shutting down the GOP websites would violate the political party’s freedom of speech; a principle highly valued by protestors and activists such as themselves (Shachtman, 2004, para. 6). In response to this criticism, the Black Hat Hackers Bloc called off the planned attacks. Even though the Black Hat Hackers Bloc did not carry out their planned DDoS campaign against the US Republican Party, the threat to do so demonstrates how elections have been considered ideal opportunities to launch politically motivated cyber attacks.
**US presidential election, 2012**

In 2011 a member of Anonymous posted a video online that outlined plans to disrupt the 2012 US presidential election. Both the Democratic and Republican parties were listed as targets in the campaign, both parties having been deemed “[un]worthy of representing the voice of the Americans whom they have disenfranchised” (“Anonymous target 2012 presidential election,” 2011, para. 3). According to the video, the first attack was scheduled to occur during the Republican Iowa Caucus in January 2012 (“Anonymous target 2012 presidential election,” 2011, para. 1).

While the threat of cyber attacks being launched against the US Democratic and Republican Parties as they prepare for the 2012 US presidential election does still exist, at the time of writing, there have been no cyber attacks launched against either the Republican or Democratic parties. The Iowa caucus, which took place months ago, occurred without incident, and there have been no reported issues with any of the other caucuses since then. It remains unclear as to why the Anonymous collective had decided not to follow through with the promised attacks. Notwithstanding, there are still several months until the 2012 US presidential election during which cyber attacks could still be committed.

**Canadian NDP leadership election, 2012**

In March 2012 the Canadian National Democratic Party (NDP) held an election to determine the Party’s new leader. Voting was done online, and was limited to registered NDP members. A private company called Scytl Canada was contracted to manage the vote. As voting commenced however, the online balloting system was noticeably slow. While the reasons for this were not immediately clear, Scytl Canada later announced that someone had initiated a DDoS attack in an attempt to overload the NDP online balloting system (“Cyber attack on NDP leadership vote”, 2012, para. 2). More than 10,000 botnet computers were involved in the attack (“Cyber attack on NDP leadership vote”, 2012, para. 1). Although the DDoS attack failed to shut down the online balloting system, the attack did delay the voting process by six hours (“Cyber attack on NDP leadership vote”, 2012, para. 9).

Because the DDoS attack was not preannounced, and no individual or group has yet claimed responsibility for the attack, it is elusive as to what the overall intent of the attack was. While the attack certainly appears to have been politically motivated, it is unclear whether or not the attack was intended to make a political statement, demonstrate disdain for the NDP, or was simply motivated by malice. Accordingly, due to this uncertainty, the recent DDoS attack against the NDP may only loosely qualify as an example of hacktivism.

6.5.5 Law enforcement

Although governments and private organizations are typically the targets of hacktivists, law enforcement agencies have also been targeted by groups such as LulzSec and the Anonymous collective. There have also been instances where third party organizations have been targeted as a result of the actions of police officers. The specific motivations for targeting law enforcement or third party groups may vary, but seemingly tend to be stimulated by the opinion that police
officers have acted inappropriately. The use of excessive force and unjust practices are examples of conduct that may be deemed inappropriate.

**Operation Chinga La Migra**

In June 2011 LulzSec released a large cache of information that had been attained from the Arizona Department of Public Safety. Information contained in the release included names, passwords, online dating account information, voicemails, and social security numbers of Arizona police officers (Panda Labs, 2011, p. 5; Albanesius, 2011c, para. 2). The decision to target Arizona police officers was in response to The Support Our Law Enforcement and Safe Neighbourhoods Act, known as SB 1070, which had been passed by the Arizona Senate (Albanesius, 2011c, para. 5). This Act reinforced on-going efforts to manage illegal immigration in the State of Arizona. For example, SB 1070 requires that Arizona police officials determine an individuals’ immigration status if there are reasonable grounds to believe that the individual is an illegal alien. Opponents of the Bill voiced concerns that the legislation could lead to racial profiling and civil rights abuses (“Thousands protest Ariz. immigration law, 2010, para. 2).

The attack against Arizona police by LulzSec was dubbed Operation Chinga La Migra, a Spanish phrase which in English means “fuck the border patrol”. Although it was the government of Arizona that was in fact responsible for the legislation, it does not appear that any attacks were aimed at those parties involved. Instead, LulzSec only targeted Arizona police officers. Given the role that Arizona police have in enforcing the legislation though, it is likely that LulzSec simply considered Arizona police officers to be complicit with the Bill’s perceived anti-immigrant policies.

**Occupy Boston and Occupy Oakland**

Beginning in September 2011 protestors began organizing demonstrations and constructing tent cities in New York’s Wall Street financial district. While the issues raised during the demonstrations varied, financial inequality in society and corruption amongst corporations were perhaps the most prominent topics of discussion. This movement came to be known as Occupy Wall Street. As the movement grew, similar demonstrations and tent cities began arising in other cities throughout North America. Each of these demonstrations adopted the Occupy moniker. After several months of protests, governments began to take measures to remove the demonstrators and dismantle the tent cities. In some cases this lead to confrontations between demonstrators and the police.

In October 2011 the website for the Boston Police Department was hacked into by participants of Operation AntiSec. Data that was stolen and released included the names, addresses, passwords, and phone numbers for Boston police officers (Liebowitz, 2011, para. 3). It is understood that the attacks were committed as retribution for alleged police brutality against protestors at Occupy Boston (“Anonymous hacks police websites,” 2012, para. 8). Four months later, the Boston Police Department was again targeted by individuals associated with the Anonymous collective. This time the Boston Police website was defaced, and Anonymous issued a message criticizing the Boston Police department’s management of protestors during the eviction of Occupy Boston.
Only a few days after the second hacktivist attack against the Boston Police Department, leading officials in the City of Oakland were targeted by Anonymous. The Police Chief, the Mayor, and several other members of the Oakland City Council had personal information, such as home addresses and telephone numbers, published online (“Anonymous hacks Oakland officials,” 2012, para. 6). This attack was in response to the acts of police brutality that were allegedly committed against protestors during Occupy Oakland, and the condemnation of the Occupy movement by the city’s leading officials (“Anonymous hacks Oakland officials,” 2012, para. 1). Although this attack did not strictly target Oakland police officers, the attack certainly appears to have been motivated by the alleged unjust actions of police during Occupy Oakland.

### 6.5.6 Retaliation for arrests

Over the last few years there have also been several occasions where cyber attacks have been launched in retaliation for the arrests of individuals who are alleged to have participated in hacktivism. Although such attacks may not draw public attention to a broad social or political issue, they do serve as a means of protesting the actions of law enforcement groups; specifically, the arrest of alleged hacktivists. By temporarily shutting down an organization’s website, or publishing stolen information online, individuals who take part in such attacks are able to voice their displeasure of alleged hacktivists being arrested. In addition to embarrassing and discrediting the targeted organization, such attacks may also serve as a warning to law enforcement agencies that they too may be targeted should they be involved in any similar arrests.

---

20 Image retrieved from http://www.huffingtonpost.com/2012/02/03/anonymous-boston-police-occupy-wall-street_n_1252718.html
Spanish national police force

After several members of the Anonymous collective were arrested in Spain in June 2011, Anonymous threatened action against Spanish authorities (Wilson, 2011, para. 6). Three days after issuing the threat, the website for the Spanish national police force was briefly shut down as a result of a DDoS attack (“Spanish police website hit,” 2011, para. 2). No data was compromised as a result of the attack, and the attack was perhaps more embarrassing for Spanish authorities than costly. Although this attack only had temporary implications, it did clearly demonstrate the willingness of Anonymous members to retaliate against law enforcement agencies.

Shooting Sheriffs Saturday

In August 2011, shortly after AntiSec was formed, information relating to dozens of American law enforcement agencies was published online as revenge for several recent arrests of Anonymous members (Mills, 2011, para. 1). This massive unauthorized data released was called “Shooting Sheriffs Saturday”. Information that was released included private emails, account passwords, police officers’ social security numbers, and credit card information. In addition to publishing all of this information online, those involved in the attack also used the credit card details to make donations to such groups as the American Civil Liberties Union and the Electronic Frontier Foundation (Mills, 2011, para. 12). The total cost associated with this data breach remains unclear.

Symantec

One month after Yama Tough released portions of source code for a number of Symantec software programs, in March 2012 AntiSec released the complete source code for Norton Antivirus 2006. It is understood that the source code was released in response to the arrests of a number of individuals who were allegedly involved with LulzSec (Fisher, 2012, para. 1). A message posted in the data release demanded for the liberation of the individuals who had been arrested. Symantec has confirmed the authenticity of the source code that was released, but has maintained that the source code is outdated, and that the release poses no risk to Symantec’s customers (Fisher, 2012, para. 2). Again though, there is the potential risk that the information gleaned from the 2006 source code could reveal vulnerabilities that are still present in the current version of Norton Antivirus.

6.5.7 General contempt

While many hacktivist attacks seem to be triggered by a particular incident, there have also been several cases where cyber attacks appear to have been launched for no reason other than to derive humour, embarrass the target, and highlight an organization’s inadequate security capabilities (Carabott, 2011, para. 6; Sengupta, 2011, para. 17; LulzSec, as cited in Dickinson, A., 2011, para. 12). These types of attacks do not generally seem to have a clear social or political message. Rather, they seem to be committed for the purpose of demonstrating general contempt for the targeted organization, but are not necessarily malicious. Such attacks may in fact have serious political or social implications though. For example, many of the attacks that
have been committed by groups such as the Anonymous collective and LulzSec have increased awareness of the systemic issues with many organizations’ information security systems (Bradley, 2011, para. 11). Because of this equivocation, such attacks may best be understood as being a grey area within hacktivism.

**Pakistani National Response Center for Cyber Crimes**

In 2010 the Pakistani National Response Center for Cyber Crimes (NR3C), a branch of the country’s Federal Investigation Authority, was successfully hacked into by a member of a group called PAKbugs (“Pakistani National Response Center for Cyber Crimes website defaced,” 2010, para. 3). The individual involved in the attack defaced the NR3C website, and claimed to have gained access to the Center’s entire email database and its backup files (Ferguson, R., 2010, para. 5). These claims were supported by screenshots the hacker posted online that showed him logged into the NR3C email server (“Pakistani National Response Center for Cyber Crimes website defaced,” 2010, para. 5). As Ferguson (2010) states, a breach of this magnitude in a country as politically tumultuous as Pakistan was particularly serious (para. 5).

According to the individual who breached the NR3C website, he or she had discovered a number of glaring security vulnerabilities during a routine penetration test of the website (Ferguson, R., 2010, para. 3). Recognizing this, it seems that the attack against the NR3C was an act of opportunity, rather than a calculated attack. Given that the attacker only advertised that he or she had breached the website, rather than causing any grave damage, the attack also does not seem to have been malicious. By advertising the ease by which the attack was perpetrated, the attacker managed to not only embarrass the NR3C but also publicized the need for improved security measures.

**Stratfor**

Strategic Forecasting Inc., more commonly known as Stratfor, is an American consulting firm. Clients of Stratfor include Sony, Google, Boeing, and the US military. In December 2011, Stratfor was hacked into by members of Operation AntiSec. The group defaced the Stratfor website, and stole thousands21 of private email addresses, user passwords, phone numbers, and credit card numbers (Liebowitz, 2012, para. 3). The data was then posted online. Although Stratfor had been using encrypted software to handle customer information, the firm had stored its customers’ data in cleartext (Norton, 2011c, para. 7). When Stratfor’s security measures were breached, AntiSec had open access to all of Stratfor’s customer data.

According to those who participated in the attacks, “Stratfor was targeted because of its client list... [and] because it was terribly insecure” (Norton, 2011c, para. 10). Given Stratfor’s reputation as a secure and reliable company, coupled with its impressive lists of clients, a breach of this magnitude was particularly costly and embarrassing (Norton, 2011c, para. 2). Although AntiSec did not use the stolen credit card information for their own benefit, they did make a number of donations to organizations, such as Red Cross and Save the Children. In total approximately $700,000 worth of unauthorized charges were made using the stolen credit cards.

---

21 According to Liebowitz, AntiSec stole: 859,311 email addresses; 860,160 passwords; 68,063 credit card numbers; and 50,569 phone numbers in total.
Hacktivism and the Government of British Columbia  52

(Kerr, 2012, para. 2). Stratfor estimates that the data breach cost the company an additional $2 million in lost business and other costs associated with mitigating the damage of the data breach (Kerr, 2012, para. 7).

The Stratfor data breach provides an example of how hacktivists may target organizations without provocation. Poor security practices may be exploited simply for the purpose of publicizing an organization’s security inadequacies. This example also shows how organizations may become the target of hacktivists because of their high stature or because of the third-party organizations with whom they associate or do business.

A3P

Members of Anonymous attacked the official website for the American Third Position Party (A3P), a white supremacist group, in February 2012. In the attack the A3P website was defaced, and the names and contact information for the site’s members were published online. This attack was part of an on-going campaign against white supremacist groups known as Operation Blitzkrieg (Pieklo, 2012, para. 5). Although not explicitly stated, it can be understood that the attack was committed to embarrass members of the A3P organization and condemn white supremacist attitudes. The willingness of Anonymous members to expose, and thus attempt to deter, white supremacist groups may seem somewhat hypocritical given the group’s position on freedom of speech. Yet, such attacks suggest that the Anonymous collective believes that “the Internet freedom[s] they are fighting to protect must not be abused” (“4 signs ‘hacktivism’ has gone mainstream,” 2012, para. 5).

Figure 8. Screenshot of the defaced A3P website

One of the more interesting outcomes of the attack against A3P is that it provided evidence of a relationship between the white supremacist group and US Representative Ron Paul, who was campaigning for the Republican presidential nomination at the time of the attack. Internal A3P

communications published by Anonymous suggested that Paul had met with the group’s leaders regularly, and had received campaign funding from A3P and other white supremacist groups (Mezzofiore, 2012, para. 3, 4). Following this data breach, both Paul and A3P denied any connection between the two (Peterson, 2012, para. 7, 8). Regardless of whether or not there was in fact a connection between Paul and A3P, the matter received little attention from the media, and there was no apparent harm done to Paul’s campaigning efforts as a result of the attack.

This chapter has provided a review of what has been said about whether or not hacktivism is increasing and what has been said about governments becoming the targets of hacktivists. Also discussed were some of the factors which may trigger hacktivism and the implications associated with a successful hacktivist attack. The last half of this chapter looked at current trends within hacktivism, and provided numerous examples of organizations that have been targeted for an array of reasons. The next chapter will look at current social and political points of contention within BC, and discuss the likelihood that the BC government may be an attractive target for hacktivists. The seven themes discussed in this chapter will be used as a framework for analyzing the issues in BC which could potentially trigger hacktivist attacks against the BC government.
Chapter 7: Hacktivism and the Government of British Columbia

7.1 Introduction

The discussion thus far has offered a look at a number of the issues that hacktivists have engaged in, as well as what has been said about governments in general being a preferable target for hacktivists. Building upon this analysis, this chapter will discuss the extent to which the Government of BC may be an attractive target for hacktivists. By comparing current trends within hacktivism with some of the more prominent social and political issues in BC, this discussion is intended to provide a qualitative assessment of the risk that points of contention in BC may trigger hacktivist attacks against the BC government. Because it may not always be apparent what issues may in fact stimulate hacktivists into action though, the examples drawn upon in this chapter may not provide a complete account of every issue that could motivate hacktivists to target the Province. This chapter is organized by the seven trends within hacktivism that were discussed in the previous chapter.

7.2 Issues that may trigger hacktivist attacks

7.2.1 Privacy

Section 30.1 of FOIPPA requires that the Government of BC stores all information under its control within Canada, except for a limited number of exceptions. This allows the Province to manage and protect the information of British Columbians and prevents foreign governments from acquiring this data. Having this requirement in place may serve to bolster the perception that the Province is exercising proper data management and is being proactive in its efforts to protect the privacy of British Columbians. While the Fine Gael party in Ireland may have been targeted because it did not demonstrate similar standards, the on-going efforts of the BC government to protect the privacy of its citizens will likely limit the possibility that the Province will be targeted for perceived improper data management practices.

There are also currently no efforts underway by the BC government to allow for the monitoring of people’s activities online, nor has any interest to do so been expressed. The most recent attempt to promote online surveillance in Canada was Bill C-30. Because Bill C-30 has gone back before committee for review, it is currently unclear what the proposed legislation will look like when, or if, it is reintroduced. At this time, it seems highly unlikely that even if Bill C-30 is reintroduced that hacktivist attacks might be instigated against the BC government. Although Bill C-30 certainly attracted the ire of Anonymous members and the Canadian public when it was first introduced, this was a matter related to the federal government rather than the Government of BC.

At no point during the dispute over Bill C-30 did the BC government voice its support for the proposed federal legislation. Not surprisingly then, the Province did not attract criticism from the public or hacktivists in regards to Bill C-30. Even when the Canadian Association of Chiefs of Police, the Canadian Police Association, and the Vancouver Police Department did publicly voice their support for Bill C-30 (“Online surveillance bill backed by police chiefs,” 2012, para. 2, 4), there was no response issued from hacktivists. At no time were any threats issued or cyber
attacks launched against BC police organizations in regards to Bill C-30. Accordingly, there is nothing to suggest that hacktivists have any intention of targeting the Province in response to Bill C-30.

Taking into account that the Province has not made any recent efforts to hinder the privacy of British Columbians, and has been proactive in its efforts to protect people’s private information, it seems unlikely that the BC government would be targeted by hacktivists for anything it is currently doing in regards to privacy. There do not appear to be any policies or on-going activities that could trigger a hacktivist attack. Nevertheless, in the event that the Province was to reverse its policies on privacy, or was perceived to have infringed upon the privacy of British Columbians, it is very possible that the Province could become the target of hacktivists.

7.2.2 Censorship

Enbridge Northern Gateway Project

One of the more pronounced and contentious issues in BC at this time is the proposed Enbridge Northern Gateway Project. This proposed project aims to construct a pipeline running from near Edmonton, Alberta, across BC, to the coastal city of Kitimat. A growing number of groups have voiced their opposition to the pipeline because of environmental concerns, including a number of First Nations and environmental groups, BC municipalities, and the federal NDP and Green parties (Yaffe, 2012, para. 3). While the environmental impact of the pipeline is certainly of concern for many, there is no evidence to suggest that hacktivists have become involved, or intend to become involved, in any environmental issues. This observation echoes the sentiment that hacktivists are more concerned with issues that relate to the Internet and activities which limit rights and freedoms within society.

Even though it appears unlikely that hacktivists will react to the environmental risks associated with the Enbridge Northern Gateway Project, it is conceivable that hacktivists might respond to limitations that have been imposed on public debate of the pipeline, which could be seen as a form of censorship. For example, a scheduled public hearing about the pipeline in Bella Bella, BC, was cancelled after panel members were confronted by protestors (“Gateway hearing cancelled,” 2012, para. 1). The federal government has also shortened the regulatory review process for the pipeline, and suggested imposing limitations on the types of people and groups that are permitted to present at future reviews (“Gateway hearing cancelled,” 2012, para. 17; Paris, 2012, para. 12). Such limitations may be viewed by some as infringing upon people’s freedom of expression and contrary to the principles of a democratic society.

The proposed Enbridge Northern Gateway Project falls under federal jurisdiction, despite the fact that the pipeline will traverse BC if it is built. Because of this disassociation between the Province and the pipeline, it would seem much more probable that hacktivists would target the federal government, rather than the BC provincial government, in response to issues surrounding the project. This view is supported by the fact that the BC government has thus far avoided taking a position either in favour or against the project (Hunter, 2012, para. 11). Yet despite this separation, the BC government has also publicly commended the federal government’s decision to emplace limitations on the review process (Hunter, 2012, para. 10). As such, it is possible that
the Government of BC may be seen as complicit in the federal government’s actions. This could in turn prompt hacktivists to consider targeting the Province. Notwithstanding, there is nothing to suggest that hacktivists intend to target either the Province or the federal government in response to concerns of censorship regarding the proposed Northern Gateway Pipeline. No threats have been issued by hacktivists, and no statements have been made, in regards to the proposed pipeline.

**Bill-22**

After several months of unsuccessful contract re-negotiations between the Government of BC and the province’s teachers, teachers in BC participated in a three-day walkout in March 2012 (“B.C. teachers strike starts today,” 2012, para. 2). In response to the walkout, the BC government passed Bill-22. As part of Bill-22 teachers were required to return to work and it was legislated that there would be a six month respite to contract negotiations (Bell & Shaw, 2012, para. 3). Because this mandate effectively nullified the ability of teachers in BC to strike, some may see the BC government as infringing upon people’s right to freedom of speech and freedom of expression.

Despite this possibility, it does not appear that concerns surrounding Bill-22 or the status of the Province’s contract renegotiations with teachers are a topic of interest for hacktivists. Public debate currently seems to be focused on teachers’ withdrawal of participation in extracurricular activities and the effect this will have on students (Spencer, 2012, para. 2; “B.C. teachers begin withdrawal,” 2012, para. 1). Further, no threats have been issued by hacktivists condemning or threatening action against the BC government. Accordingly, it does not appear likely that hacktivists intend to become involved in protesting or drawing attention to issues related to either Bill-22 or the on-going contract dispute between the Province and BC’s teachers.

**7.2.3 Corruption**

The BC government’s efforts towards transparency, including the Open Information and DataBC websites, may serve to diminish notions that the BC government is a corrupt body. As stated in Chapter One, the proactive release of government information to the public provides the Province the opportunity to demonstrate that it does not have any hidden agendas and promotes the idea of accountability. Yet despite such efforts, statements made by groups like Anonymous and TeamPoison suggest that many hacktivists perceive all governments to be intrinsically corrupt. As a consequence, participants in hacktivism may deem the BC government to be corrupt despite its efforts to suggest otherwise.

Specific incidences may also contribute to the notion that the BC government is corrupt. In June 2011 TELUS was awarded a 10 year contract with the Province that is worth one billion dollars. A Times Colonist news story that was printed in March 2012 alleged that TELUS’s procurement of the deal was unfair and potentially illegal (Shaw, 2012, para. 1). Drawing upon FOI requests that are available through the Province’s Open Information website, the author highlighted the fact that the other telecommunications companies who had unsuccessfully bid on the contract had voiced opposition to the deal between TELUS and the Province, and had considered legal recourse (Shaw, 2012, para. 3). It is of value to note that the documents referred to in the article
only show one side of the dispute, and that they may not accurately reflect how the complainants currently feel. Nevertheless, this article suggested that the Province may have acted unfairly.

A Times Colonist news story printed two weeks later publicized the fact that all of the telecommunications companies involved in bidding for the contract had donated money to the BC Liberal party. The journalist who authored the article also made note of the fact that TELUS, which was awarded contract, was also the telecommunications company that had donated the most amount of money to the BC Liberal party (Lloyd, 2012, para. 1). By insinuating that there was a connection between TELUS being awarded the contract and the amount of financial support it had provided to the BC Liberal party, the article further advanced the perception that the BC government acted in an unethical, and thus corrupt, manner when managing the telecommunications contract with TELUS.

Regardless of whether or not there were in fact legitimate issues with the Province’s contract with TELUS, the articles printed in the Times Colonist promote the notion that there is corruption within the BC government. Because hacktivists attacks are fuelled by the perception that there have been wrongdoings on the part of an organization, it is possible that these articles could have stimulated hacktivists into launching cyber attacks against the Government of BC. Interestingly, there was no widespread public criticism in response to the articles, nor did any self-identified hacktivist issue threats against the BC government. As such, it does not seem that concerns regarding how the Province managed its telecommunications contract with TELUS will trigger hacktivist attacks.

Although there does not appear to have been any risk of hacktivists attacks occurring in response to the Province’s contract with TELUS, the articles printed in the Times Colonist do highlight the potential risk associated with the Province’s efforts to promote open government and transparency. Document releases may be misleading, or they may not offer a complete depiction of an issue. This may lead to misunderstandings amongst the public and media about how the Province operates, which may foster notions that the BC government is corrupt. If the public is increasingly disposed to believe that the BC government is corrupt, it could very well increase the chances of hacktivists launching cyber attacks against the Province.

7.2.4 Elections

The upcoming BC provincial election, although not scheduled until May 2013, is increasingly being discussed amongst media outlets. Already attention is being paid to how the different political parties are faring in the polls. One poll, conducted in early April 2012, found that BC’s three more prominent political parties each have relatively equal levels of support amongst the public (“Poll puts B.C. Conservatives in 2nd place with Liberals,” 2012, para. 1). While it is too early to project how each party will fare in one year’s time, this poll suggests that it may be a very close, and thus quarrelsome, election.

Given the uncertainty surrounding the 2013 election, each political party may be particularly susceptible to public scrutiny and criticism. It is possible that hacktivists may use the upcoming provincial election as an opportunity to launch hacktivist attacks. Successful cyber attacks may

23 The BC Liberals, the BC NDP, and the BC Conservatives.
serve as a means to either embarrass or criticize BC’s political parties and candidates, or both. In
the event of a data breach that entailed the release of sensitive or damaging documents, public
confidence in a particular candidate or party could be swayed. As such, it is possible that a
successful hacktivist attack could in fact impact how people vote, and thus effect the outcome of
the election. While this is certainly a possibility, to date no statements have been made by
hacktivists condemning BC’s politicians, and no threats to launch cyber attacks have been
issued.

At this time the BC electoral system does not allow for electronic voting, known as e-voting.
Consequently, it is not possible that an attack could be launched in an attempt to disrupt the
actual election process, as happened with the recent federal NDP’s leadership election.
Nonetheless, it is possible that hacktivists could launch an attack against the BC Elections
website. An attack on the site could be used protest the electoral system in BC, criticize the
province’s political parties, or be orchestrated in an attempt to gain unauthorized access to the
information of registered voters in BC. Such an attack could affect how the public regards the
BC electoral system, or damage the public’s confidence in how the Province manages online
security and protects the personal information of British Columbians. Yet despite this risk, again,
there have been no statements made to suggest that hacktivists intend to carry out any such cyber
attacks.

While it may simply be too far in advance of the upcoming provincial election for individuals
inclined to participate in hacktivism to consider targeting groups associated with the BC
provincial election, there is nothing to suggest that there is any intention to use the election as an
opportunity to launch cyber attacks. The fact that there are relatively few cases of hacktivist
attacks targeting elections further supports the notion that it is unlikely that hacktivists will
involve themselves in the 2013 BC provincial election. Nonetheless, the risk of such attacks
occurring does still exist.

7.2.5 Law enforcement

Several of the hacktivist attacks discussed in Chapter Six occurred in response to perceived
instances of police brutality, excessive force, or improper actions on the part of police officers.
Despite this common trigger, it remains unclear why hacktivists have opted to target some police
organizations for their actions but not others. While there are recent examples of accusations of
excessive force and improper conduct on the part of police officers in BC, neither the BC
government nor BC police organizations appear to have ever been targeted by hacktivists for the
perceived wrong-doings of BC police officers.

The 2007 taser-related death of Robert Dziekanski, a Polish immigrant, at the hands of Royal
Canadian Mounted Police (RCMP) officers at Vancouver International Airport could easily have
been used by hacktivists as a reason to launch attacks against the RCMP. The actions of the
officers involved attracted the attention of media across the world, and fuelled discussion
regarding excessive and improper conduct by police. The decision by RCMP officials to not
correct misinformation in the media, and accusations of misconduct and perjury on the part of
officers involved in the death of Dziekanski (Hall, 2012, para. 13; (Chau, 2009, para. 39, 52)
could also have fuelled resentment towards the officers involved. This in turn could have sparked
hacktivist attacks against the RCMP. Because the incident occurred in BC, it is possible that the BC government could also have been viewed as accountable in the death of Dziekanski. Yet despite this risk, no threat was ever issued from any self-identified hacktivists against the officers involved in Dziekanski’s death, the RCMP, or the Government of BC.

A video of a Victoria police officers kicking and kneeling a group of individuals during an arrest outside of a Victoria club was posted on YouTube in 2010. To date, this video has been viewed over 57,000 times. Despite an internal investigation of the incident, and accusations of brutality and excessive force on the part of officers shown in the video (“Officer in YouTube video faces new police probe,” 2010, para. 1, 11), the incident never attracted the attention of hacktivists. Even after the officers involved in the incident had the charges dropped, there were no responses from any self-identified hacktivists threatening retaliation.

In light of current trends, it does not appear that there are any on-going issues regarding BC police officers that will trigger hacktivist attacks against BC police organizations or the BC government. The lack of attention awarded by hacktivists towards law enforcement concerns in BC suggests that hacktivists simply do not consider BC an attractive or deserving target. This is not to suggest that the actions of BC law enforcement officers are immune to hacktivist attacks. It is possible that an incident in the future could attract the attention of individuals willing to participate in hacktivism. The likelihood of such an incident occurring, and the extent to which the Government of BC may find itself a target, however is uncertain.

7.2.6 Retaliation for arrests

To date there have been no cases of anyone being arrested in BC for their alleged involvement in a hacktivist attack. Recognizing this then, there is nothing at this time to suggest that the BC government may be targeted as retaliation for the arrest of alleged hacktivists. In the event that police in BC were to arrest someone for their alleged involvement in a hacktivist attack though, in light of current trends, the arrest could very well trigger retaliatory cyber attacks. While it is possible that such attacks may be aimed at the Province, the extent to which this is a likely scenario remains unclear.

7.2.7 General contempt

Because participants in hacktivism have expressed an interest in targeting government organizations in general, based on the assumption that all governments are intrinsically bad, it is possible that hacktivists may target the Government of BC simply because of its status in society. Attacks may be conducted in an effort to find evidence of wrong-doing on the part of the BC government, to demonstrate disdain for and embarrass the Province, or to derive humour. Cyber attacks of this nature may be particularly disparaging because they may not be provoked by a particular incident, which may diminish the ability of the Province to anticipate hacktivist threats.

Although attacks motivated by general contempt may not be clearly socially or politically motivated, they may draw attention to legitimate issues and concerns. For example, dissatisfaction with decisions made by the BC government may provoke individuals to launch
Two recent government directives that have been met with formidable opposition by many in BC include the Harmonized Sales Tax (HST) and BC Hydro smart meters (Wintonyk, 2011, para. 12; Smyth, 2012, para. 11). This is not to suggest that public opposition equates to a strong likelihood of hacktivist attacks though. Nonetheless, it is possible that these points of contention, and others, could inspire hacktivists to target the BC government.

Recognizing that people may be opposed to the BC government for any number of reasons, it is extremely difficult to ascertain the likelihood that the Province could be targeted by hacktivists for reasons of general contempt. While the potential for such attacks against the BC government does exist, there is nothing at this time to suggest that hacktivist do intend to target the BC government. Nevertheless, this uncertainty illustrates the value of ensuring that the BC government has a developed and current security infrastructure in place, and is prepared to guard against cyber attacks.

7.3 Analysis

While there are certainly on-going points of contention in BC that could stimulate hacktivists into action, there is nothing at this time to suggest that there are any impending hacktivist threats to the BC government. To date, no self-identified hacktivists or groups have issued threats to, or criticisms of, the Province. There have also been no reports of any cyber attacks having been perpetrated against the Government of BC. The reasons for this lack of attention remain unclear however. Perhaps the BC government is not seen as being an attractive or deserving target. Another possibility is that the social and political issues in BC are simply not contentious or interesting enough to warrant the attention of hacktivists.

Accordingly, at the time of writing it seems unlikely that hacktivists consider the BC government to be an attractive target. Despite this observation, it is still possible that hacktivists could involve themselves in the social and political issues of BC. Efforts to promote online surveillance or instances of government corruption, whether legitimate or perceived, could easily galvanize hacktivists into targeting the BC government. Also, as the Enbridge Northern Gateway Project continues to gain international attention, it is possible that hacktivists may attempt to address the restrictions that have been emplaced upon the review process. It is even possible that hacktivists may attempt to protest or draw attention to the environmental concerns surrounding the pipeline; although there is nothing at this time to suggest that there is any interest in doing so. By continuing to afford consideration to the social and political issues in BC that may attract the attention of hacktivists, it is expected that the BC government will be better prepared to anticipate and mitigate the likelihood of successful hacktivist attacks against the Province in the future.

This chapter has provided a review of a number of the more prominent points of contention in BC, and has discussed the likelihood that the BC government may be considered by hacktivists to be an attractive target. Chapter Eight will look at some of the best security practices for guarding against cyber attacks.
Chapter 8: Best Security Practices

8.1 Introduction

The Government of BC has an interest in protecting itself from cyber attacks. By establishing effective security safeguards and practices, the Province will be better situated to protect information under its custody, offset public embarrassment, and maintain its reputation as a reliable and secure organization. Even though hacktivism may pose a legitimate risk to the Province, it is unlikely that an attacker’s motivations will be the immediate concern following an attack. Rather, the immediate concern will be with how the attack was perpetrated, what data was compromised, and what may be the short- and long-term implications of the attack (Mansfield-Devine, 2011b, p. 7). Recognizing this, it is essential that the Province takes measures to protect itself against all cyber attacks. In order to guard against potential cyber threats there is a need for the BC government to be proactive in employing comprehensive and consistent measures to uphold information security across government.

Passive security practices and a lack of security standards today has weakened the security of many organizations (Florêncio & Herley, as cited in Watson, 2010a, para. 4). This in turn has increased the susceptibility of many organizations to cyber attacks. In addition to posing a risk to the organizations themselves, this disregard also poses a risk to those individuals who have entrusted an organization with their information. Some have even gone so far as to assert that organizations that implement insufficient security measures are guilty of gross negligence (Panda Labs, 2011, p. 3).

Befitting security practices improve the ability of the Province to obstruct cyber attacks and provide greater protection to the information and resources under its management. Effective security practices also allow the Province to demonstrate that it has exercised due diligence in maintaining security. The ability to demonstrate that due diligence has been exercised will reinforce the BC government’s reputation for security, and provide British Columbians with greater confidence that their information is secure. In the event of a successful cyber attack, the Province will also be more able to manage criticism from the public and the media (Anderson, 2008, p. 11) if it is able to demonstrate that proper security mechanisms were in place and that security was maintained to the best of its ability.

In terms of providing better protection to an organization’s IM/IT infrastructure, there are several best practices that organizations can adopt. This chapter will provide a look at some of the best practices for guarding against cyber attacks. The examples drawn upon were selected because of their connection to the tactics used by hacktivists. This chapter does not provide an assessment of the Province’s current security capabilities, nor does it provide an overview of every security practice an organization may implement in an effort to protect its IM/IT infrastructure. The BC government has already implemented a number of the security practices discussed in this chapter.
8.2 Best security practices

8.2.1 Invest the time and resources

According to Peter Wood, the CEO of the security firm First Base Technologies and a member of the Information Security Audit and Control Association (ISACA) advisory group, a large number of organizations today are reluctant to examine their systems for vulnerabilities because of the belief that such inspections are time intensive, and may consequently hinder organizational productivity (as cited in Mansfield-Devine, 2011b, p. 12). Akin to this sentiment, security shortcomings can also be attributed to fiscal limitations and the lack of consideration given to security on the part of organizations (Temple, 2011, para. 10; Bradley, 2011a, para. 3). While there may be merit to the opinion that proactive efforts to maintain security can be somewhat exacting, this argument does not take away from the fact that improper security practices put organizations at greater risk of cyber attacks and security breaches; the potential implications of which were discussed in Chapter Six.

Firewalls and anti-virus programs are two fundamental mechanisms by which organizations can protect their networks and computer systems from cyber attacks (Milone, 2003, p. 78). Because vulnerabilities can still exist within an organization’s IM/IT security infrastructure though, there is a need for servers to be regularly audited, firewalls kept up to date, and security vulnerabilities patched when they are identified (Ferguson, R., 2010, para. 6; “With new tactics,” 2011, para. 9). Vulnerabilities may include SQL and XSS coding weaknesses (Trend Micro, 2010, p. 3) or defects in a server’s security system. Related to the need for penetration tests, security threat assessments provide a useful means for identifying where security-related issues exist, and whether the risks are acceptable.

As Wood has asserted, many organizations have neglected to update and patch their servers as regularly as they should (as cited in Mansfield-Devine, 2011b, p. 11). This has left many organizations exposed to a number of security vulnerabilities that could easily be exploited. The breach of the Pakistani Cyber Crime Center provides a glaring example of what can happen when a network’s vulnerabilities are not regularly audited and patched. As the computer security company McAfee (2010) has advised, organizations should regularly conduct penetration tests of their systems and look for vulnerabilities that may exist (p. 30). By replicating the methods by which hacktivists and other cyber attackers are often able to identify weaknesses in an organization’s system, an organization will be better able to rectify vulnerabilities and guard against successful cyber attacks (McAfee, 2012, p. 30).

It can be expected that an organization will be much more prepared to counter the efforts of hacktivists and types of cyber attackers by investing the time and resources needed to ensure that an organization’s security systems are protected, and by recognizing the guidance and support an organization’s security group is able to provide (Woods, as cited in Mansfield-Devine, 2011b, p. 12). Proactive efforts towards security can improve an organization’s reputation for keeping information and data secure, and better serves the individuals who have entrusted an organization with their private information.
8.2.2 Protect sensitive and private data

The risks associated with unauthorized data releases highlight the need for organizations to ensure that sensitive and private materials are protected. It has been suggested that “data storage systems should be the best protected resources in any organization” (McAfee, 2012, p. 24). By taking appropriate measures to ensure that sensitive and private data is protected, an organization is better prepared to mitigate the effect of cyber attacks and demonstrate that it has exercised due diligence. Additionally, by being proactive about maintaining IM/IT security, it can be expected that confidence in the organization’s ability to effectively manage and protect information under its custody will be strengthened.

There are several best practices used throughout the security industry regarding how sensitive and private data should be protected. According to the study conducted by the Ponemon Institute, organizations should firstly have clear policies that establish how sensitive data is to be managed (Bradley, 2011a, para. 5). In order to establish how sensitive data should be managed though, an organization will firstly need to establish an information security classification system. Once a classification system has been created, employees need to be informed about what security controls are in place and how they are expected to exercise proper information security management. Improved understanding amongst all employees about organizational security policies and requirements will likely reduce the chance that sensitive and private data are mismanaged. Another recommended practice is to simply not store sensitive or private information on public servers (“With new tactics,” 2011, para. 9). By storing data of this calibre on detached servers, it is much less likely that data will be compromised in the event of a successful data breach.

The 2011 hacktivist attack against Stratfor demonstrated the value of ensuring that sensitive and private materials are not stored in cleartext. By encrypting sensitive data, organizations are able to provide an extra layer of security to their system and better protect the data they control. The release of sensitive information may be damaging for both the targeted organization and the individuals who have had their information released. Recognizing the value of data encryption, Bradley (2011a) even goes so far as to suggest that organizations should introduce policies that require automating the encryption of data (para. 5). Given that not all data needs to be managed to the same degree, this suggestion is perhaps overstated. Nevertheless, it does exemplify the need for effective and thorough policies regarding the management and protection of sensitive and private data.

Because data encryption and data loss prevention tools can be expensive, the ability to procure these tools may be problematic for organizations that have limited financial resources. The purchase of the tools may be seen as too onerous of an investment. As Bradley (2011a) asserts however, the costs incurred by an organization as a result of a data breach may be far greater than the cost to invest in the proper security tools (para. 6). Depending upon the sensitivity of the data that is stolen in a data breach, the costs to an organization could be quite high. For organizations that manage sensitive and personal data then, the investment in sufficient data encryption and data loss prevention tools may be very much worthwhile.
8.2.3 Mitigate potential of successful DDoS attacks

DDoS attacks may not necessarily be destructive to an organization but they can be disruptive. The overall effect of DDoS attacks will vary though, depending upon the number of computers involved in an attack. While the broad access afforded by the Internet may limit the extent to which DDoS attacks can be prevented, there are several measures that organizations can adopt to mitigate the extent to which DDoS are successful. As Froutan (2004) asserts, by implementing an effective DDoS mitigation tool, organizations will be better prepared to withstand DDoS attacks (p. 2). Some of the practices for subduing DDoS attacks include sinkhole routing and bandwidth over-provisioning.

Sinkhole routing, is a security approach in which suspicious or bogus Internet traffic, such as the traffic sent during a DDoS attack, is diverted before it is sent to the intended server (Patrikakis, Masikos, & Zouraraki, 2004, “Route filter techniques”). The traffic is then analyzed by the server to determine whether or not the traffic is legitimate. Illegitimate traffic is dropped, while authentic traffic is sent to the intended server. This routing approach enables an organization to filter out unwanted traffic, mitigating the effects of a DDoS attack, while still allowing legitimate traffic to come in. Because it is not always possible to isolate unwanted traffic from legitimate traffic (Patrikakis, Masikos, & Zouraraki, 2004, “Route filter techniques”), this approach may result in some legitimate traffic inadvertently being discarded.

Over-provisioning is another means by which organizations can abate the effects of DDoS attacks (Froutan, 2004, p. 2). Over-provisioning refers to an organization’s ability to increase the amount of bandwidth its system can provide as the amount of online traffic increases (Froutan, 2004, p. 2). Because DDoS attacks work by repeatedly bombarding a network’s servers with high volumes of traffic, effectively consuming an organization’s available bandwidth, over-provisioning can be an effective means for responding to, and reducing the effects of, a DDoS attack.

8.2.4 Secure user accounts

Rendering secure user accounts is another important aspect of information security. Although protected user accounts in themselves will not prevent cyber attacks such as DDoS attacks or code injection, they do enable an organization to guard against outside users gaining unauthorized access to an organization’s internal resources and data. Some of the best practices regarding secure user accounts include taking measures to prevent brute force attacks, establishing strong password requirements, and generating usernames that are not obvious. Practices such as these improve the security of user accounts, and allow an organization to better protect its internal resources and data.

Establishing requirements for users to develop strong passwords is one best practice for securing user accounts. Strong passwords can be understood as denoting passwords comprised of multiple numbers and letters, both lower and upper case. The longer and more complex a password is, the less likely it will be that someone else will be able to guess someone’s login credentials (“Password management policies,” 2006, para. 6). As such, strong passwords serve as an effective access control mechanism. It has been noted that the more complex a password is, the
more difficult it may be for users to remember their passwords (“Password management policies,” 2006, para. 6). Accordingly, users may be more inclined to keep a written copy of their password which may weaken the overall security of an organization (“Password management policies,” 2006, para. 10).

Taking active steps to prevent brute force attacks is another method for establishing secure user accounts. Bill Cheswick, an employee at AT&T Labs Research, recommends requiring account lockouts after three to five failed login attempts as one method for inhibiting brute force attacks (as cited in Watson, 2010b, para. 3). By temporarily blocking continued efforts to access an account, an organization is able to thwart the efforts of individuals who may otherwise discover a user’s password through trial and error.

Another measure to enhance user account security is to make usernames hard to guess (Cheswick, as cited in Watson, 2010b, para. 3). If usernames are simply comprised of the first initial of someone’s first name, followed by their last name, individuals who are attempting to gain unauthorized access to a user’s account are only left with having to determine the user’s password. By generating usernames that are much less straightforward, an organization is able to make it increasingly difficult for attackers to discover, and subsequently exploit, an individual’s user account. This in turn adds another layer of security to the user accounts of an organization’s employees, and thus to the security of the organization overall.

8.3 Summary

In summary, there are a number of best practices for information security that have been advocated by security practitioners. A willingness to invest the time and resources necessary to check for network vulnerabilities, ensuring that sensitive data is encrypted, and establishing password requirements that are both practical and effective are just some of the smart security practices discussed in this chapter. While there are certainly additional best security practices used within the information security field, the examples drawn upon for this chapter were intended to highlight measures by which the BC government can shelter itself from the tactics commonly used by hacktivists.
The next chapter will provide a brief overview of this report’s discussion, and offer some final insights into the phenomenon of hacktivism and its relationship with the Government of British Columbia.

---

**BEST SECURITY PRACTICES**

- Invest the time and resources needed to regularly audit servers and conduct penetration tests of IM/IT systems
- Patch systems when vulnerabilities are discovered
- Develop a system for classifying the sensitivity of information
- Establish clear policies for how sensitive data should be managed
- Do not store sensitive data on public servers
- Encrypt all sensitive and private information
- Establish measures for mitigating the effects of DDoS attacks, such as over-provisioning
- Establish requirements for strong passwords
- Temporarily lockout user accounts after a pre-determined number of failed login attempts
- Make usernames more complex

---

Figure 9. List of best security practices
Chapter 9: Conclusion

Hacktivism is a complex phenomenon that has come to encapsulate much more than its original meaning. At first limited to technological development for the purposes of protecting people’s rights, hacktivism has since drawn comparisons to everything from electronic civil disobedience, to cyber vandalism, to cyber warfare. It is a complicated term that has consequently fostered a number of misconceptions about what hacktivism really means. The definition of hacktivism advanced in this report has emphasized the need for cyber attacks to protest or draw attention to social or political issues, without causing grievous harm to one’s target or deriving benefit for those involved in such attacks, in order to be considered acts of hacktivism.

While the number of issues that have galvanized socially and politically motivated cyber attacks since the late 1980s has been quite broad, recent instances of hacktivism may be understood as generally aligning with one of seven categories: privacy concerns; perceived instances of censorship; alleged corruption; elections; wrongdoing on the part of law enforcement; retaliation for arrests of alleged hacktivists; and general contempt. Yet despite these recurring trends, the extent to which instances of hacktivist attacks are actually increasing in number is somewhat inconclusive. Further complicating discussion of the topic is that the implications of successful hacktivist attacks may be overstated. Nevertheless, the fact remains that instances of hacktivism are occurring, and hacktivist attacks can pose serious risks to organizations.

Drawing upon current trends within hacktivism, and comparing them to the more prominent issues within BC today, there certainly appear to be a number of points of contention that could galvanize hacktivists into targeting the Government of BC. Yet despite this observation, there is nothing at this time to suggest that participants in hacktivism have any intent to target the Province. To date there have been no reports of hacktivist attacks being launched against the BC government. There have also been no instances of threats being issued, or condemnation being voiced, in response to the social and political issues in BC. As such, it does not appear that there is a strong likelihood that the BC government will be targeted by hacktivists. However, the threat of such attacks does still exist. Recognizing this, it is of value that the Province regularly reviews recent instances of hacktivism, and is cognizant of the types of policies or activities that could trigger hacktivist attacks.

Exercising best security practices is an effective means for protecting the Province’s resources and information under its custody. Such practices include regularly auditing IM/IT systems for security vulnerabilities, ensuring that all private and sensitive data is encrypted, and taking proactive measure to guard against the techniques most often used by hacktivists. By exercising due diligence in maintaining security, it is expected that the Province will be better prepared to guard against all cyber attacks and reduce the likelihood that such attacks are successful. This will likely improve the reputation of the Province for being a secure organization, reduce the likelihood that the Province will be subjected to the costs and embarrassment associated with attacks, and instil British Columbians with greater confidence that their personal and sensitive information is in fact protected.

The next chapter provides recommendations for how the Government of BC may improve its ability to anticipate and guard against hacktivist threats.

Hacktivism and the Government of British Columbia

67
Chapter 10: Recommendations

Drawing upon the report’s discussion, there are three recommendations for how the BC government can continue to improve its ability to anticipate and guard against hacktivist threats.

**Recommendation 1: The BC government should continue to monitor trends within hacktivism.**

By continuing to monitor trends within hacktivism, it is expected that the BC government will be better able to recognize the types of issues that galvanize hacktivists. This will reinforce the BC government’s knowledge about the types of issues that attract the attention of hacktivists, and subsequently improve the Province’s ability to identify emerging trends within hacktivism.

**Recommendation 2: The BC government should continue to periodically identify issues in BC that may attract the attention of hacktivists.**

Building upon its continued monitoring of hacktivist trends, periodically identifying issues in BC that may attract the attention of hacktivists will better allow the BC government to assess the possibility that it may be targeted by hacktivists. This will improve the Province’s ability to anticipate and guard against potential hacktivist attacks. In addition to reducing the likelihood that the Province may be unexpectedly targeted by hacktivists, this proactive approach may also foster improved information security awareness amongst the Province’s personnel.

**Recommendation 3: All areas within the BC government should be proactive about exercising best security practices for managing resources and information under their custody.**

In order to effectively guard against cyber attacks, it is essential that all areas with the BC government exercise best security practices for managing resources and information under their custody. When best security practices are adhered to, the Province is not only better able to protect information under its management, but is also able to demonstrate that it is exercising due diligence. In the event of a successful attack, it may be both embarrassing for the BC government and harmful to those individuals who have had their sensitive information compromised. A reluctance to adopt best security practices throughout government may impede the Province’s ability to guard against cyber attacks.
References


Anon_Central. (2012b, January 22). Dear new friends, #Anonymous is not a group which you can join. It is an idea which if you like, you follow & implement. You are the power [Twitter post]. Retrieved from http://twitter.com/#!/Anon_Central/status/161048597004169216


Hacktivism and the Government of British Columbia


Haktivismus and the Government of British Columbia 74


Hacktivism and the Government of British Columbia


---

Hacktivism and the Government of British Columbia


YamaTough. (2012b, January 16). We've decided not to release code to the public until we get full of it =) 1st we'll own evrthn we can by 0din' the sym code & pour mayhem [Twitter post]. Retrieved from http://twitter.com/#!/YamaTough/status/158995467861102592


Appendix 1. Research approach

The first step in the research process entailed reviewing what books about hacktivism the University of Victoria library had available. Using the search term hacktivism under ‘keyword anywhere’, only a limited number of books were found. Because hack did not provide any results, the search term cyber activism was also used. Quite a number of titles were found, but again only a limited number of books referenced hacktivism. Google Scholar was used to identify additional books about hacktivism that may have been overlooked in this initial search. Many of the books found in this search on Google Scholar were in fact available at the University of Victoria library. For books that were not available online or through the University of Victoria library, interlibrary loan requests were submitted to the University of Victoria library.

Several online databases made available through the University of Victoria’s library were also used during the initial research phase. Summon, JSTOR, and Academic Search Complete provided a wide array of academic journal articles and magazine and news articles related to the subject of hacktivism. These articles were useful for this report’s literature review and hacktivism background sections. Search terms that were used included hack, hacktiv, hacktivism, cyber security, cyber activ, cyber activism, cyber activist, internet activ, internet activist, and internet activism.

Building upon the materials made available through the University of Victoria, Google, Google News, and Wikipedia were used to identify additional resources and provide further detail about hacktivism and groups that commit hacktivism. Google and Google News were very useful for providing information about current instances of hacktivism, and what was being said about the phenomenon. These resources were also useful for identifying background information about the BC government, its security policies and efforts to promote transparency, and current contentious issues in the Province. Broad search terms used included hack, hacktivism, hacktivists, cyber activ, cyber activism, cyber activist, BC government, information security, and open government. When looking for details relating to a specific attack or group, more specific search terms were used. For example, one search phrase used in Google was “Anonymous and hacktivist and tactic”. Wikipedia was useful for providing context when gaps in the literature existed about a specific topic or event, as well as for identifying further resources using pages’ reference sections.

By adopting this research approach, an extensive number of resources are referenced in this paper. This approach was intended to reconcile any ambiguities or misunderstandings that exist within the literature, and provide an impartial discussion about hacktivism. As such, it is felt that this report provides a well-rounded discussion of what is currently being said about hacktivism, and a thorough review of current trends within the phenomenon.
Appendix 2. Hacktivism Background – Timeline

This timeline is comprised of events discussed in Chapter Five of this report. As a result, this timeline does not provide an exhaustive list of every socially or politically motivated cyber attack that may have occurred since the late 1980s. Readers should not infer that that socially or politically motivated cyber attacks did not occur during years where no events have been listed. Events included in this timeline are arranged chronologically.
Appendix 3. Hacktivism Today – Timeline

This timeline is comprised of events discussed in Chapter Six of this report. This timeline does not provide an exhaustive list of every socially or politically motivated cyber attack that has recently occurred. Additionally, readers should not infer that socially or politically motivated cyber attacks did not occur during years that have not been included in this timeline. Events included in this timeline are arranged chronologically.